



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring D-Link Wireless 802.11b/g Access Point and Extender Adapter to Support Avaya VPNremote™ Phone - Issue 1.1

Abstract

These Application Notes provide a sample step by step procedure for configuring the D-Link wireless router and extender to support an Avaya VPNremote™ Phone in an environment consisting of Avaya Communication Manager and Avaya IP Telephones.

1. Introduction

These Application Notes provide a solution for configuring the D-Link router and D-Link extender to support an Avaya VPNremote Phone. The D-Link DWL-G820 extender is a wireless 802.11b/g (WiFi) solution that provides a wireless transport within the reasonable/acceptable range of the D-Link equipment. This wireless network spares the expense of installing cables in a home environment and it will allow the client computer and the Avaya VPNremote™ Hard Phone (via the extender) to be relocated to another part of the office or room.

These Application Notes present the following steps to configure the D-Link Access Point and D-Link extender:

- Basic configuration of the Access point
- Basic configuration of the Extender / gaming adapter
- Verify the WiFi operational connectivity between the 2 D-Link devices

1.1 Product Overview

1.1.1. D-Link DWL-G820

The D-Link DWL-G820 is a wireless extender / wireless gaming adapter which will transform any Ethernet device (i.e., Avaya VPNremote™ Phone) into a wireless device. The D-Link DWL-G820 provides wireless access to the Access Point (AP) for devices such as the Avaya VPNremote Phone.



1.1.2. D-Link DWL-2100AP

The D-Link DWL-2100AP acts as a bridge between the wired network and wireless devices. Multiple devices can connect through the D-Link DWL-2100AP to gain access to the network.



2. Network Architecture Environment

Figure 1 illustrates the configuration used in these Application Notes. Avaya IP Telephones register with Avaya Communication Manager at the Corp site. The DHCP server will assign an IP address to the VPNremote Phone. The VPNroute phone is configured to use the Juniper Networks SSG 520 for VPN termination. No changes or modifications are required to the existing IP Telephony infrastructure.

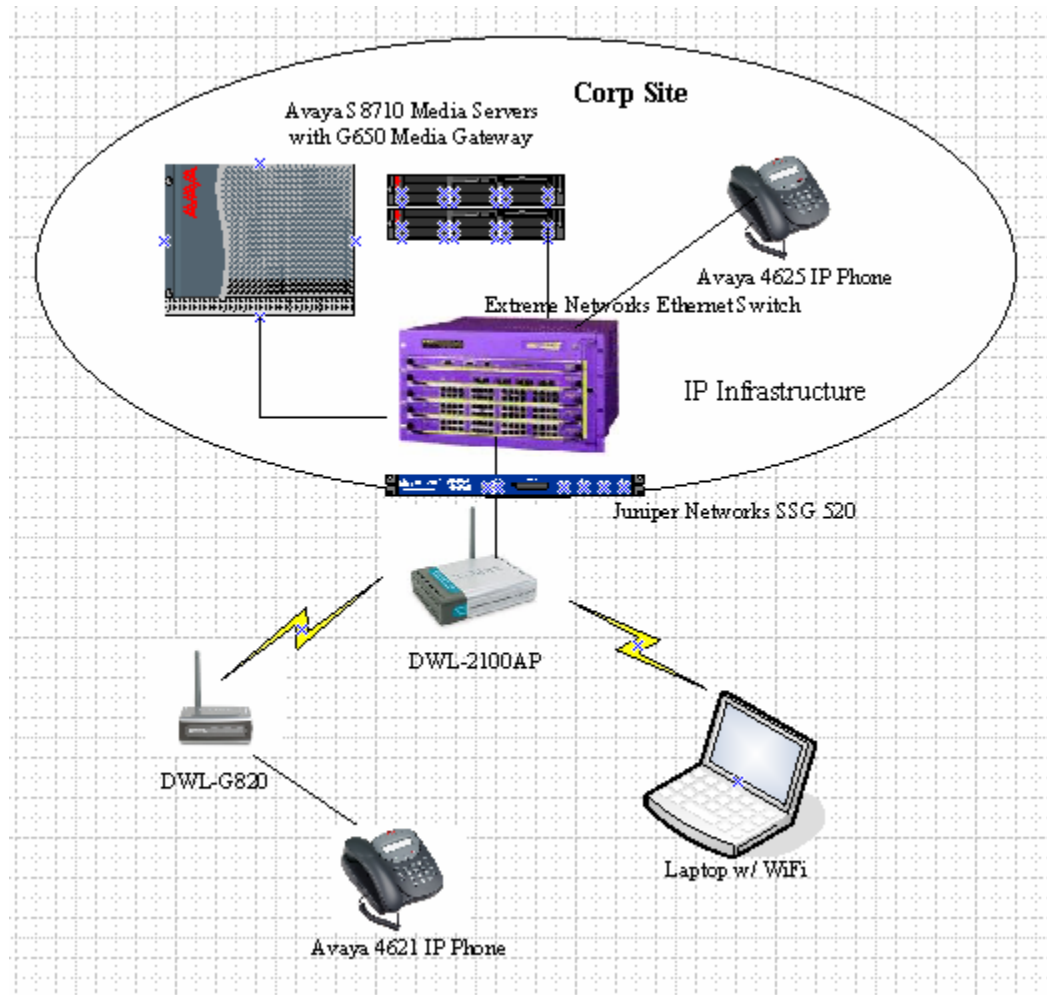


Figure 1 Network Configuration

2.1 Terms and Definitions

Basic Wired Equivalent Privacy (WEP) encryption method will be used in this small wireless network application to stop the interception of radio frequency signals by unauthorized users. WEP

is based on the RC4 encryption algorithm by RSA Data Systems. All clients and Access Points must be configured with the same key for encryption and decryption to work properly.

