Uttlesford District Council

Wireless Network Security Policy Review

V0.1 Initial Draft Document

Amendments

Prepared by: Rob Glover, Alun Harrison & Steve Smith
Date: 26 January 2007

Astro Communications Ltd
Astro House, 41 High Street, Swanley, Kent, BR8 8AE
Tel: 01322 610100 Fax: 01322 610101
Web: www.astro.co.uk & www.classhawk.co.uk

Contents

Astro Communications Ltd
Astro House, 41 High Street, Swanley, Kent, BR8 8AE
Tel: 01322 610100 Fax: 01322 610101
Web: www.astro.co.uk & www.classhawk.co.uk

astro COMMUNICATIONS LTD
CONNECTIVITY WITH BUSINESS EFFICIENCY

Introduction

This report details Astro Communications' findings and recommendations in relation to wireless network provision at Uttlesford District Council offices.

The report details the following:

- **Wireless Audit** – determines the initial wireless activity and equipment in the vicinity of Uttlesford District Council offices and checks for potential overspill from Uttlesford District Council's own wireless network into public areas surrounding the building.

- **Wi-Fi Policy** – recommends a wireless policy and ensures that it conforms to current best practice for deploying wireless networks in this particular scenario.

- **Wireless Recommendations** – for a future wireless networking strategy. This will take into consideration current data only requirements and potential future requirements for Voice over IP over Wireless LAN (VoWLAN).

Wireless Audit - General

The wireless audit provides a 'snap shot' of Uttlesford District Council's own wireless network devices and other domestic and commercial wireless networks in the surrounding area.

The tables in each floor section below show all of the Access Points seen during the survey and specifically details:

- SSID - where it has not been suppressed
- MAC address of Access Point
- The 802.11 standard being used for radio access
- The 802.11 channel number
- If privacy is being used

The tables highlight the need for suppressed SSIDs and for not using meaningful character strings in the SSID to indicate the identify the organisation associated with the wireless network.

We can also see that the most used channels are 1, 6 and 11. This ties in fairly well with FCC standards (USA) which state that non-overlapping channels for FCC are 1, 6 & 11. In Europe, the standard is ETSI, which uses 1, 7 & 13 as their non-overlapping channels.

A look up of the first 6 hexadecimal digits of the MAC address can identify the manufacturer of the access point. Someone who wants to compromise a system could check the first half of the MAC address to determine the manufacturer. They can then identify any weaknesses such as software bugs in their access points and exploit this vulnerability. It is important to monitor software and firmware developments from the manufacturer of your access points to ensure the risks of weaknesses and vulnerabilities are reduced by upgrading when necessary or by implementing configuration 'work arounds' as advised by the manufacturer.

There are a number of Uttlesford District Council Access Points showing up in the tables but our test results show sporadic cover across the floors from the existing Access Points. This is mainly due to the lack of design in the implementation – for example, APs sited on top of equipment cabinets.

Limitations

The survey software will identify the security method as WEP for any encrypted network. It is not possible at this time for the software to identify the exact encryption method as this could potentially be a security infringement. The Access points that are identified as Uttlesford District Council AP's have been manually identified as running WPA encryption.

Where the AP and channels identified by the survey software have a blank SSID, this indicates the SSID beacon is not broadcast in the beacon frame, therefore, it is impossible to identify the network with the tools used in this survey.

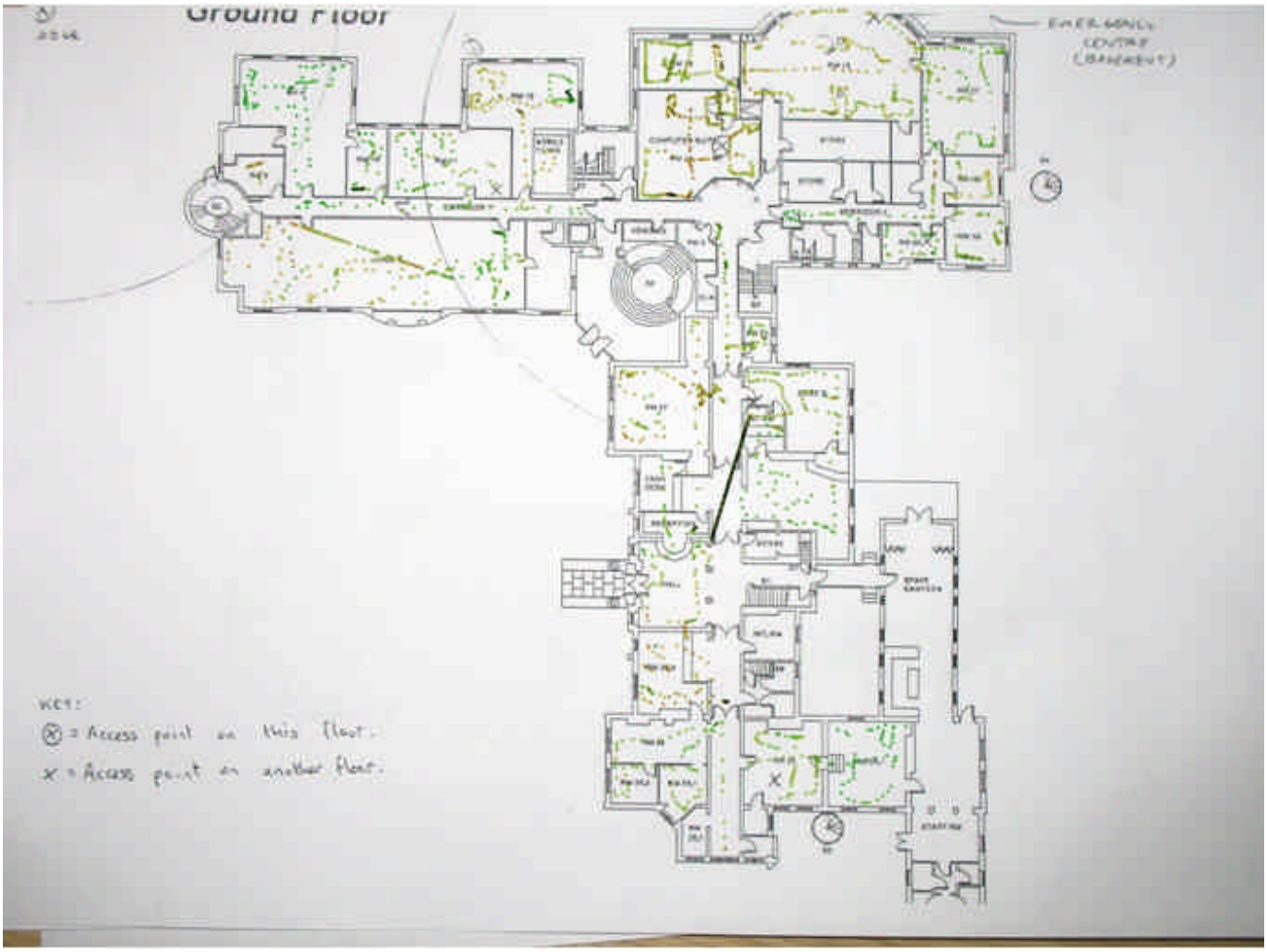
As with any wireless installation, our test results relate to the hardware and software client in our test PCs. Other PCs may get slightly different results.

Wireless Audit - Ground Floor

Access Points identified...

