Suruhanjaya Komunikasi Dan Multimedia Malaysia

Malaysian Communications And Multimedia Commission

GUIDELINE ON THE PROVISION OF WIRELESS LOCAL AREA NETWORK (WLAN) SERVICE

Malaysian Communications and Multimedia Commission

Off Persiaran Multimedia, 63000 Cyberjaya, Selangor Darul Ehsan.

Tel: +60 3 86 88 80 00 Fax: +60 3 86 88 10 00

www.skmm.gov.my

Introduction

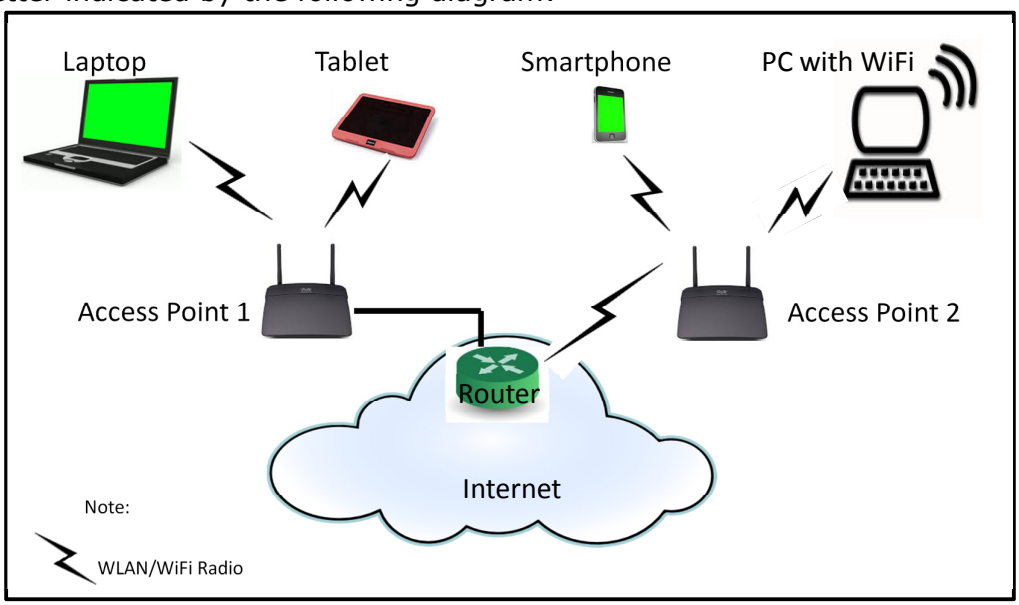
1. The Malaysian Communications and Multimedia Commission (the Commission) notes that there is a proliferation of parties deploying Wireless Local Area Network (WLAN) technologies using the 2400 MHz to 2500 MHz, 5150 MHz to 5350 MHz, 5470 MHz to 5650 MHz and 5725 MHz to 5875 MHz frequency bands to provide access to Internet service. The low cost of the equipment and the ease in setting up such networks, among others, make it an interesting and hassle-free arrangement in providing short-range wireless internet access to the public.

2. However, these "private" WLANs need to be connected to the public communications network, such as an Internet Access Service Provider (IASP) to provide both bandwidth and access to the Internet.

3. This guideline serves as a guide to any interested individual or business entity in providing internet access to the public by utilizing the frequency bands identified in this guideline.

The Ecosystem of WLAN

4. A WLAN allows for wireless connection between communication terminals. An access point (AP) would enable these terminals to access the Internet. This is better indicated by the following diagram:



5. An AP allows wireless devices to connect to a wired network using WLAN (e.g. Wi-Fi). The AP usually connects to the Internet via a router through wired (Ethernet) or Wi-Fi connections or it is part of a router itself. APs should include features such as firewall (FW) and Intrusion Prevention Systems (IPS) to protect users' incoming and outgoing traffic. This safety measure is critical to ensure that the relevant network is protected from any malicious activity[1].