Service Set Identifier (SSID) functions as a simple password by allowing a wireless network to be split up into different networks each having a unique identifier. The SSID must be set in the Access Point. Each client computer and extender must be configured with the corresponding SSID for that network.

2.2 D-Link Performance Option Settings

- **Standard/default (Disable)** – Standard 802.11g support, no enhanced capabilities (up to 54Mbps).
- **Super G without Turbo** – Capable of Packet Bursting, FastFrames, Compression, up to 72Mbps and no Turbo mode.
- **Super G with Dynamic Turbo** - Capable of Packet Bursting, FastFrames, Compression, and Dynamic Turbo. This setting is backwards compatible with non-Turbo (legacy) devices. Dynamic Turbo mode is only enabled when all devices on the wireless network are Super G with Dynamic Turbo enabled.
- **Super G with Static Turbo** - Capable of Packet Bursting, FastFrames, Compression, and Static Turbo. This setting is not backwards compatible with non-Turbo (legacy) devices. Static turbo mode is always on and is only enabled when all devices on the wireless network are Super G with Static Turbo enabled.

3. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration provided:

Device Description	Versions Tested
Avaya S8710 Media Server	Avaya Communication Manager 3.1.2 (R013x.00.1.632.1)
Avaya G650 Media Gateway	-
TN2312BP IPSI	FW 22 (HW6)
TN799DP C-LAN	FW 16 (HW1)
TN2302AP IP MedPro	FW 108 (HW12)
Avaya 4621SW IP Telephones	R2.6 – (a02d01b2_6.bin)
Avaya 4625SW IP Telephones	R2.5 – Application (a25VPN252_1.bin)
Juniper Networks Secure Service Gateway 520	ScreenOS 5.4.r1.0
D-Link DWL-G820 Extender/Gaming Adapter	Firmware Version: 1.00
D-Link Broadband Router – DWL-2100AP	Firmware Version: 2.10

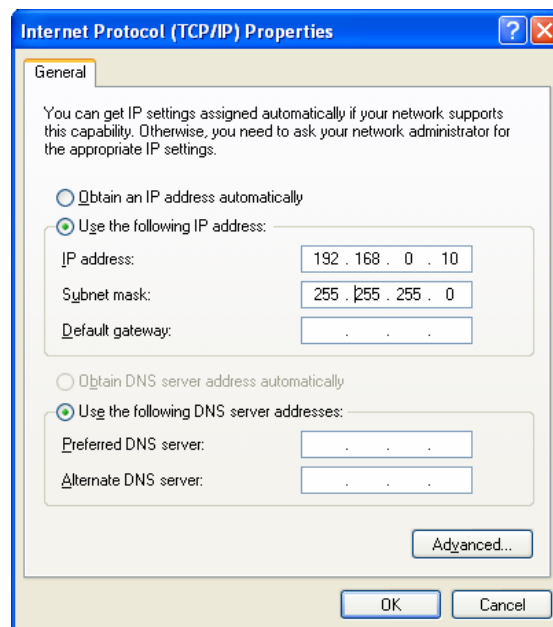
Table 1 – Equipment and Software Validated

4. Configure D-Link Wireless Devices

This section describes the configuration for the D-Link DWL-2100AP and DWL-G820 devices shown in **Figure 1**. Both of these D-Link devices can be configured using a computer connected directly with an Ethernet cable and using the web browser or the AP Manager software that is included in the CD with the D-Link package. These Application Notes utilize the web browser configuration utility to configure both of these devices.

4.1 Configure the D-Link DWL-2100AP Access Point

1. Connect the power adapter to the back of the DWL-2100AP and then plug the other end of the power adapter to the wall outlet. The power LED will indicate the proper operation.
2. Connect the Ethernet cable to the DWL-2100AP and the other end directly to a computer for the initial configuration. (Note: The Ethernet port of the DWL-2100AP is Auto-MDI/MDIX which means a straight-through or a crossover Ethernet cable can be used.)
3. Assign a static IP Address to the computer so it communicates with the DWL-2100 AP as shown below. Go to **Control Panel > Network Connections > Local Area Connection > Properties > Internet Protocol (TCP/IP)** and check “Use the following IP address”. Enter 192.168.0.10 for the IP address and 255.255.255.0 for the subnet mask. Select “OK” on this screen and subsequent screens to exit the Control Panel. It is not necessary to complete the rest of the fields, since it is on the local network.



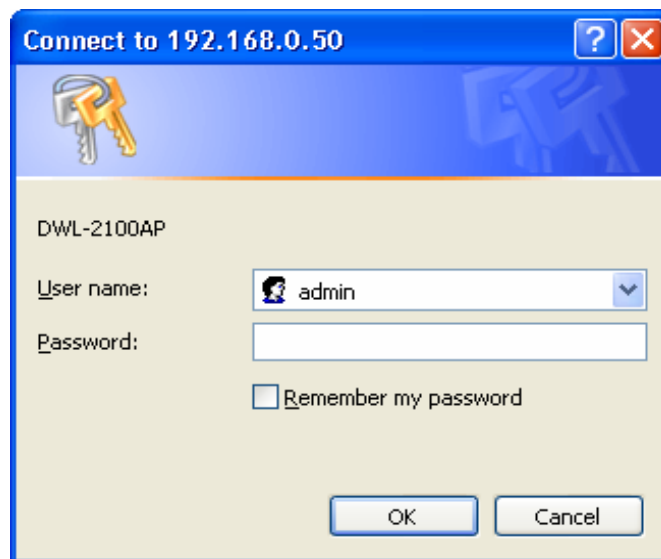
4. Open the web browser and enter the following URL using the DWL-2100AP default IP address “http://192.168.0.50” and press **Enter**.