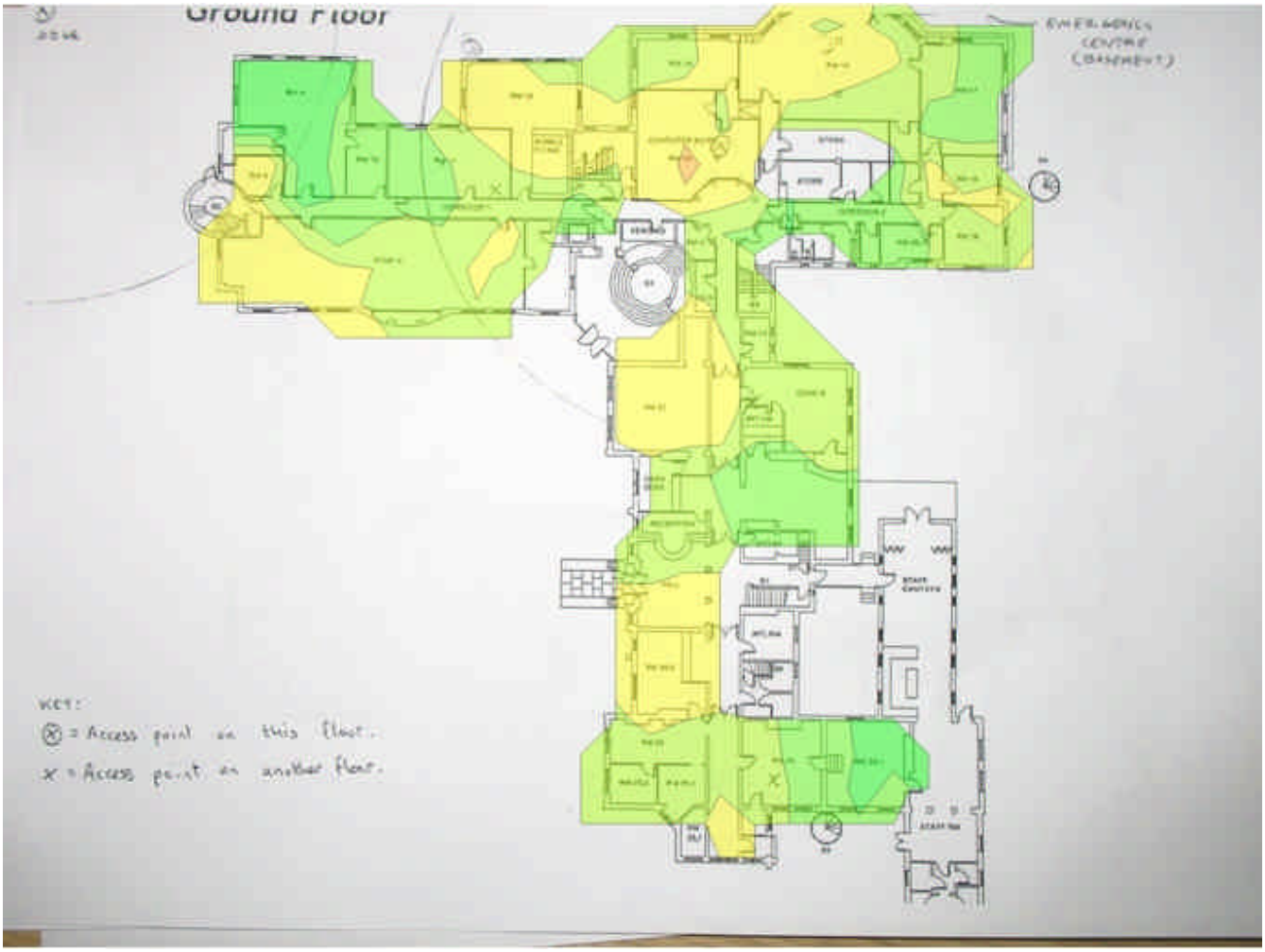
ESSID	Name	Band / Channel	Privacy
	00:0F:90:3A:28:90	802.11g / 13	WEP
BTHomeHub-F49D	00:14:7F:60:E1:18	802.11g / 6	WEP
GSMITH	00:0F:B5:5F:F2:C4	802.11g / 11	WEP
Home	00:14:85:BE:AF:36	802.11g / 6	WEP
MSHOME	00:40:F4:F4:2F:7B	802.11g / 6	WEP
UDCBB01	00:0F:B5:36:79:F8	802.11g / 5	WEP
UttlesfordDC	00:0F:B5:36:5D:DF	802.11g / 11	WEP
UttlesfordDC	00:0F:B5:36:7A:48	802.11g / 11	WEP
UttlesfordDC	00:0F:B5:3B:BB:B2	802.11g / 11	WEP
UttlesfordDC	00:14:6C:38:DB:11	802.11g / 11	WEP
UttlesfordDC	00:0F:B5:36:7A:85	802.11g / 11	WEP
UttlesfordDC	00:0F:CB:B4:47:B1	802.11g / 11	WEP
UttlesfordDC	00:0F:B5:36:79:33	802.11g / 1	WEP
cook	00:0F:90:3A:28:90	802.11g / 13	WEP

Sample Points and Access Point Locations



Astro Communications Ltd
Astro House, 41 High Street, Swanley, Kent, BR8 8AE
Tel: 01322 610100 Fax: 01322 610101
Web: www.astro.co.uk & www.classhawk.co.uk

Signal Strength…



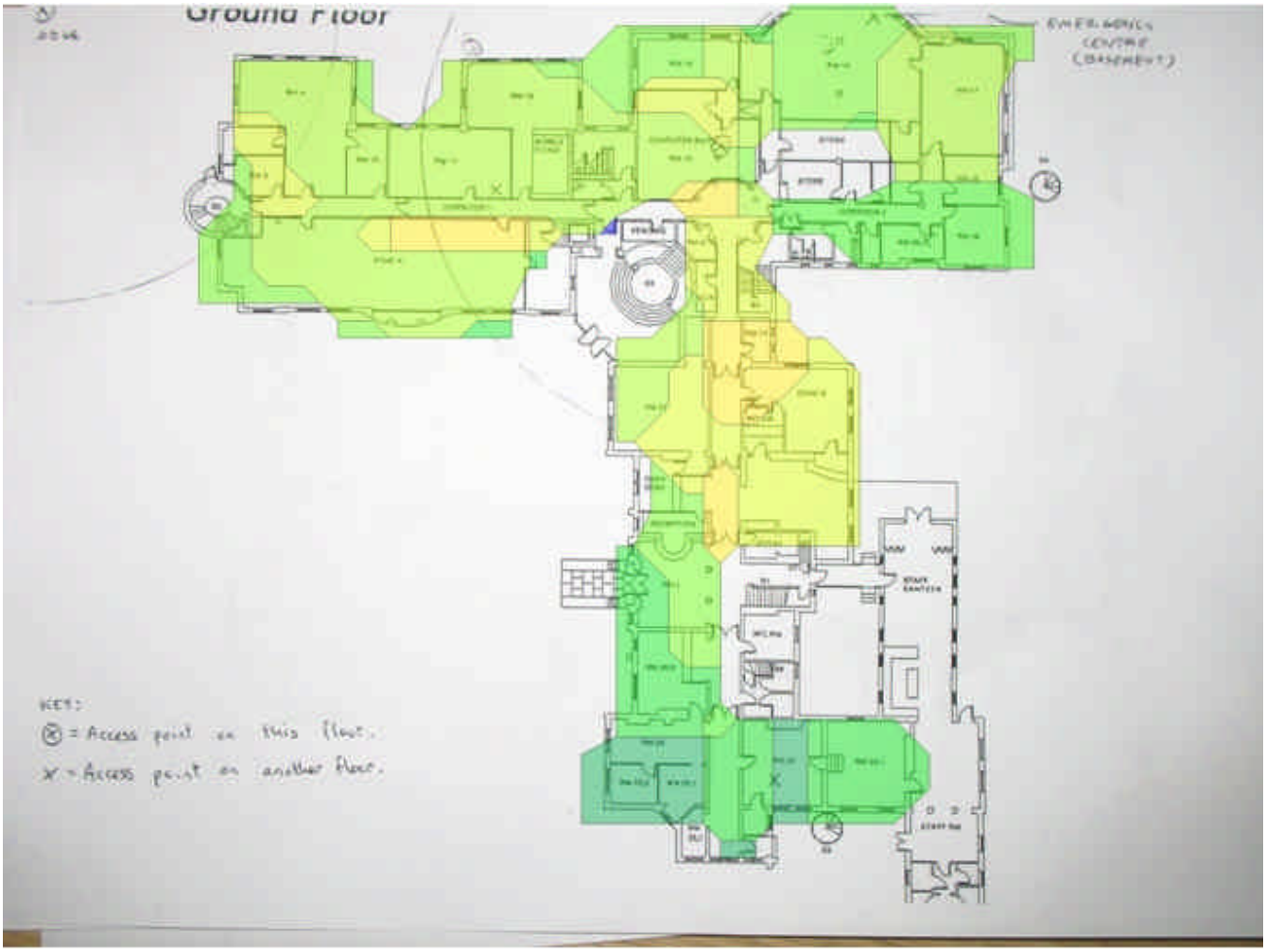
Signal Strength coverage (RSSI) of the selected access points. The strongest RSSI is shown per location.

