Guide for Businesses

wireless @SG

Version	Date	Updates/Changes
1.0	9 Jan 2015	
1.1	13 Apr 2016	Access speed upgrade to 5Mbps
1.2	10 May 2016	Revision of backhaul requirements
1.3	13 Oct 2016	Changes of reference to IDA
1.4	28 Apr 2017	Revision to general info, inclusion of MyRepublic, access speeds of at least 5Mbps, registration and authentication, and branding
1.5	8 Apr 2019	Revision to requirements

General Information

Intended Audience

This document is intended for businesses, venue owners, premise tenants (“Companies”) who are planning to procure Wireless@SG services from any of the designated Wireless@SG operators (“Operators”).

Purpose

The document aims to

- Illustrate some of the considerations and highlight some guidelines Companies should consider when planning for Wireless@SG deployments;
- Inform Companies of the base specifications that are required for Wireless@SG hotspots. Companies can consider increasing some of the base specifications and including these as part of their requirements in their service contract with the Operators.

Structure

This document is divided into 2 parts:

1. General Information on Wireless@SG
2. Procuring Wireless@SG services for Venues

1. General Information on Wireless@SG

About Wireless@SG

Info-communications Media Development Authority (IMDA) launches the Wireless@SG programme in 2006 to accelerate the deployment of high-speed wireless broadband, promote wireless broadband lifestyle amongst citizens, and catalyse the wireless broadband market in Singapore. Since its launch, Wireless@SG has successfully catalysed Singapore's wireless broadband market, and spawned an "always connected" culture amongst Singaporeans.

Over the years, the programme has introduced several new enhancements to improve user experience and drive adoption of innovative enterprise services.

Beginning from April 2014, consumers get to enjoy faster basic access speed of at least 5 Mbps. Accessing the hotspots has been simplified, where users can now seamlessly login using the Wireless@SG app (one-time setup required) on supported smartphones and tablets without the need to enter their login credentials (user ID and password), and be able to automatically connect all the time. For foreign visitors, they are now able to perform account registration at any Wireless@SG hotspot and an OTP will be delivered to their foreign mobile numbers.

The programme has also evolved to encourage the Operators to develop innovative enterprise services leveraging on the same Wireless@SG network ("Network"). These innovative services will enable venue owners to be more productive, and at the same time, generate revenue for the Operators, enabling a self-sustainable model to help support the continued provision of free Wi-Fi access to the public.

Venue owners, who desire to provide free Wi-Fi to their premises, are encouraged to work with the Operators on commercial agreements. The Operators will need to explore with the venue owners to understand their business needs before extending the service coverage to their premises.

2. Procuring Wireless@SG services for Venues

Considerations for Planning and Deployment

Companies need to consider the intended area of coverage, the capacity and type of crowd, and the availability of supporting infrastructure. These are factors that will be asked by the Operators during the initial planning and site survey, so that they can design the network infrastructure and configuration.

Wireless@SG Requirements

1. Intended Coverage Area

   Companies will have to consider the size and environment of the intended coverage area. This, together with the expected crowd size and usage, will determine the number of APs and the degree of weatherproofing that will be required. Varying degrees of coverage include closed indoor environments such as lobbies, restaurants and retailers, and outdoor environments such as roof gardens and taxi stands. The crowd size at these locations and the type of applications that might be used will also be considered.

2. Existing Infrastructure

   From the physical infrastructure point of view, the location of the MDF (Main Distribution Frame) room, the server room and the intended coverage area will need to be identified for the network cabling.

   From the network perspective, IMDA recommends that all newly deployed hotspots to have a backhaul of at least 100 Mbps bandwidth for sites with one access point.

   In the event that backhaul bandwidth utilization exceeds 80% of its capacity limit over five (5) consecutive occurrences or eight (8) occurrences in a calendar month, Companies are advised to engage the appointed Operator for a bandwidth upgrade recommendation.

3. Equipment

   When setting up the infrastructure for Wireless@SG, Companies can choose to own the Wireless LAN equipment, or lease the equipment from the Operators as a managed service. As a best practice, Companies should also request that Operators declare the brand and model of the equipment in their contracts.

   Each hotspot shall support at least twenty (20) concurrent devices. However, the Wireless@SG programme requires that a downlink access speed of at least five (5) megabits per second (5 Mbps) be available per device at each hotspot. Companies can choose to increase the number of concurrent devices and the downlink access speed above and beyond the programme requirements. To illustrate an example, a hotspot with a backhaul bandwidth of 250 Mbps can support:

- a maximum of fifty (50) concurrent devices with a downlink access speed of five (5) megabits per second, or
- a minimum of twenty (20) concurrent devices with a downlink access of five (5) megabits per second

4. Guidelines around Wireless@SG Services

The Wireless@SG service consists of basic services, which is free to general public; and other value-added services that can be provided based on the Company's request. The following describes some of the guidelines around the use of Wireless@SG equipment, services as well as the registration and authentication of users.

a) Use of Wireless@SG equipment

All Access Points shall be compliant with standards depicted by IMDA and shall broadcast both "Wireless@SG" and "Wireless@SGx" Service Set Identifiers (SSIDs) for the purpose of providing Wireless@SG services at the Company's premise. IMDA reserves the right to stipulate additional SSIDs where necessary for basic tier service. The Network shall support at least 16 SSIDs and a different set of services can be provided with each SSID. Each access point shall be able to support both IPv4 and IPv6 protocols, and all equipment and elements within the Network shall be IPv6 ready. It shall be able to support devices/clients that are certified by Wi-Fi Alliance, Wireless Broadband Alliance, Next Generation Hotspots, and type-approved by IMDA. Access points have to be dual-band ready (2.4GHz & 5GHz). The Network shall be configured to prioritise 5GHz channels as the preferred connectivity option for client devices. The access point deployed shall support IEEE 802.11 a/b/g/n/ac devices.

b) Basic Tier Service

All deployed Wireless@SG hotspots shall offer a basic tier service ("Basic Services") free to the general public. Basic Services shall offer unlimited service plans with a downlink access speed of at least 5 megabits per second and uplink access speed of at least 2.5 megabits per second. Companies can consider requiring network speeds above and beyond these numbers in their service contracts with the Operators.