In the login screen that appears, use the following user name and password.

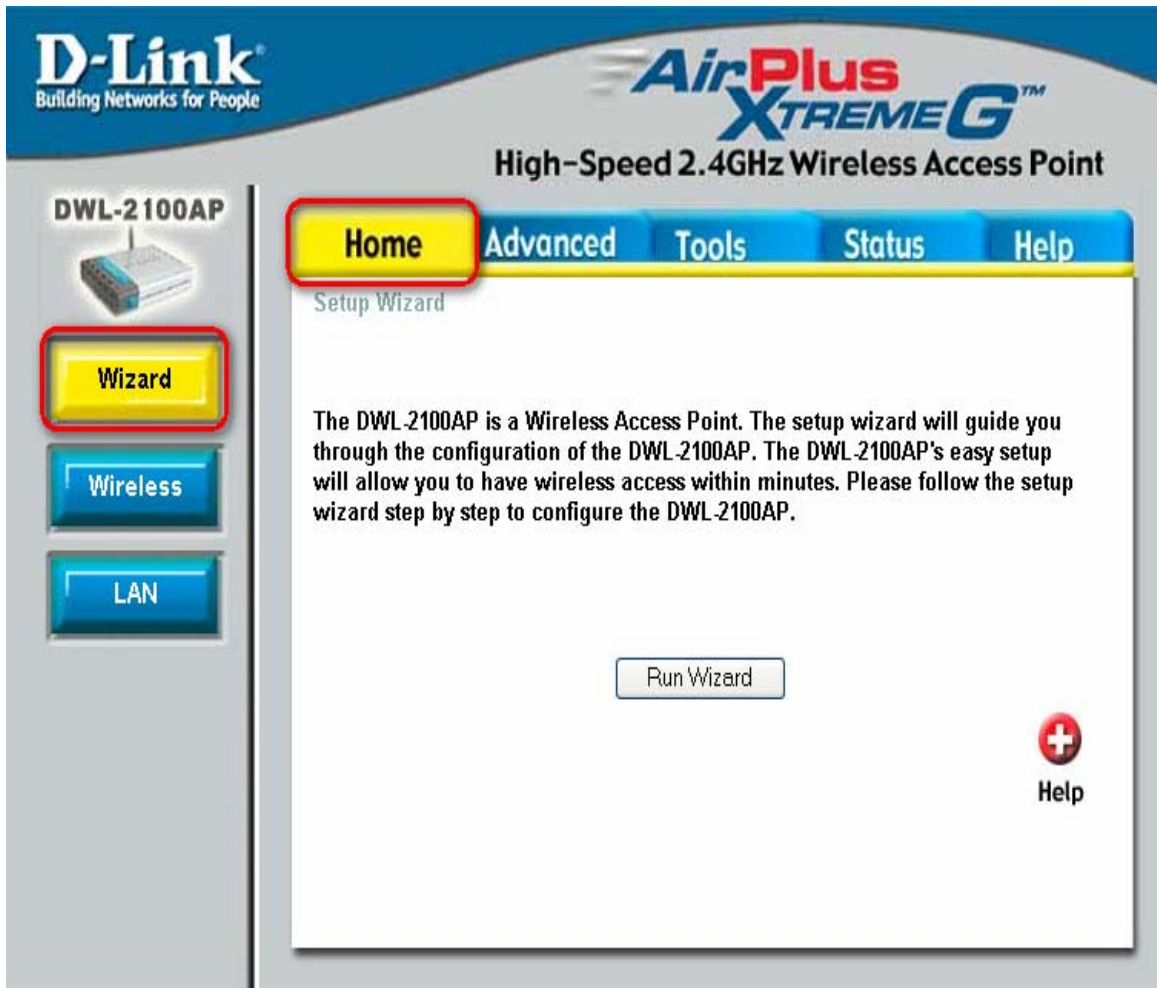
User name: admin

Password: (blank for default)



The DWL-2100AP configuration home page is displayed after successful logon.

5. On the DWL-2100AP home page, select the **Home** tab followed by the **Wireless** button in the left column.



6. On the screen that appears, enter the values as shown below.

SSID → lab

Encryption → Enable

Key Type → ASCII

Option to use either ASCII or HEX key type

Key Size → 64 bits

64 bits encryption key is only use for basic security demonstration setup for this application note.