-100.0..-90.0	-90.0..-80.0	-80.0..-70.0	-70.0..-60.0	-60.0..-50.0
-50.0..-40.0	-40.0..-30.0	-30.0..-20.0	-20.0..-10.0	-10.0..0.0

The signal strength is dictated by the transmitting power of the access point, the type of antenna used, the materials of physical obstructions in the transmission path and other environmental conditions.

The radio foot print can be controlled by adjusting the power output of the access point and the shape of the foot print can be controlled by using different types of antenna. Omni directional antennas tend to propagate radio waves in a circular fashion in all directions and directional antennas can be used to propagate a beam in a particular area. The antenna can also provide additional signal gain or attenuation

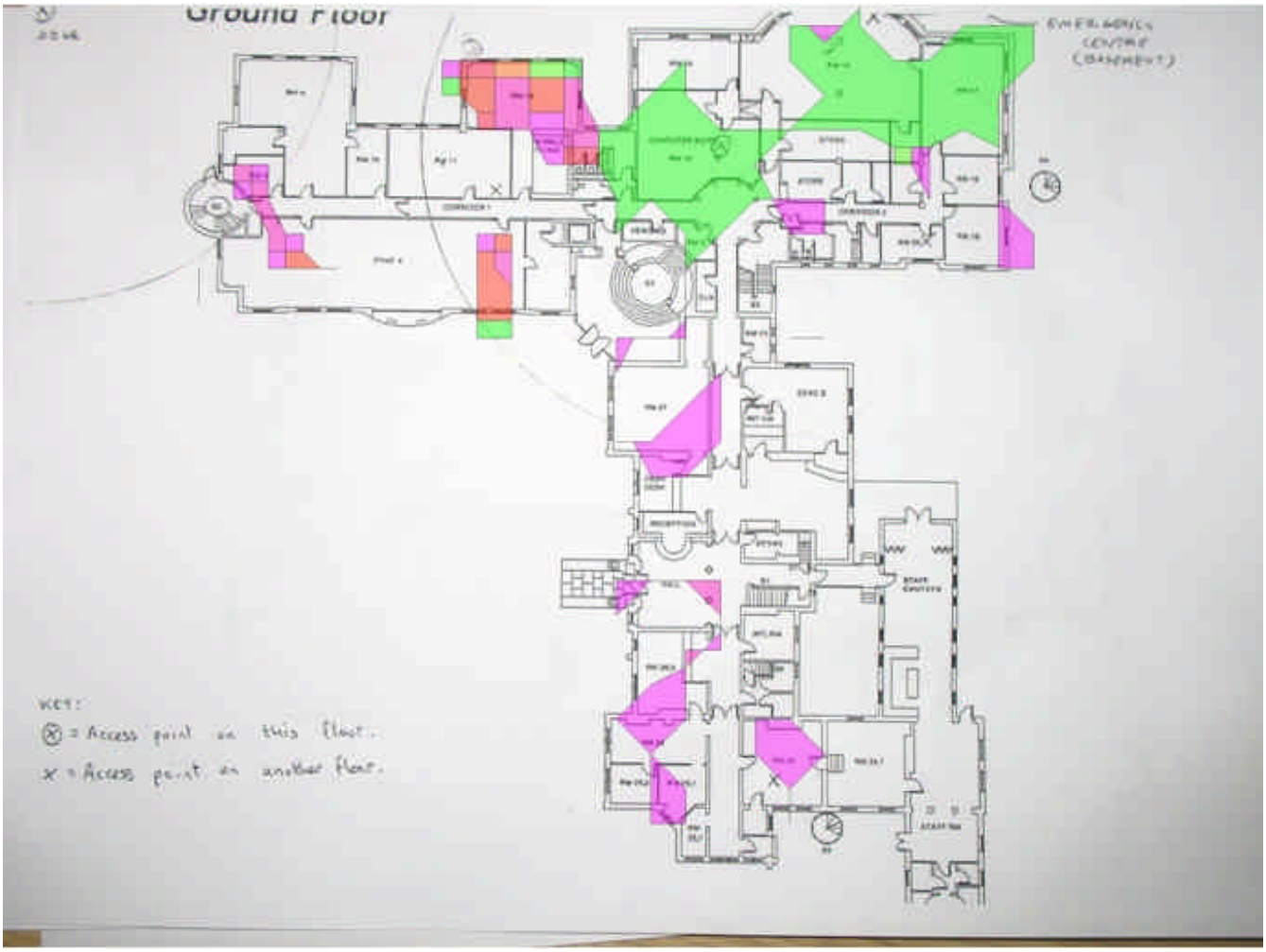
Access Point Count



Displays the number of audible access points per location with respect to the selected minimum RSSI requirement.