6. Communication terminals are devices that have WLAN transceivers built in or connected to it to enable wireless interface with the AP.

7. Most WLANs are based on IEEE[2] 802.11 standard which is also known as "Wi-Fi". This standard exists in several protocols namely 802.11a, 802.11b, 802.11g and 802.11n. These protocols differ in relation to data throughput and channel sizes as shown in the following table:

Characteristics	**802.11b**	**802.11a**	**802.11g**	**802.11n**
Data rate (Maximum)	11 Mbit/s	54 Mbit/s	54 Mbit/s	288.9 Mbit/s for 20 MHz channel spacing From 6 to 600 Mbit/s for 40 MHz channel spacing
Channel size	5 MHz			5 MHz in 2.4 GHz band 20 MHz in 5 GHz band

Reference: Recommendation ITU-R M.1450-4 Characteristics of Broadband Radio Local Area Networks

[1] Such as hacking attempt, **Distributed Denial of Service (**DDoS) attack, malware propagation etc.
[2] Institute of Electrical and Electronics Engineers

WLAN Access

8. There are several types of accessing network within a relevant WLAN. The table below provides some examples:

Access Network Type	Description
Private network	Non-authorized users are not permitted on this network (e.g. home networks and enterprise networks).
Private network with guest access	Private network but guest accounts are available (e.g. enterprise network offering access to guest users)
Chargeable public network	The network is accessible to anyone with charges (e.g. hotel offering in-room internet access service)
Free public network	The network is accessible to anyone with no charges (e.g. airport hotspots, municipal network providing free service etc).
Personal device network	A network of personal devices (e.g. a PC connected to a printer)

Reference: IEEE PART 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

Network Security in WLAN

9. WLAN Hotspot Providers (WHP) should install security features to their APs to prevent any malicious activity and protect the network. There are several methods that can be employed to ensure the security of the WLAN. The method chosen would depend on the type of protection required and the users that the service is being provided to.

Encryption Technique

10. The encryption method which is widely used is Wi-Fi Protected Access II (WPA2). This particular method is the current generation of security protocol in Wi-Fi networks that incorporates Advanced Encryption Standard (AES) for data protection and improved network access control. This approach involves using password to gain access to the AP.

11. The encryption technique is normally used in public hotspots which provide free Internet access (e.g. restaurants, shopping outlets, airports etc.).

Access Control

12. Access to the AP is controlled using Remote Authentication Dial In User Service (RADIUS) protocol. In order to implement this security measure, the WHP should have a RADIUS Server to provide centralized authentication, authorization and accounting (AAA) for users.

13. This method is normally used in private or chargeable public hotspots for paid Internet service.

Relevant Regulatory Framework under the Communications and Multimedia Act 1998

14. The relevant regulatory framework which applies to WLAN activities would include the following:

(a) Communications and Multimedia Act 1998 (CMA 1998);
(b) Communications and Multimedia (Licensing) Regulations 2000;
(c) Communications and Multimedia (Spectrum) Regulations 2000;
(d) Communications and Multimedia (Technical Standards) Regulations 2000;
(e) Standard Radio System Plan on Requirement for WLAN Systems operating in the frequency bands 5150 MHz to 5350 MHz;
(f) Notification of Issuance of Class Assignments (Second Schedule); and
(g) The Malaysian Communications and Multimedia Content Code.

Licensing Requirements

15. The licensing requirements for the provisioning of WLAN services is as follows:

(a) An IASP which provides internet access and wireless hotspots services to end users will require the following licenses:
    i. An Applications Service Provider (ASP) class license for the provisioning of retail internet access service;

ii. A Network Facilities Provider (NFP) license if the IASP intends to own or deploy the network facilities [e.g. fixed links and cables and RTL (AP)]; and

iii. A Network Service Provider (NSP) license if the IASP is providing network and bandwidth management services as well.

An IASP can also choose to work with an existing NFP and NSP licensee under the CMA 1998. Details of the said licensee must be provided to the Commission.