Valid Key → First

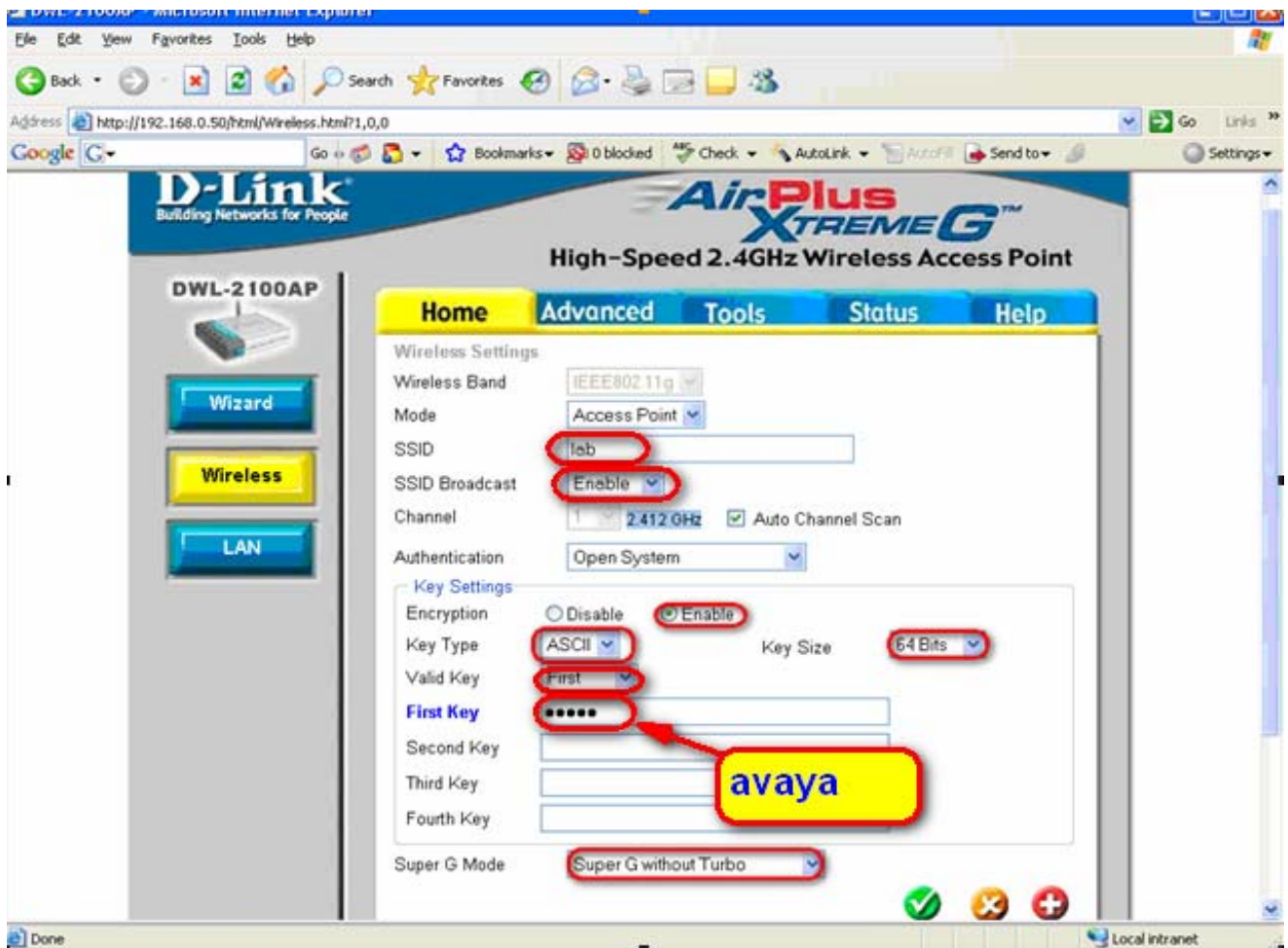
to indicate the use the “First” set of encryption key

First Key → avaya (only display dots)

Sample of the ascii key to use

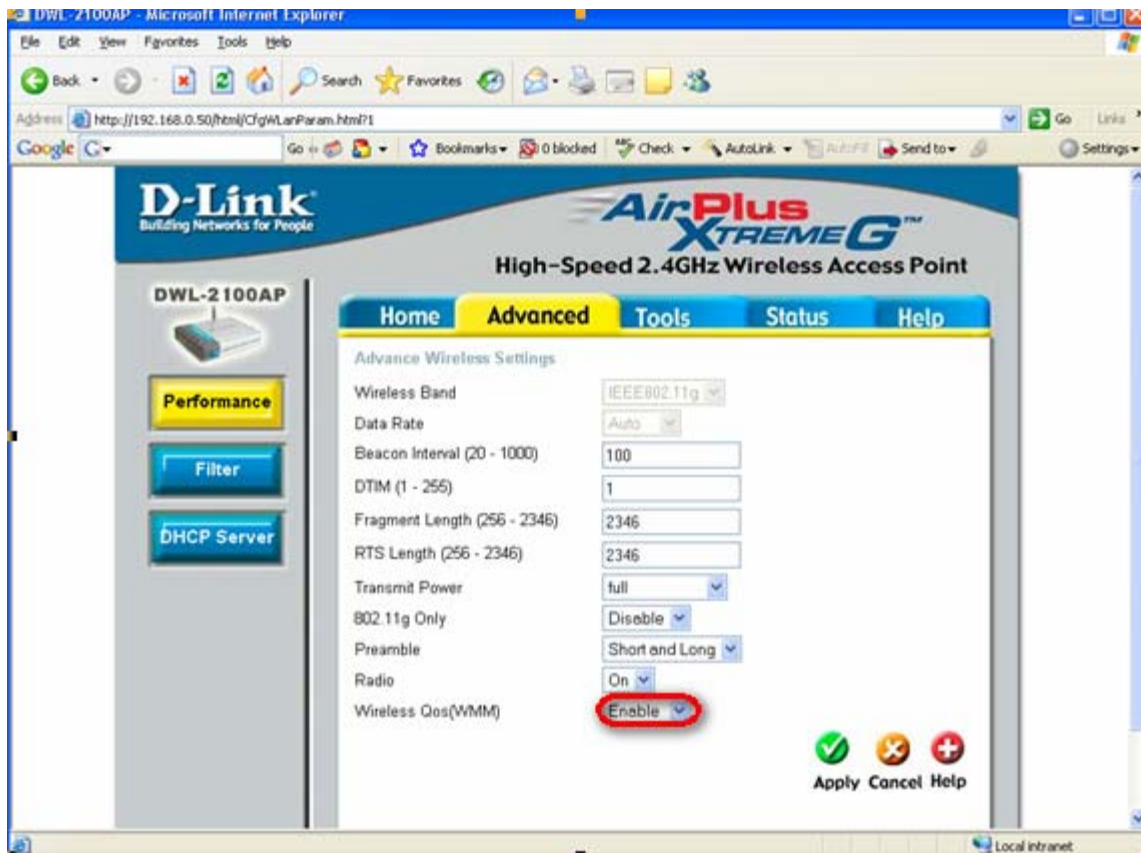
Super G Mode → Super G without Turbo

Scroll down and select “Apply” (not shown).