1	2	3	4	5	6	7
8	9	10	11	12	13	14

Data Rate



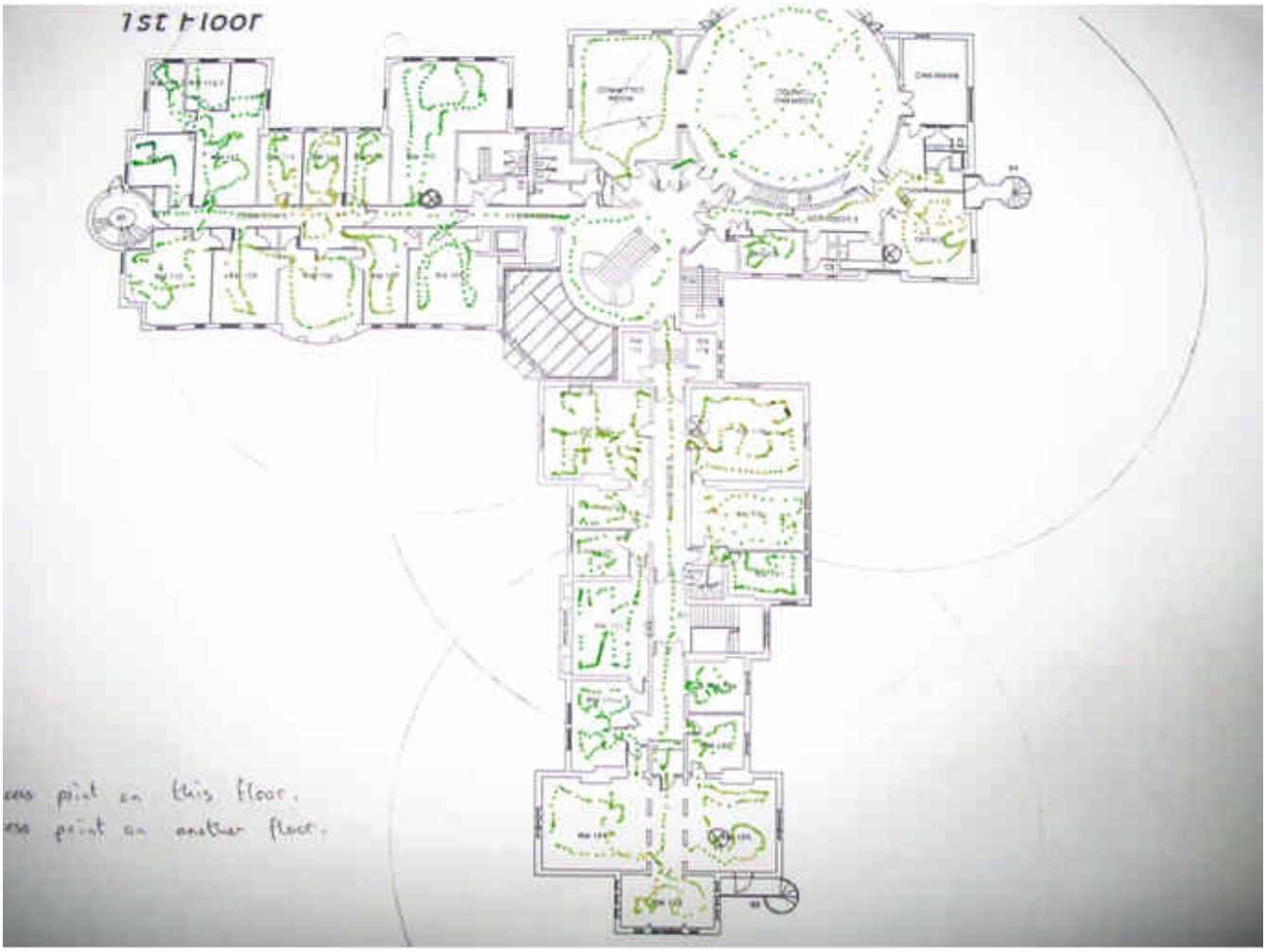
Astro Communications Ltd
Astro House, 41 High Street, Swanley, Kent, BR8 8AE
Tel: 01322 610100 Fax: 01322 610101
Web: www.astro.co.uk & www.classhawk.co.uk

Wireless Audit - First Floor

Access Points identified...

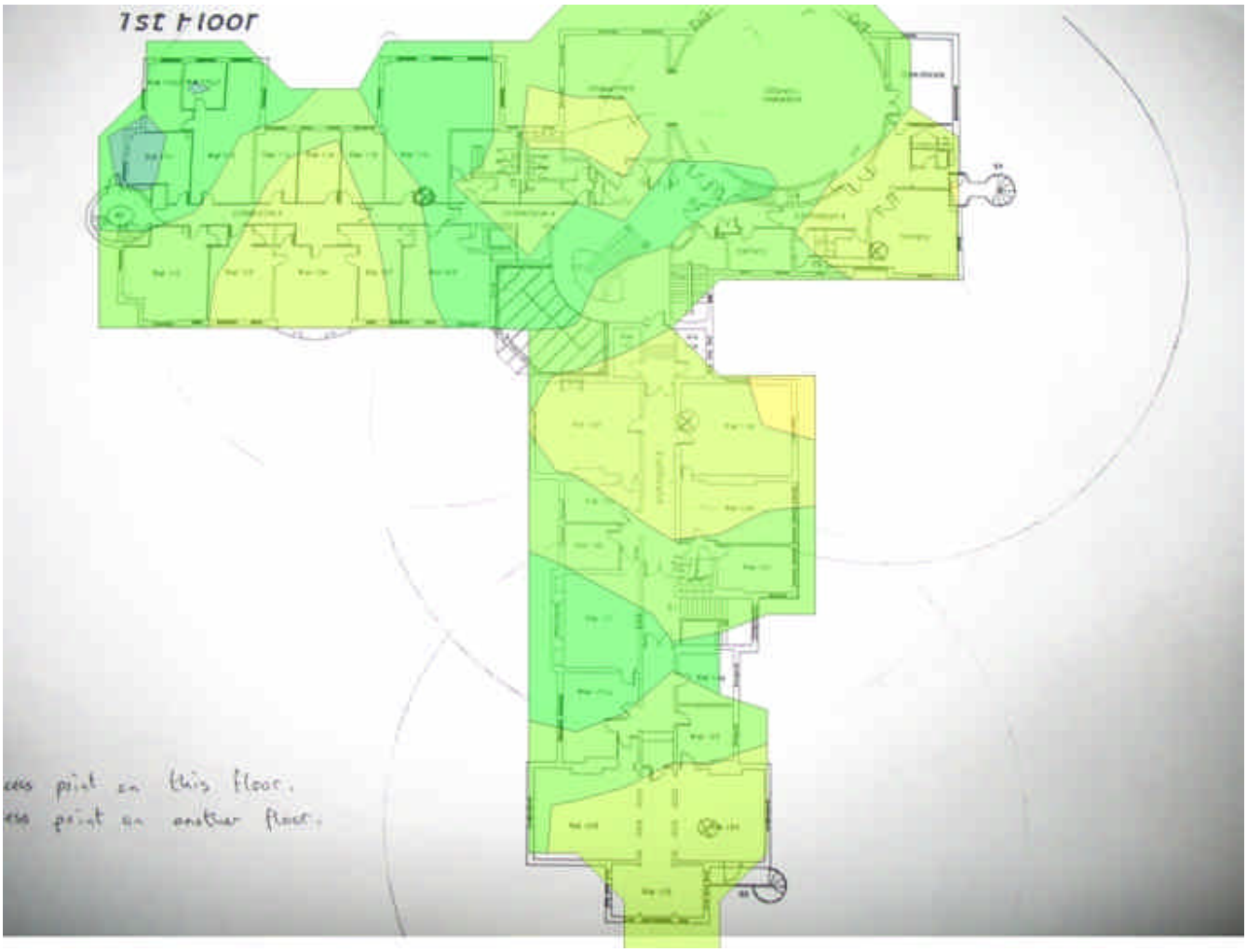
ESSID	Name	Band / Channel	Privacy
Antbits	00:14:6C:78:2B:50	802.11g / 11	WEP
BTHomeHub-F49D	00:14:7F:60:E1:18	802.11g / 6	WEP
Belkin_G_Plus_MIMO_20BD73	00:17:3F:20:BD:73	802.11g / 6	
GSMITH	00:0F:B5:5F:F2:C4	802.11g / 11	WEP
Home	00:14:85:BE:AF:36	802.11g / 6	WEP
ITISO	00:09:5B:88:B4:64	802.11g / 11	
UDCBB01	00:0F:B5:36:79:F8	802.11g / 5	WEP
UttlesfordDC	00:0F:B5:36:7A:85	802.11g / 11	WEP
UttlesfordDC	00:0F:CB:B4:47:B1	802.11g / 11	WEP
UttlesfordDC	00:0F:B5:3B:BB:B2	802.11g / 11	WEP
UttlesfordDC	00:0F:B5:36:7A:48	802.11g / 11	WEP
UttlesfordDC	00:0F:B5:36:5D:DF	802.11g / 11	WEP
UttlesfordDC	00:0F:B5:36:79:33	802.11g / 1	WEP
UttlesfordDC	00:14:6C:38:DB:11	802.11g / 11	WEP
WANADOO-6B38	00:16:CE:26:91:F8	802.11g / 1	WEP
WLAN	00:30:BD:67:09:6B	802.11b / 1	WEP
osbourn	00:11:50:61:7D:2B	802.11g / 11	WEP

Sample Points and Access Point Locations



Astro Communications Ltd
Astro House, 41 High Street, Swanley, Kent, BR8 8AE
Tel: 01322 610100 Fax: 01322 610101
Web: www.astro.co.uk & www.classhawk.co.uk