The NFP and NSP license falls under two broad categories namely, the Individual license and Class license category.

The Commission will assess and inform applicants of the appropriate type or category of the license that it has to hold in order to provide the above facilities and/or service. This is dependent on the Commission's assessment of the scope and scale of the applicant's proposed activities.

Please refer to the License Application Procedure and Licensing Criteria Guidebook that is available on the Commission's website for further explanation and guidance.

(b) Owners or tenants of any premise or establishment that employ or subscribe to WLAN facilities and services from licensed service providers[3] under the CMA 1998 need not apply for any licenses from the Commission.

The party that acts as the **service provider** is the **party** that must hold the requisite license(s).

[3] ASP, NFP and NSP licensees

16. Any parties who need any further clarification on licensing matters should contact the Commission's Licensing Department.

Content Filtering

17. WHPs should take the necessary action to ensure that users of the WLAN do not access online content that is prohibited under the relevant laws of the country.

18. In this regard, WHPs should install the appropriate facilities (such as filters) in their network to ensure that this prohibited content[4] is not accessible.

19. WHPs should also include the appropriate warning notices on prohibited content on their service's landing page.

Spectrum and conditions

20. The Commission, pursuant to Section 169, CMA 1998, had on 1 April 2010, issued Class Assignments No. 1 of 2010, which cover "Short Range Radiocommunications Device". Short range radiocommunications device is defined as "radiocommunications device that provides either unidirectional or bidirectional communication over short distances for mobile and fixed applications in the designated frequency bands".

21. The short range radiocommunications device is not restricted by technology as long as it is being used for the purpose as defined above.

22. Interested users should ensure that the device used complies with the conditions specified in the Class Assignment.

23. The frequency bands and the maximum Effective Isotropic Radiated Power (EIRP) for the short range radiocommunications device[5] which are related to WLAN are:

[4] Prohibited content would include, but is not limited to content that is indecent, obscene, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass any person

Item	Frequency Bands	Maximum EIRP	Usage
1.	2400 MHz to 2500 MHz	500 milliWatts	Outdoor/Indoor
2.	5150 MHz to 5350 MHz	1 Watt	Indoor
3.	5470 MHz to 5650 MHz	1 Watt	Outdoor/Indoor
4.	5725 MHz to 5875 MHz	1 Watt	Outdoor/Indoor

24. It has to be noted that installation of WLAN systems in the 5150 to 5350 MHz band within 30 km of any airports in Malaysia requires special approval from the Commission.

25. To ensure that parties deploying WLAN comply with the EIRP limit of the relevant WLAN equipment, no adjustment to the WLAN antenna is allowed.

26. The formula to determine EIRP is shown below and some sample calculations are provided in **Appendix A**:

$EIRP = P_{out} - C_t + G_t$

P_{out} = transmitter power output (dBm)
C_t = signal loss in cable (dB)
G_t = gain of the antenna (dBi)

Interference in WLAN

27. Most of the WLANs use frequencies within the 2.4 GHz band. The use of this band by WLAN users is quite extensive compared to other types of users.

28. Interference can occur between two or more WLANs. This type of interference is known as co-channel and adjacent channel interference. However, since WLAN devices use the same protocols, the interference can be managed within the network itself.

[5] Refer to Table A (Frequencies and Maximum EIRP), Second Schedule, Notification of Issuance of Class Assignments No. 1 of 2010.

29. The same band is also shared by industrial, scientific and medical (ISM) related devices. As such, there is a higher likelihood of interference between ISM and WLAN users. Therefore, new deployment of WLAN especially in urban and industrial areas is encouraged in the 5 GHz band, which is relatively less congested compared to the 2.4 GHz band.

30. Some of the WHPs also use WLAN to connect their APs to internet router (bridging). To ease congestion in the 2.4 GHz band, this type of application will only be allowed in the 5 GHz band.