7. Select the “**Advanced**” tab followed by the **Performance** button in the left column. The following screen will display below.

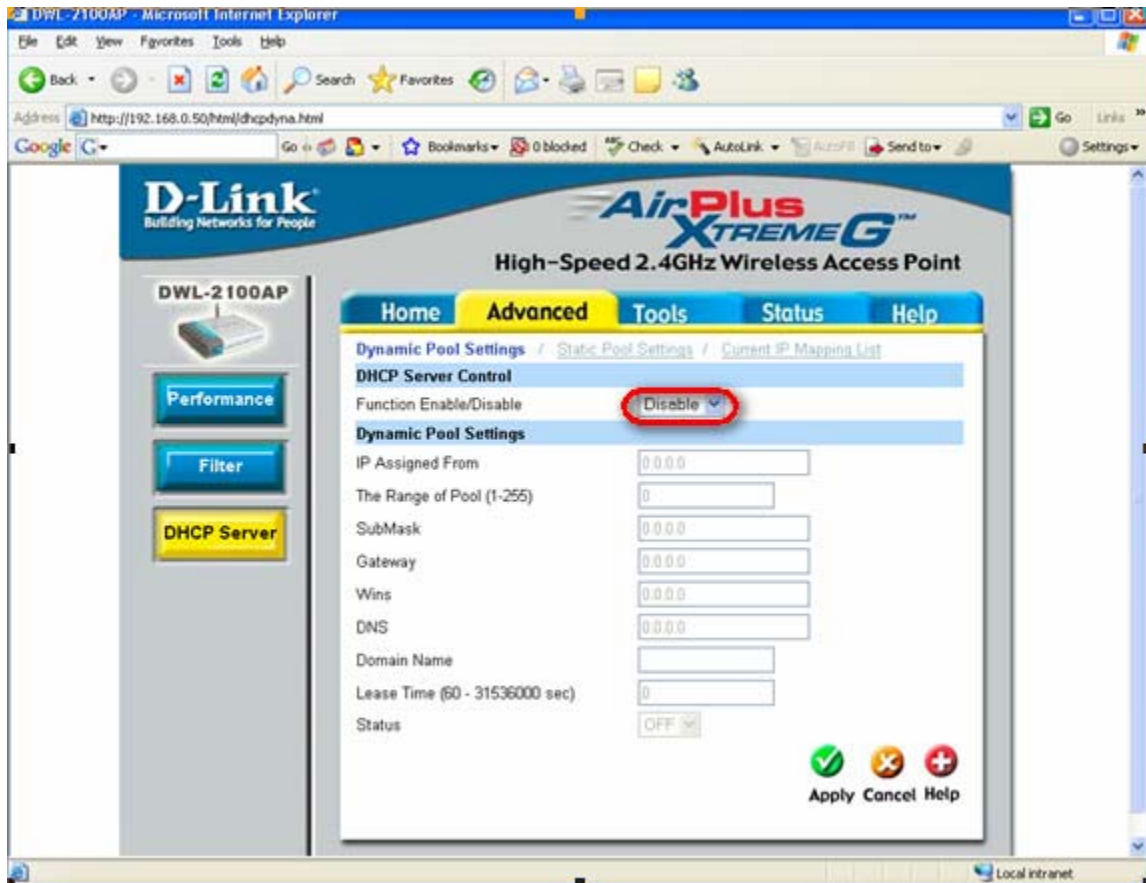
All fields should remain as the default value as shown below, except for **Wireless QoS** must be set to “**enable**” as shown below. WMM (Wi-Fi Multimedia) provides features that improve the user experience for audio, video and voice applications over a network. WMM is based on a subset of the IEEE 802.11e WLAN QoS draft standard. The default is "disable". This feature is recommended when using a wireless laptop and Avaya VPNremote Phone simultaneously to connect to the Access Point in order to provide voice quality thru the wireless network.



8. Select “**DHCP Server**” button on the left column of the screen:

Make sure the **DHCP Server Control Function** is set to “Disable”, since it will only provide as a pass-thru bridge for the wireless network as shown below.

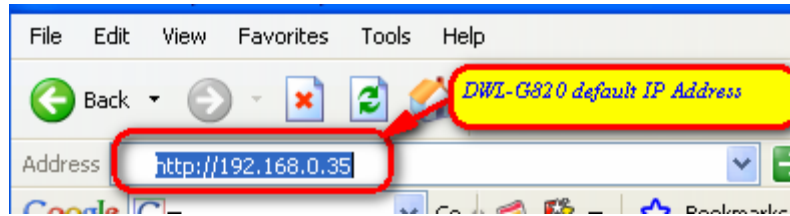
Select “**Apply**” to save the option.



4.2 Configure the D-Link DWL-G820 Extender / Gaming Adapter

This section shows the necessary steps in configuring the DWL-G820 Extender / Gaming Adapter shown in **Figure 1**. Follow steps 1-3 in section 4.1 to setup the computer to communicate with the DWL-G820.