The Network shall allow access to applications such as, but not limited to, email, internet browsing, instant messaging, peer-to-peer programs, virtual private network ("VPN") tunnelling, voice over Internet Protocol ("VOIP"), online gaming, video-streaming, and video-conferencing provided that such applications are in compliance with standard-based technology and the bandwidth requirements of Basic Services at all times. Ports used by these applications shall not be blocked. The Network shall also be capable of supporting traffic originated from multicast protocol within the bandwidth requirements of Basic Services. However, Operators will be allowed to take appropriate actions if any user of such applications poses a threat to the health and security of the Network.

c) Roaming Support

The Network shall allow registered users of all Operators to roam in its Network.

d) Registration and Authentication for Wireless@SG Users

Users of the Wireless@SG service will need to login using their Wireless@SG account credentials to access the Wireless@SG service. There are two methods for user authentication:

i. Universal Access Method (via Web Login)

Registered users can access the Wireless@SG service via a captive web portal. The captive portal shall provide a registration and login page for users to enter their mobile number and One-Time Pin (OTP) to access the Wireless@SG service.

ii. Extensible Authentication Protocol Method – EAP-PEAP/ EAP-SIM/ EAP-AKA (one-time setup via App)

The network shall authenticate the Wireless@SG users to the Wireless@SG network using IEEE 802.1x authentication framework with Protected Extensible Authentication Protocol version 0 / Microsoft Challenge Handshake Authentication Protocol version 2 (PEAPv0/MSCHAPv2) authentication method.

This network shall also authenticate users based on the identification details stored in the users' 3G/4G SIM card after a one-time configuration. Operators shall implement Extensible Authentication Protocol for SIM-login authentication such as GSM Subscriber Identity Module (EAP-SIM) and Universal Mobile Telecommunications System (UMTS) Authentication and Key Agreement (EAP-AKA) and the like in all of its Wireless@SG Hotspots.

The designated Operator for the hotspot shall ensure that they interface with all Operators for

i. The authentication of all locally issued SIM and USIM cards.

ii. The purpose of performing EAP-SIM/ EAP-AKA authentication and ensure that all EAP-SIM/ EAP-AKA transactions can be routed successfully to and fro all Operators based in Singapore.

iii. In the case whereby the designated Operator is also a mobile operator based in Singapore, the designated Operator shall ensure all locally issued SIM and USIM cards issued by the designated Operator can successfully be authenticated. For the avoidance of doubt, this shall include SIM and USIM issued to Postpaid, Prepaid, Multi-SIM and the like of all mobile subscribers of the designated Operator.

All authentication services above shall be available twenty-four (24) hours a day, seven (7) days a week and provided free-of-charge to all Wireless@SG users during the entire Wireless@SG Programme.

e) Security

In terms of security, Companies are to engage Operators to ensure the physical security for network equipment and proper authorised access. Companies can also choose to include additional requirements for network security.

f) Physical security

Companies shall assist Operators to put in place measures to ensure the physical security for all critical network equipment within the direct control of the Company and in accordance with standards and procedures adopted by the Company and the building management where such equipment is located. Subject to any third party approval being sought, the Company shall use reasonable efforts to ensure that the wireless network equipment installed on-site shall be controlled and restricted to authorised personnel only; and shall not be easily accessible by the public.

g) Network Security and Vulnerability Management

Operators shall ensure that the wireless network equipment is configured securely in accordance to the industry best practices. Relevant steps shall be undertaken to manage all the security vulnerabilities that affect the wireless network equipment. Companies can consider requiring Operators to include network intrusion detection systems and/or host based intrusion detection systems as part of their tender.

h) Network Segregation

If Wireless@SG service is provided through infrastructure shared with other Wireless LAN (WLAN) services, Virtual LAN shall be created to segment the Wireless@SG network from the rest of the WLANs.

5. Additional Features

a) Customer support and Problem Resolution for Wireless@SG Users

Operators must provide users with customer support for Basic Services which, at the minimum, shall provide resolution to issues related to Network connectivity problems and service interruption or degradation, provided that such issues or problems are not caused by any wilful act, omission and default by the users.

Companies shall engage Operators to provide additional levels of customer support beyond the existing avenues which include hotline number and email.

b) Network Audits

IMDA conducts network audits on Wireless@SG network from time to time. This is done to ensure that the network meets IMDA's service level requirements that are stipulated to the Operators. The Company shall allow IMDA-appointed network auditors to conduct such audits at their premises.

c) Operating Hours

All deployed Wireless@SG Hotspots shall:

i. Be operated twenty-four (24) hours a day, seven (7) days a week;

ii. Achieve at least 95% deployed hotspot availability;

iii. Achieve at least 99% site availability; and

iv. Achieve at least 99.9% network availability.

d) Branding

Wireless@SG service is a trademark owned by IMDA. The Company is allowed to be associated with the trademark and the use of the Wireless@SG logo. The designated Operator shall maintain the Wireless@SG service in relation to all the requirement specifications stipulated by IMDA throughout the Contract Period.