WLAN Common Platform

31. In public hotspot, users normally have to search and choose WLAN network, request and acknowledge the connection to the AP for the first time login. Subsequent access to the same AP will not require active input from users since the user's device would memorize the login password associated with the AP. However, the first time login has to be repeated when accessing different AP with different Service Set Identifier (SSID) or network name.

32. In private and chargeable public hotspots, access to AP is via login password that is associated with the particular user. The user's information is kept in a database (Radius server) by the WHP.

33. Seamless access to APs from different networks is possible if there is a common platform where the user's database can be shared. WHPs are encouraged to work together toward sharing their database at a common platform for seamless roaming or transfer between their APs.

34. The use of any solutions that support the seamless access (e.g. Seamless Session Transfer) to the APs across different networks is also encouraged.

35. This common platform can enable mobile data offloading (WiFi offloading) to WLAN. However, the WHP needs to ensure that this is not to detrimental to WLAN common users.

Support Service

36. WHPs that provide chargeable access need to provide support services to the users of their WLAN.

37. They should be able to do remote service monitoring and system restoration in case of system failure.

38. WHP should publish their hotline number for users to contact in case of service failure.

Short Range Radiocommunications Device

39. The Class Assignments (No. 1 of 2010) indicates that only a certified short range radiocommunications device shall be used or operated in the frequencies specified above.

40. As such, prospective WHP shall ensure that short range radiocommunications devices used in respect of the wireless hotspot service are certified by the Commission's designated certifying agency (SIRIM QAS International) in accordance with the Communications and Multimedia (Technical Standards) Regulations 2000.

Fees Payable

41. Regulation 27 of the Communications and Multimedia (Spectrum) Regulations 2000 states that "no fee shall be payable for a class assignment" in respect of the use of the frequency bands identified.

Compliance to standards and procedures

42. It is a mandatory requirement for current and potential WHP or WLAN users to ensure that their devices (access points and WLAN modules in their communication devices) operate within the allowable power limits and in accordance with the process stipulated in the relevant instruments such as the SRSP and Class Assignment issued in relation to this matter. Non-compliance with these instruments is an offence under section 242 of the CMA and the offender shall be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

Effective Date

43. This Guideline is effective from 11 November 2013 and supersedes the previous Guideline on The Provision of Wireless LAN Service (MCMC/G/01/05 – WLAN).

Contacts

44. For any queries and further information, please contact:

Policy Planning and Review Department (PPRD)
Malaysian Communications and Multimedia Commission
Tel : +60 3 8688 8000
http : www.skmm.gov.my

and for specific query on certification process please contact:

SIRIM QAS International Sdn. Bhd.
Tel : +60 3 5544 6400
Fax : +6 03 5544 6407
http : www.sirim-qas.com.my

Appendix A

Effective Isotropic Radiated Power (EIRP)

$EIRP = P_{out} - C_t + G_t$

EIRP = Effective Isotropic Radiated Power (dBm)
P_{out} = transmitter power output (dBm)
C_t = signal loss in cable (dB)
G_t = gain of the antenna (dBi)

The maximum EIRP for Class Assignment WLAN type devices;

Item	Frequency Bands	Max EIRP (Watts)	Max EIRP (dBm)
1.	2400 MHz to 2500 MHz	500 milliWatts	27 dBm
2.	5250 MHz to 5350 MHz	1 Watt	30 dBm
3.	5470 MHz to 5650 MHz	1 Watt	30 dBm
4.	5725 MHz to 5875 MHz	1 Watt	30 dBm

dBm to Watt Conversion Table :