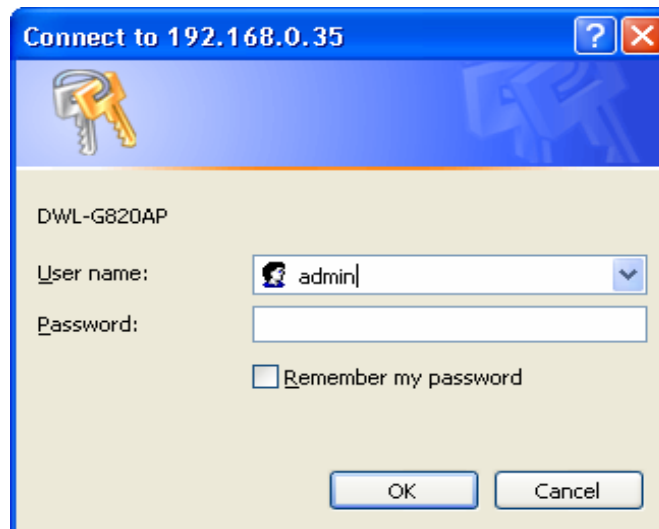
1. Open the web browser and enter the following URL using the DWL-G820 IP default address “http://192.168.0.35” and press **Enter**.



In the login screen that appears, use the following user name and password.

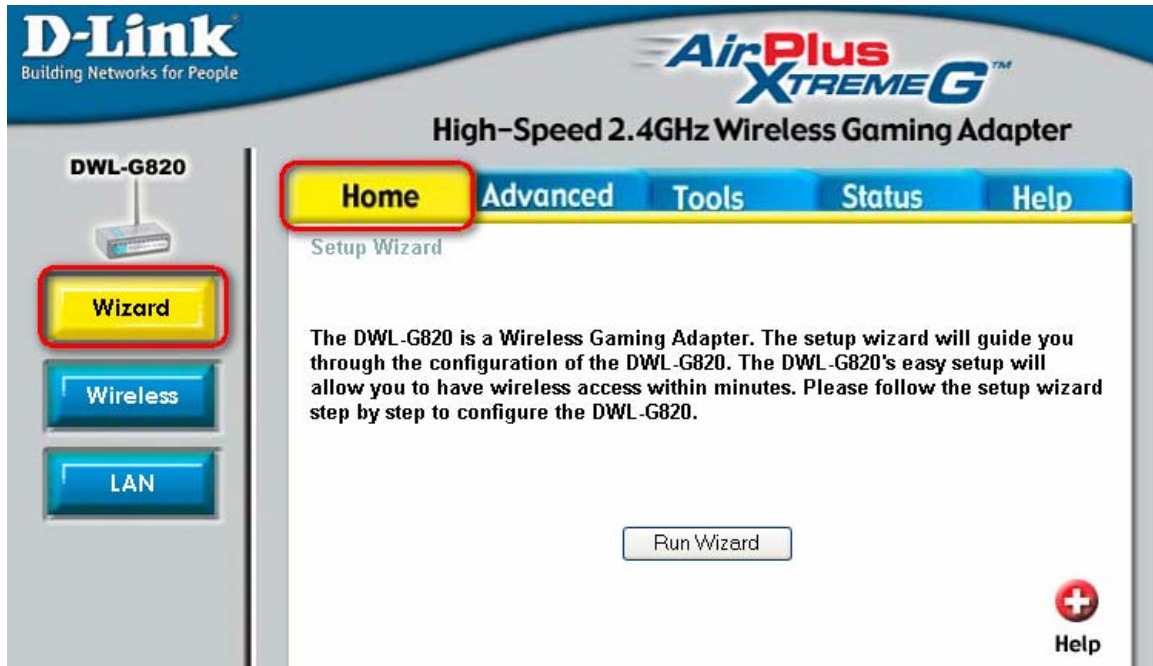
User name: admin

Password: (blank for default)



The DWL-G820 configuration home page is displayed below after successful login.

2. On the DWL-G820 home page, select the **Home** tab followed by the **Wireless** button in the left column.

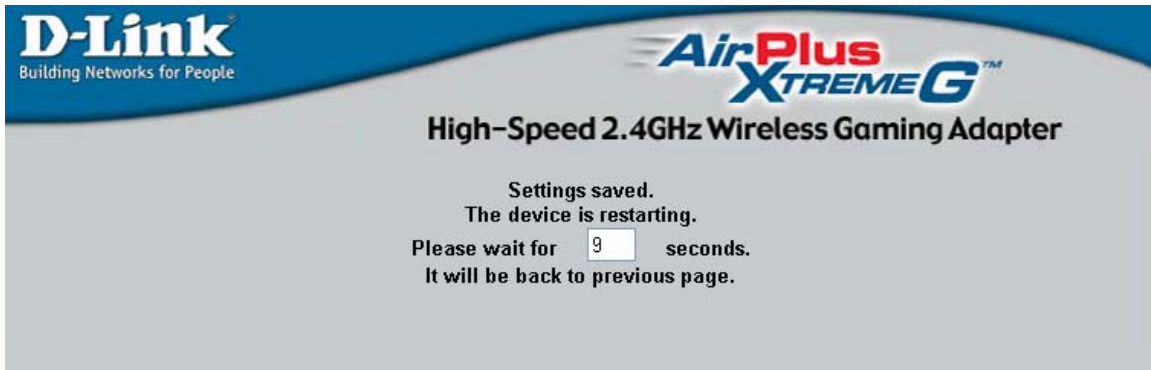


3 On the screen that appears, enter the values as shown below.

Change SSID → lab
Channel → 6 (Default)

