The SQUNet Wireless Local Area Network FAQ

Welcome to the SQUNet Wireless Local Area Networking (Wi-Fi) Service. This Frequently Asked Questions (FAQ) text is designed to answer the majority of the questions that you may have about our service. If you need more help please contact us.

1. **What is SQUNet Wi-Fi?**
2. **Where is service available?**
3. **Can I use wireless services outside of the coverage areas?**
4. **Can I do everything with a wireless connection that I could do with a wired network connection?**
5. **What does 802.11 mean?**
6. **Can I expect same data transfer rate as shown in my connection speed?**
7. **Can I use a PDA or Pocket PC to access the wireless network?**
8. **Is it true that a wireless connection disrupted more often than a wired network connection?**
9. **What level of security will the University Computing offer for my wireless connection?**
10. **Does wireless interfere with my cell phone?**
11. **Where can I get more help?**

1. **What is SQUNet Wi-Fi?**

SQUNet Wi-Fi is an enhancement to the local area network service at the Sultan Qaboos University. It is designed to complement and extend the existing on-campus wired network, providing support in areas where it is impractical to provide wired networking.

SQUNet Wi-Fi is standards compliant, supporting IEEE 802.11g wireless networking, as well as providing limited backwards compatibility with the older (and slower) IEEE 802.11b standard. SQUNet Wi-Fi does not support IEEE 802.11a.

The SQU has implemented Wi-Fi using a technology built on thin client access points. **Unlike the fat access clients often used in home environments the SQU’s devices will only work when used in a network environment that includes a special Security/Management controller.**

The SQU's Security/Management controller, located in the CIS, gives the University many capabilities not usually found in more basic Wi-Fi environments. For example it enables the SQU to continually monitor the operation of the SQUNet Wi-Fi service centrally. Using this capability we can detect whether access points distributed around campus are properly operational, we can also detect the attachment of unauthorised Wi-Fi devices.
2. **Where is service available?**
Service is available at designated hot spots on-campus only, the diagram below summarises the coverage.

(Consider making this a clickable diagram, alternatively include a table based on the actual installation as done, since this does differs in some areas of details in comparison to the original plan.)

3. **Can I use wireless services outside of the coverage areas?**
The CIS has carefully designed the present network to provide service in specific locations. Since wireless transmissions may "spill over" into areas where service was not planned you may get service in other locations also. Since, for technical reasons, the CIS may need to relocate equipment from time to time we cannot guarantee continued service availability in these "spill over" areas.
4. **Can I do everything with a wireless connection that I could do with a wired network connection?**
Theoretically you should be able to do exactly the same things using a Wi-Fi connection as you can with a wired connection. However, for practical reasons, you will be subject to some restrictions in respect of your Wi-Fi usage. Restriction may include:

- Barred access to certain on-campus resources based on your need and entitlement. For example students will not be permitted access to resources designated as being for adminstrativer personnel.
- Barred access to certain high bandwidth applications.
- Barred access to certain resources based on security considerations.

Access restrictions will be maintained under continuous review, and may be changed as required to ensure the best service for the entire campus community.

5. **What is IEEE 802.11?**
IEEE 802.11 is a set of standards developed by the Institute of Electrical and Electronic Engineers (IEEE). It covers a wide variety of services and facilities made available under the original wireless specifications, these services and facilities extend and complement the basic standard. Different components of the IEEE 802.11 standards are designated by the application of a suffix letter, for example:

<table>
<thead>
<tr>
<th>802.11</th>
<th>The basic standard provides up to 2 Mbps transmission in the 2.4 GHz band.</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a</td>
<td>Provides up to 54 Mbps transmission in the 5 GHz band.</td>
</tr>
<tr>
<td>802.11b</td>
<td>Provides up to 11 Mbps transmission in the 2.4 GHz band.</td>
</tr>
<tr>
<td>802.11g</td>
<td>Provides up to 54 Mbps transmission in the 2.4 GHz band.</td>
</tr>
</tbody>
</table>

6. **Can I expect the data transfer rate shown in my connection speed?**
The 802.11 wireless standards allows for specific theoretical maximum connection speeds (54 Mbps for 802.11g, 11 Mbps for 802.11b). However under no circumstances are you likely to receive this theoretical maximum data rate. This is because:

- Administrative data exchanges take place between your equipment and the wireless access point (AP), these can use up to 40% of the raw connection speed.
- Your data transfer rate will drop as more people connect to your access point (the data rate is per access point, not per user).
- The amount and type of user activity can affect your connection speed.
- Signal conditions, a poor signal will cause the data rate to be reduced to ensure reliable communication. Typically this would happen if you are a long way from the access point, there are obstructions in the signal path, or there is interference from other electronic devices.
7. **Can I use a PDA or Pocket PC to access the wireless network?**
   You can use any device provided it supports the IEEE protocols used by SQU (IEEE 802.11g preferred, IEEE 802.11b otherwise), as well as the authentication and encryption mechanisms applied for SQUNET Wi-FI security.

8. **Is it true that a wireless connection can be disrupted more often than a wired network connection?**
   The quality of your wireless network connection will depend upon signal conditions. Many factors can affect wireless connections (walls, desks, large metal objects, etc.). A major source of disruption is devices operating in the same 2.4 GHz frequency range. Probably the largest offender in this respect in microwave ovens, however certain other devices may use this transmission frequency also. Wired networks, of course, do not usually suffer such disruption since they are designed to be resistant to electrical interference. (Note: GSM telephones do not use the 2.4 Ghz frequency range, so should not cause any problems.)

9. **What level of security will the University Computing offer for my wireless connection?**
   This CIS intends to implement a good standard of security by using two processes:
   - Access to the SQUNET Wi-FI LAN will be controlled through an identification and authentication. The intent is to ensure that only authorised users can access the Wi-Fi LAN.
   - Encryption will be used to ensure that data being transmitted is being sent as encrypted not plain text. The intention is to ensure that should access be obtained directly to data packets, the content will not be revealed (as it would be if sent as plain text).
   Notwithstanding these precautions you should note that there are always risks in transmitting confidential information over networks. Consequently the University can assume no responsibility for any loss of data or the compromise of private information such as passwords, credit card information, registration data, and so forth.

10. **Does wireless interfere with my cell phone?**
    GSM telephones use a completely different transmission frequency to the SQUNET Wi-Fi LAN service. There is minimal likelihood of interference between the two.

11. **Where can I get more help?**
    Please contact University Centre for Information Systems (CIS) Help Desk at ext: 2888 for inquiries or Email helpdesk@squ.edu.om.

For more information about this service, please visit [www.squ.edu.om/cis](http://www.squ.edu.om/cis).