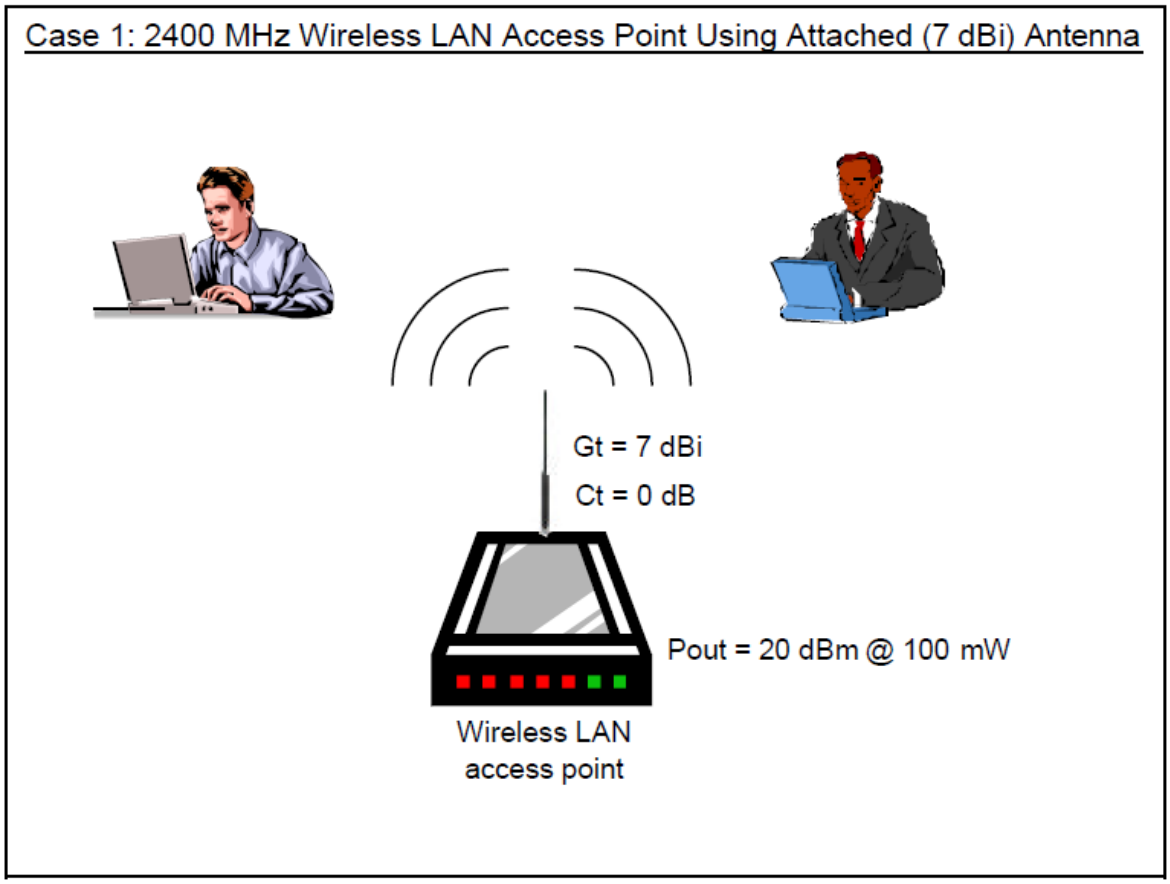
dBm	Watts (W)
0	1.0 mW
1	1.3 mW
2	1.6 mW
3	2.0 mW
4	2.5 mW
5	3.2 mW
6	4 mW
7	5 mW
8	6 mW
9	8 mW
10	10 mW
11	13 mW
12	16 mW
13	20 mW
14	25 mW
15	32 mW

dBm	Watts (W)
16	40 mW
17	50 mW
18	63 mW
19	79 mW
20	100 mW
21	126 mW
22	158 mW
23	200 mW
24	250 mW
25	316 mW
26	398 mW
27	500 mW
28	630 mW
29	800 mW
30	1 W
31	1.3 W

dBm	Watts (W)
32	1.6 W
33	2.0 W
34	2.5 W
35	3.2 W
36	4.0 W
37	5.0 W
38	6.3 W
39	8.0 W
40	10 W
41	13 W
42	16 W
43	20 W
44	25 W
45	32 W
46	40 W
47	50 W