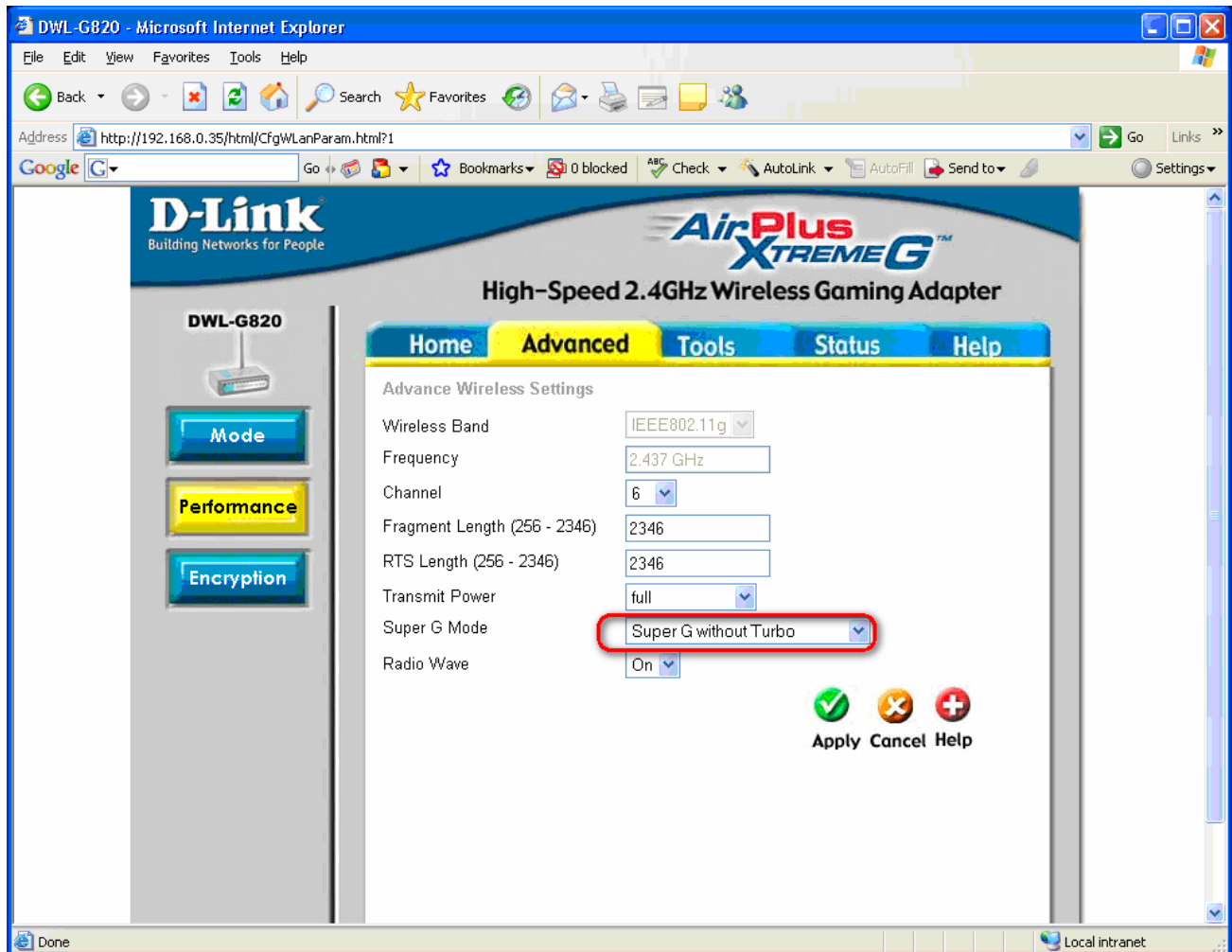


4. Select “Apply” to save the settings and the device will restart/reset as displayed below:



5. Select **Advanced** tab, followed by **Performance** button in left column.

Enable Super G Mode by selecting “**Super G without Turbo**” mode as shown below, all other fields are the default value.



Select “**Apply**” to save the configuration and the device will restart/reset:

6. Select **Advanced** tab followed by **Encryption** button in left column. On the screen that appears, enter the values as shown below.