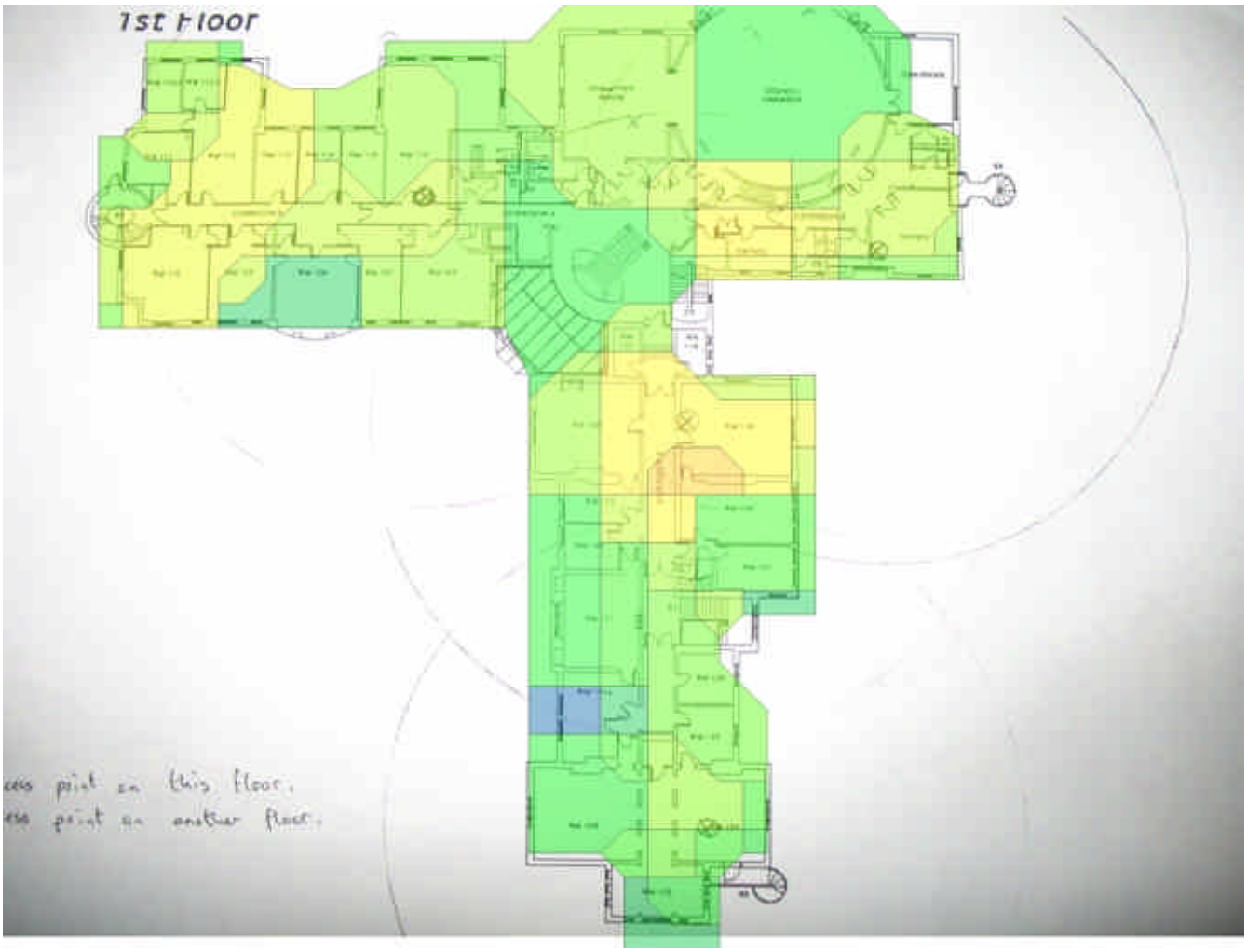
Signal Strength



Signal Strength coverage (RSSI) of the selected access points. The strongest RSSI is shown per location.

-100.0..-90.0	-90.0..-80.0	-80.0..-70.0	-70.0..-60.0	-60.0..-50.0
-50.0..-40.0	-40.0..-30.0	-30.0..-20.0	-20.0..-10.0	-10.0..0.0

Access Point Count

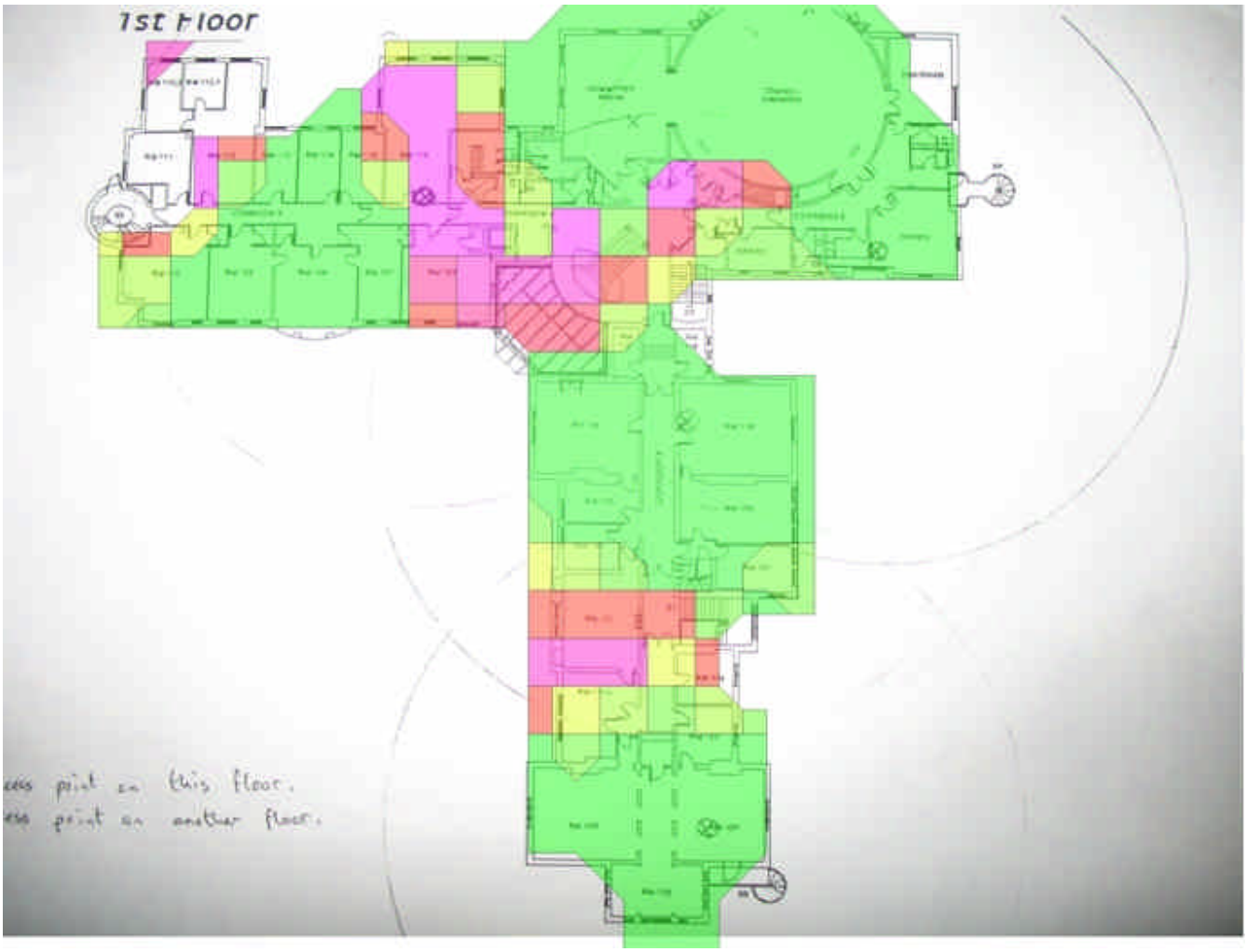


Displays the number of audible access points per location with respect to the selected minimum RSSI requirement.