mW = miliWatts

Sample EIRP Calculation : Case 1

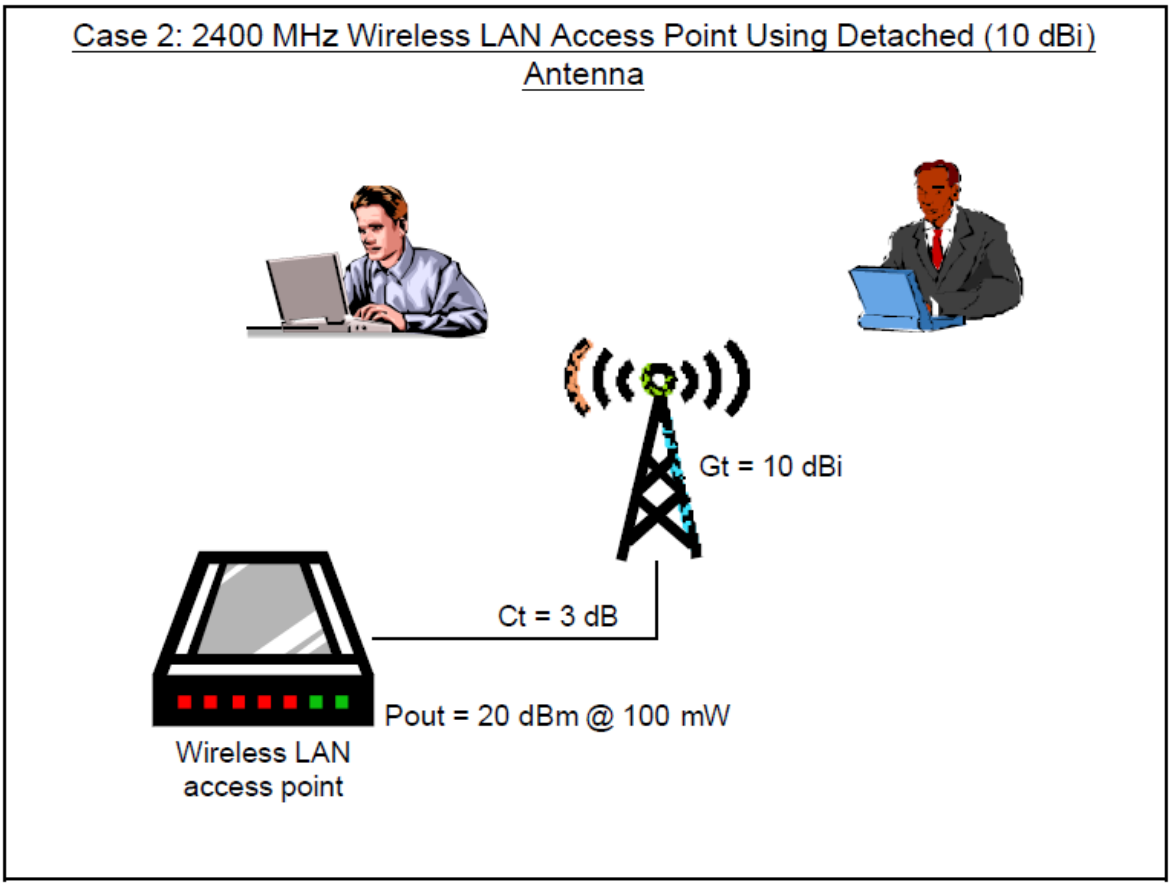


The EIRP calculation;

EIRP = 20 dBm – 0 dB + 7 dBi
= 27 dBm @ 500 milliWatts

The usage of the 2400 MHz Wireless LAN device with a 7dBi antenna is within the allowed maximum EIRP which is at 500 milliWatts.