Authentication → Open system

Encryption → Enable

Key Type → ASCII

Option to use either ASCII or HEX key type

Key Size → 64 bits

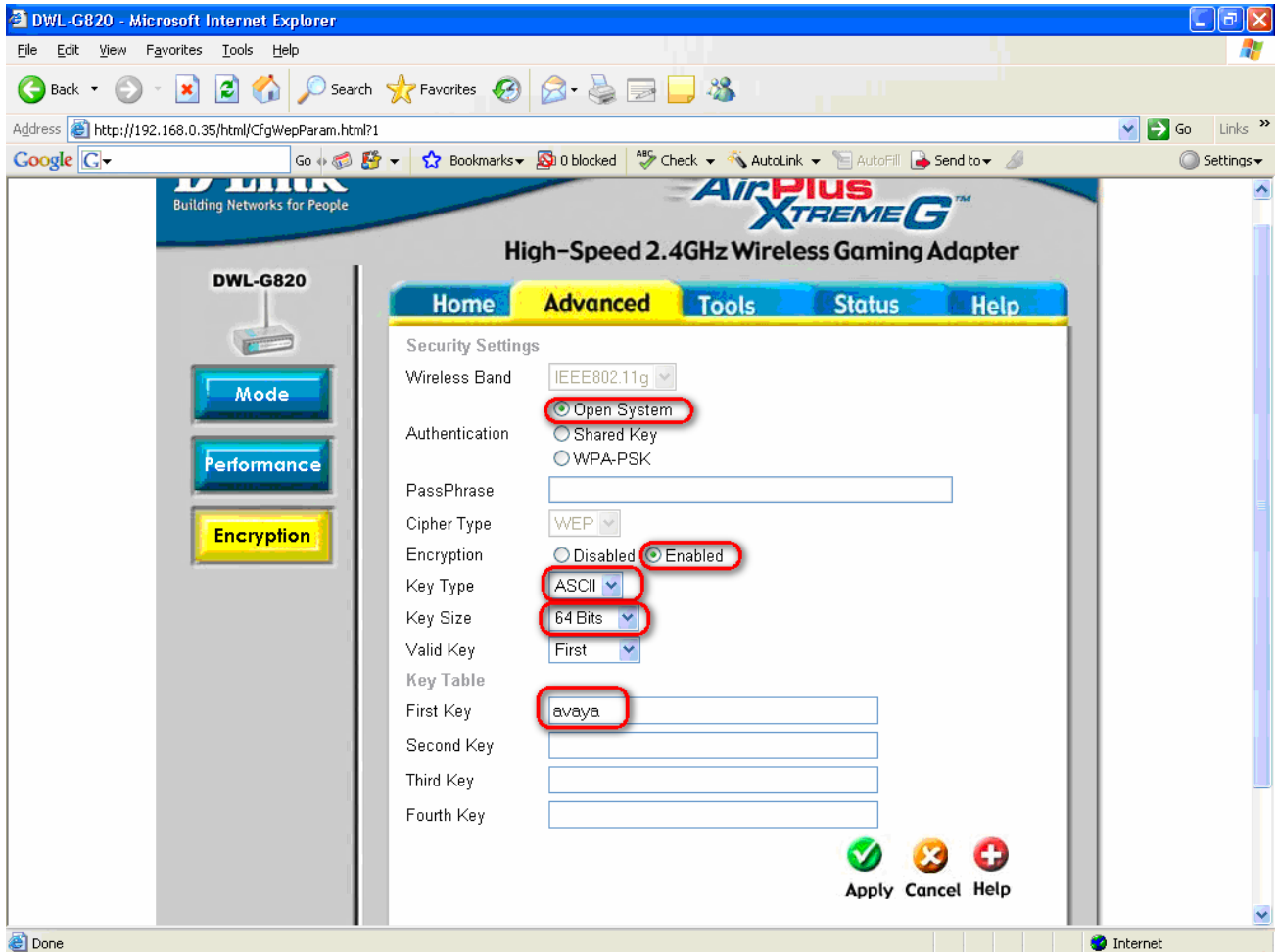
64 bits encryption key is only use for basic security demonstration setup for this application note.

Valid Key → First

to indicate the use the “First” set of encryption key

First Key → avaya (only display dots)

Sample of the ascii key to use



Select “**Apply**” to save the configuration and the DWL-G820 will reset as shown below:



5. Verification Steps

The following steps may be used to verify the configuration:

- Avaya VPNremote Phone should successfully register with Avaya Communication Manager.
- Validate dial tone on Avaya VPNremote Phone
- Place inter-site calls

6. Conclusion

These Application Notes describe the configuration steps required to configure the D-Link Access Point and Extender Adapter to support the Avaya VPNremote Phone. All feature functionality of the VPNremote Phone over the wireless 802.11b/g with respect to registration, connection and user experience is the same as using the wireline connection. The D-Link successfully achieved enabling the Avaya VPNremote Phone to function in a wireless environment. The Avaya VPNremote Phone successfully received appropriate IP addresses from the Avaya DHCP server and completed the registration with the Avaya Communication Manager. However, it is recommended that when it is configured in a public area/domain, assign a secure login password to the devices and enable the highest level of encryption.

6.1 Observation

The D-Link DWL-G820 is limited to one device. Connecting additional devices using a hub/switch off the DWL-G820, or connecting another computer thru the Avaya VPNremote Phone will not work. When switching between devices the DWL-G820 must be reset (power “off” and “on”).

The drawback of the wireless network is that the QoS (Quality of Service) and security are not guaranteed and if there is any interference (i.e., cordless 2.4MHz phone) with the link then the connection may be dropped.

6.2 General Security Tips

- When away from the WiFi network, disable Microsoft File and Printer sharing on your laptop (which enables other computers to access resources on your computer) so as not to leave your computer vulnerable to hackers.
- Use the highest level of encryption available between the two wireless devices.
- If the interference from other Wireless Access Points or wireless devices in the area is a concern, set the AP and wireless clients to use a non-overlapping channel such as 1, 6 or 11.
- Change the configuration interface password of the access point before enabling it. Most people overlook this part of setting up a wireless network.
- Only buy an access point that has upgradeable firmware. This will allow you to take advantage of security enhancements or interface updates.
- Keep the access point firmware up to date. Upgrade your firmware whenever a new one is available. It will probably contain a new or improved feature.

Notes:

Hardware vendors, such as Linksys and D-Link have also announced the use of MIMO (Multiple-In-Multiple-Out) in their products. MIMO allows the signal to be bounced off several antennas and paths so that data delivery is guaranteed. Basically, many unique data streams are passed in the same frequency channel. It is a technology that allows for the boosting of wireless bandwidth and range, effectively providing better performance for wireless multimedia and entertainment systems.

D-Link recommends that the DWL-G820 is used with D-Link AirPlus Xtreme G products to gain maximum wireless signal rate derived from IEEE Standard 802.11g specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead lower actual data throughput rate.

7. Additional References

- Product documentation for Avaya products may be found at <http://support.avaya.com>
- Product documentation for D-Link products may be found at <http://www.dlink.com> and their support hotline (877) 453-5465

©2006 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com.