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	

Astro Communications Ltd
Astro House, 41 High Street, Swanley, Kent, BR8 8AE
Tel: 01322 610100 Fax: 01322 610101
Web: www.astro.co.uk & www.classhawk.co.uk

Data Rate



An estimate of maximum data rate per location, with respect to the selected Signal-To-Noise threshold and the selected wireless network card receiver sensitivity values

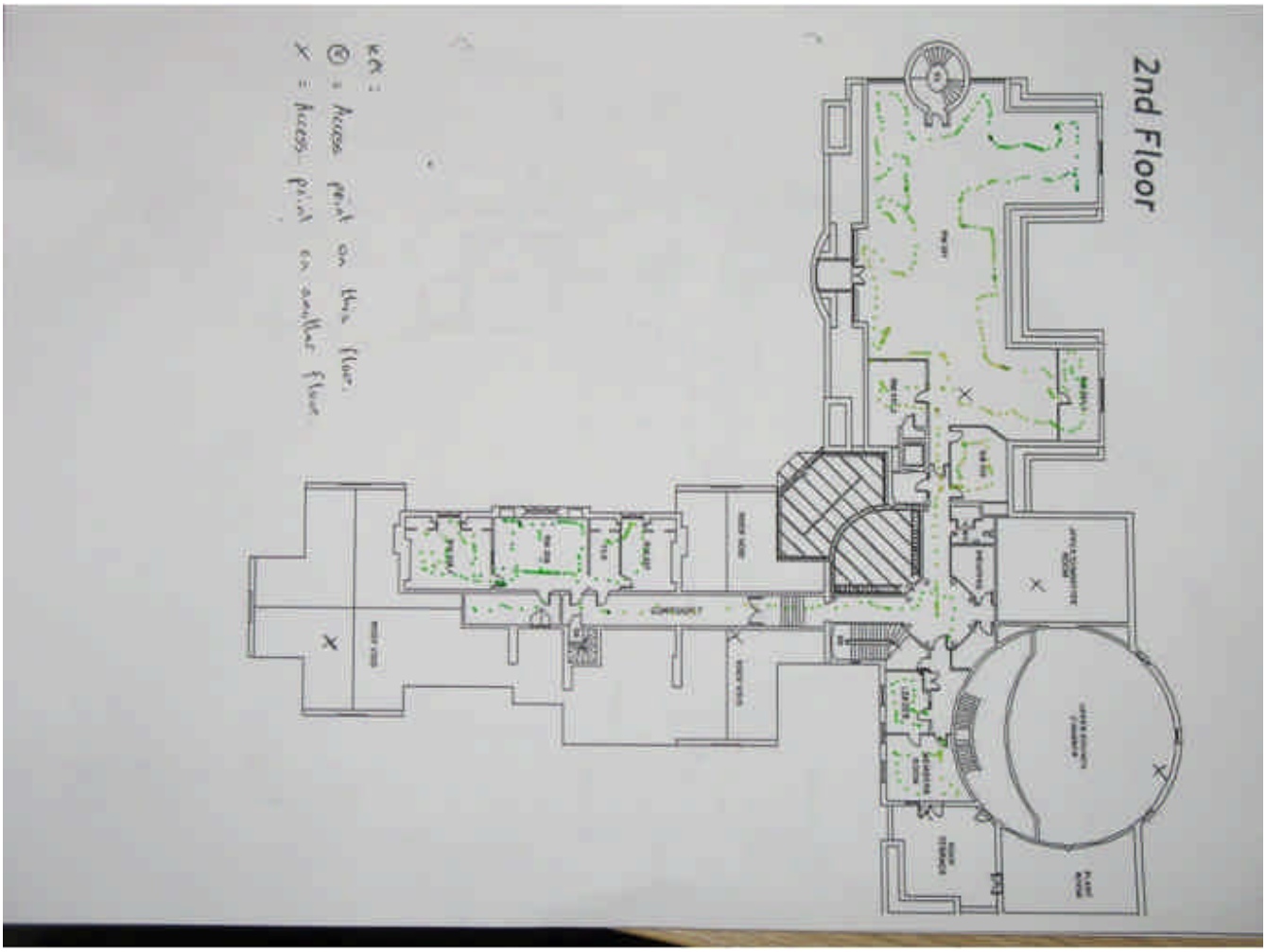
1.0	2.0	5.5	6.0	9.0	11.0
12.0	18.0	24.0	36.0	48.0	54.0

Wireless Audit - Second Floor

Access Points identified...

ESSID	Name	Band / Channel	Privacy
BTHomeHub-F49D	00:14:7F:60:E1:18	802.11g / 6	WEP
Belkin_G_Plus_MIMO_20BD73	00:17:3F:20:BD:73	802.11g / 6	
Home	00:14:85:BE:AF:36	802.11g / 6	WEP
ITISO	00:09:5B:88:B4:64	802.11g / 11	
UDCBB01	00:0F:B5:36:79:F8	802.11g / 5	WEP
UttlesfordDC	00:0F:B5:36:7A:85	802.11g / 11	WEP
UttlesfordDC	00:0F:B5:3B:BB:B2	802.11g / 11	WEP
UttlesfordDC	00:14:6C:38:DB:11	802.11g / 11	WEP
UttlesfordDC	00:0F:CB:B4:47:B1	802.11g / 11	WEP
UttlesfordDC	00:0F:B5:36:79:33	802.11g / 1	WEP
UttlesfordDC	00:0F:B5:36:7A:48	802.11g / 11	WEP
UttlesfordDC	00:0F:B5:36:5D:DF	802.11g / 11	WEP

Sample Points and Access Point Locations



Astro Communications Ltd
Astro House, 41 High Street, Swanley, Kent, BR8 8AE
Tel: 01322 610100 Fax: 01322 610101
Web: www.astro.co.uk & www.classhawk.co.uk

Signal Strength

Signal Strength coverage (RSSI) of the selected access points. The strongest RSSI is shown per location.

-100.0..-90.0	-90.0..-80.0	-80.0..-70.0	-70.0..-60.0	-60.0..-50.0
-50.0..-40.0	-40.0..-30.0	-30.0..-20.0	-20.0..-10.0	-10.0..0.0

Access Point Count

Displays the number of audible access points per location with respect to the selected minimum RSSI requirement.

1	2	3	4	5	6
7	8	9	10	11	12

Astro Communications Ltd
Astro House, 41 High Street, Swanley, Kent, BR8 8AE
Tel: 01322 610100 Fax: 01322 610101
Web: www.astro.co.uk & www.classhawk.co.uk

Data Rate

An estimate of maximum data rate per location, with respect to the selected Signal-To-Noise threshold and the selected wireless network card receiver sensitivity values

1.0	2.0	5.5	6.0	9.0	11.0
12.0	18.0	24.0	36.0	48.0	54.0

Wireless Communication Policy

This section forms the basis of a policy that prohibits access to Uttlesford District Council networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by Uttlesford District Council are approved for connectivity to Uttlesford District Council's networks. This does not apply to any Guest Internet access wireless network, if provided.

This policy covers all wireless data communication devices (e.g. personal computers, cellular phones, PDAs, etc.) connected to any of Uttlesford District Council's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to Uttlesford District Council's networks do not need to comply with this policy. The policy section can be produced as a 'standalone document' to be added to Uttlesford District Council's general Security, Disaster Recovery and Business Continuity Policies.

***** Policy *****

Register Access Points and Cards

All wireless Access Points connected to the corporate network must be registered and approved by Uttlesford District Council. These Access Points/Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in corporate laptop or desktop computers must be registered with Uttlesford District Council and if not used for internal network access should be disabled while connected to the corporate network if possible.

Approved Technology

All wireless LAN access must use corporate-approved vendor products and security configurations.