Sample EIRP Calculation : Case 2

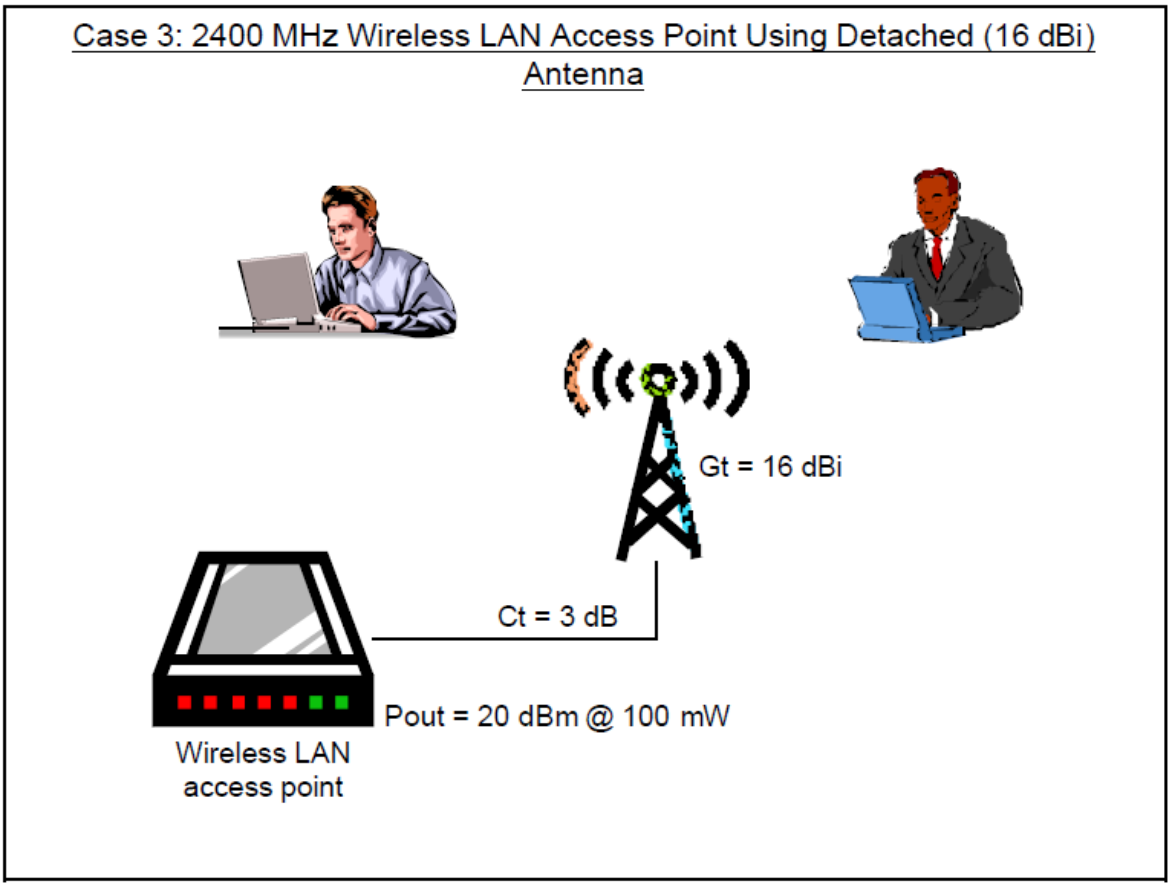


The EIRP calculation;

EIRP = 20 dBm – 3 dB + 10 dBi
= 27 dBm @ 500 milliWatts

The usage of the 2400 MHz Wireless LAN device is within the allowed maximum EIRP which is at 500 milliWatts .

Sample EIRP Calculation : Case 3



The EIRP calculation;

EIRP = 20 dBm – 3 dB + 16 dBi
= 33 dBm @ 2 Watts

The usage of the 2400 MHz Wireless LAN device **exceeds and breaches** the allowed maximum EIRP which is at 500 milliWatts. Users have to either reduce the P_{out} or use lower gain antenna to meet the maximum allowed EIRP.