Wireless Encryption and Authentication

While there are only a few wireless clients WPA-PSK (pre-shared-key) with TKIP (subset of the 802.11i) is an acceptable security regime. When client numbers start increasing, a PSK solution is not scalable and the 802.1X framework should be used to provide authentication for clients. (See 'Policy Notes' 1 to 3).

VPN Encryption and Authentication (if applicable)

To further strengthen security, the wireless network can be treated as an un-trusted Internet and all users provided with access via a VPN gateway. If this option is deployed in the strategy, all computers with wireless LAN devices must utilise a corporate-approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain strong point to point hardware encryption. All implementations must support a hardware address that can be registered and tracked, i.e. a MAC address. All implementations must support and employ strong user authentication, approved by Uttlesford District Council's ICT department.

Setting the SSID

The SSID shall be configured so that it does not contain any identifying information about the organisation, such as the company name, division title, employee name, or product identifier. When the SSID is suppressed it is still possible for a hacker to obtain it by intercepting a 'probe request' or 'association request' frame sent from the client to the AP when requesting service on the wireless network. This is why the SSID should not identify the organisation, even when the SSID is suppressed.

Revision History

This section must detail any changes throughout the history of this policy document

***** Policy Ends *****

Wireless Recommendations - General

Uttlesford District Council are aware of the potential threats associated with the implementation of wireless networking and as such are moving forward in this area with caution. There is always a balance between security and ease of operation The main business driver for the introduction of wireless access include:

- Portability – there are times when executives and staff members need access to systems from various areas in our offices and this would be better facilitated by wireless connectivity – Corporate WLAN.

- There is a potential requirement for Internet access to consultants/visitors without connecting directly to the corporate LAN – Guest WLAN.

- Readiness for future business requirements with correct security measures in place. An example may be wireless telephone handsets/headsets that integrate with an IP Telephony (IPT) solution – VoWLAN.

The results of our predictive analysis for minimum wireless cover is provided for each floor area in the plans a notes below. Minimum wireless cover allows data access in all office areas in Uttlesford District Council's offices. This wireless space can be divided into VLANs to provide separate networks for Corporate, Guest and VoWLAN over the same infrastructure.

Wireless Predictive Survey - Ground Floor

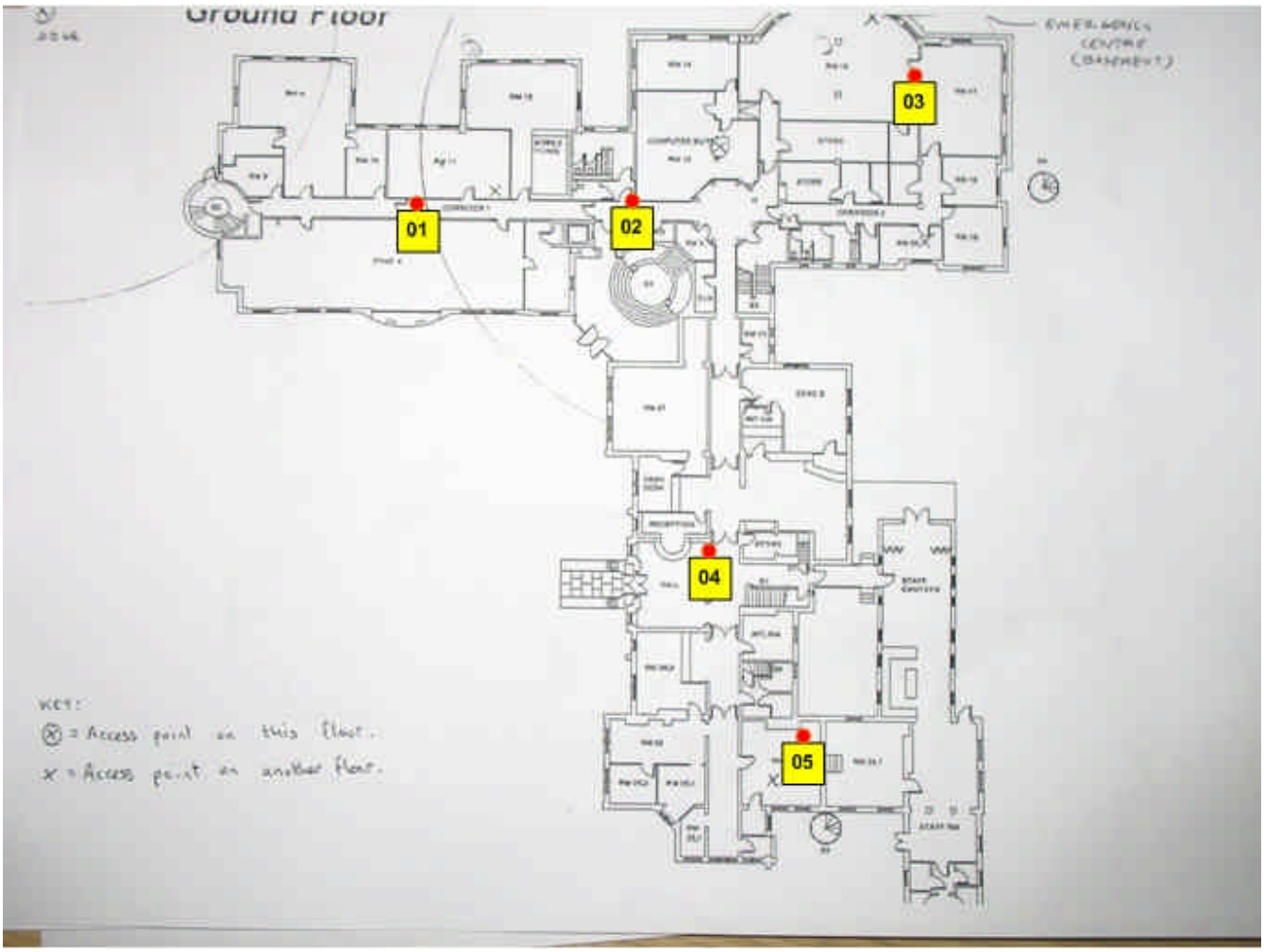
Access Point 802.11b channel allocations

ESSID	Name	Band / Channel	Privacy
Simulated Network	00:00:00:00:00:02	802.11b / 3	
Simulated Network	00:00:00:00:00:03	802.11b / 6	
Simulated Network	00:00:00:00:00:05	802.11b / 1	
Simulated Network	00:00:00:00:00:04	802.11b / 9	
Simulated Network	00:00:00:00:00:01	802.11b / 1	

Access Point antenna characteristics

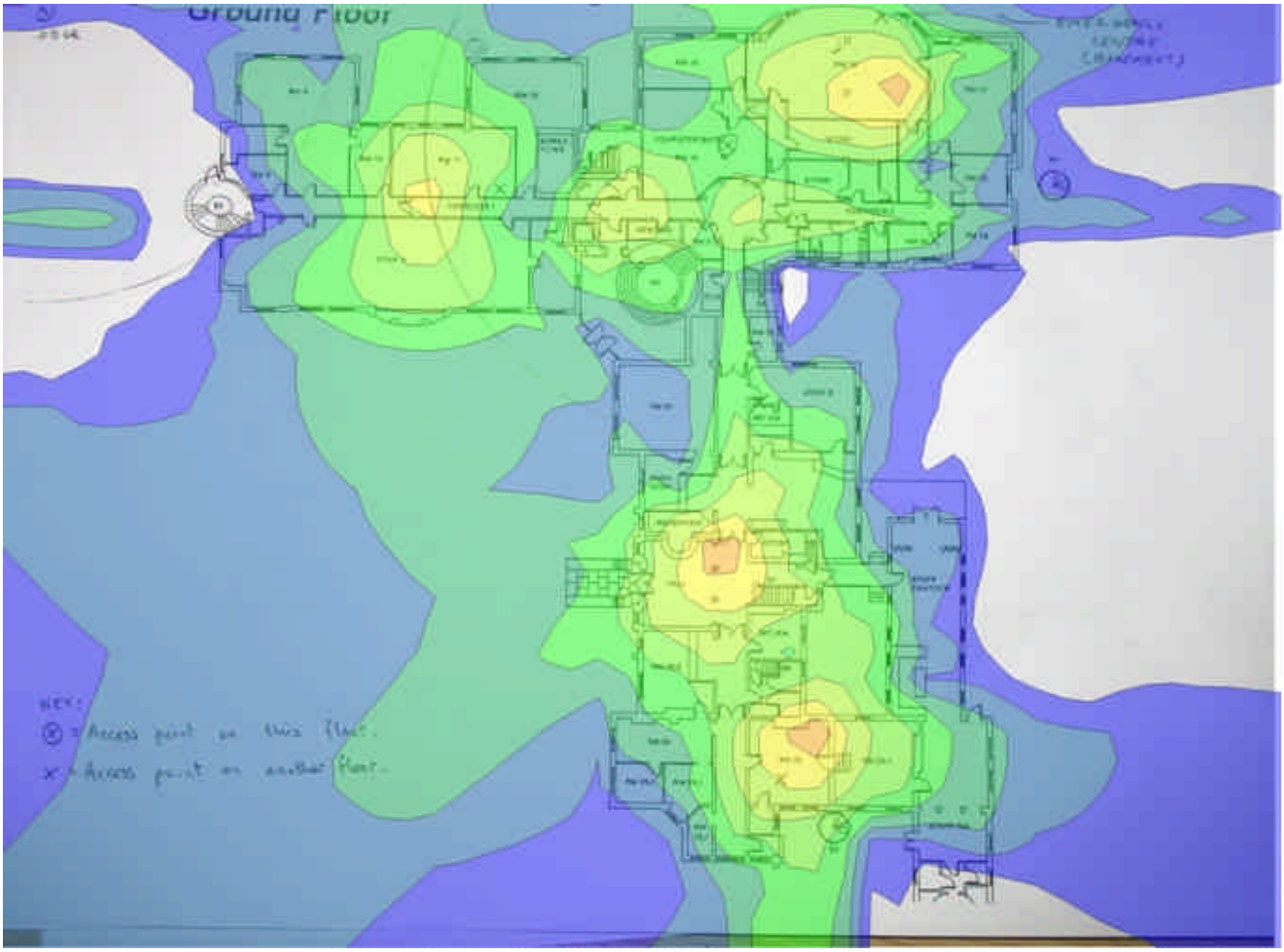
Name	Transmit Power	Antenna	Height	Direction
00:00:00:00:00:02	100	Omni-directional Antenna (2.15 dBi)	2	0
00:00:00:00:00:03	100	Sector Panel Antenna (10 dBi, 60 degree)	2	240
00:00:00:00:00:05	100	Omni-directional Antenna (2.15 dBi)	2	0
00:00:00:00:00:04	100	Sector Panel Antenna (3.5 dBi, 180 degree)	2	130
00:00:00:00:00:01	100	Omni-directional Antenna (2.15 dBi)	2	0

Access Point Locations



Astro Communications Ltd
Astro House, 41 High Street, Swanley, Kent, BR8 8AE
Tel: 01322 610100 Fax: 01322 610101
Web: www.astro.co.uk & www.classhawk.co.uk

Signal Strength

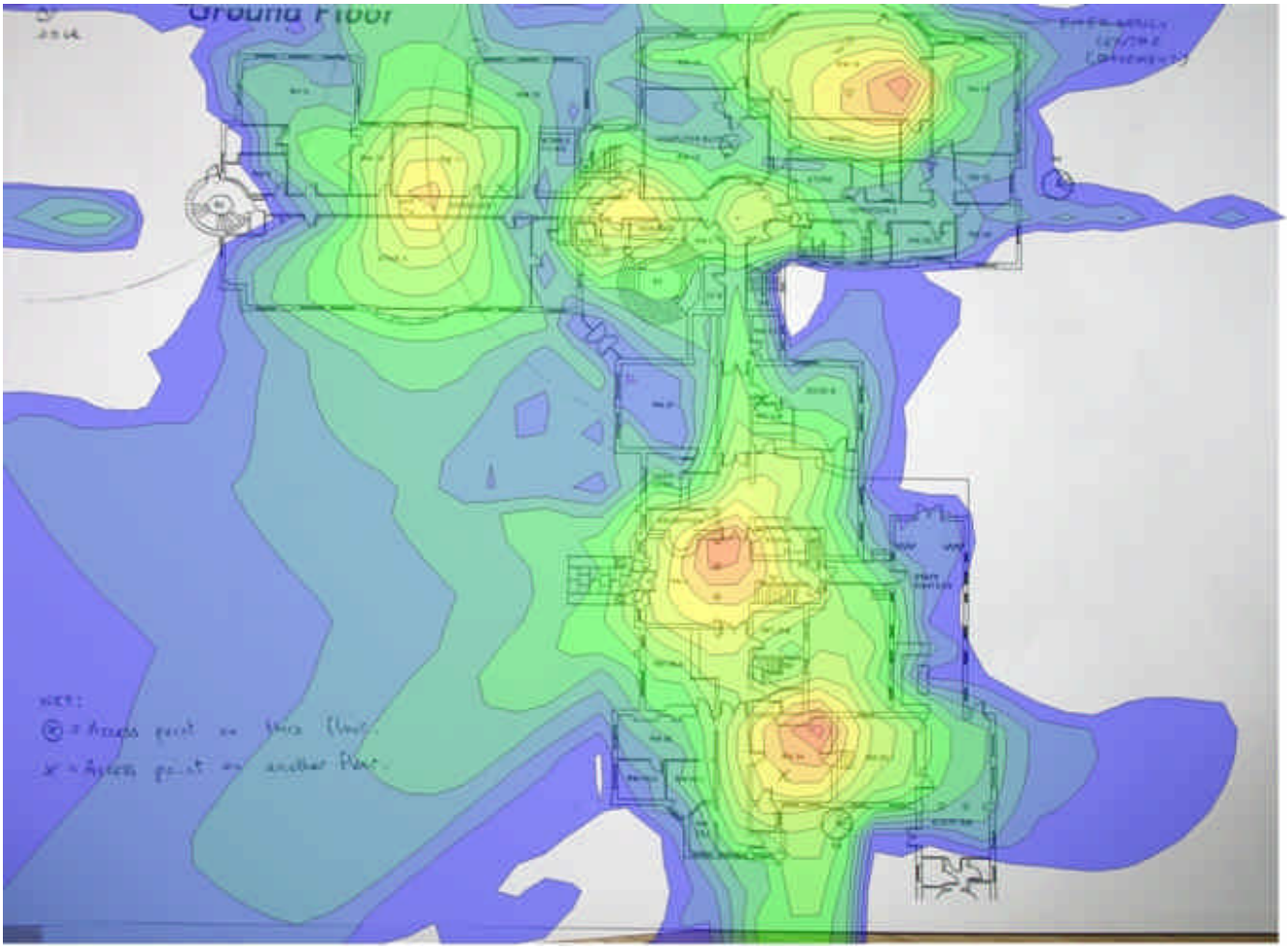


Signal Strength coverage (RSSI) of the selected access points. The strongest RSSI is shown per location.

-100.0..-90.0	-90.0..-80.0	-80.0..-70.0	-70.0..-60.0	-60.0..-50.0
-50.0..-40.0	-40.0..-30.0	-30.0..-20.0	-20.0..-10.0	-10.0..0.0

Astro Communications Ltd
Astro House, 41 High Street, Swanley, Kent, BR8 8AE
Tel: 01322 610100 Fax: 01322 610101
Web: www.astro.co.uk & www.classhawk.co.uk

Signal-to-Noise Ratio

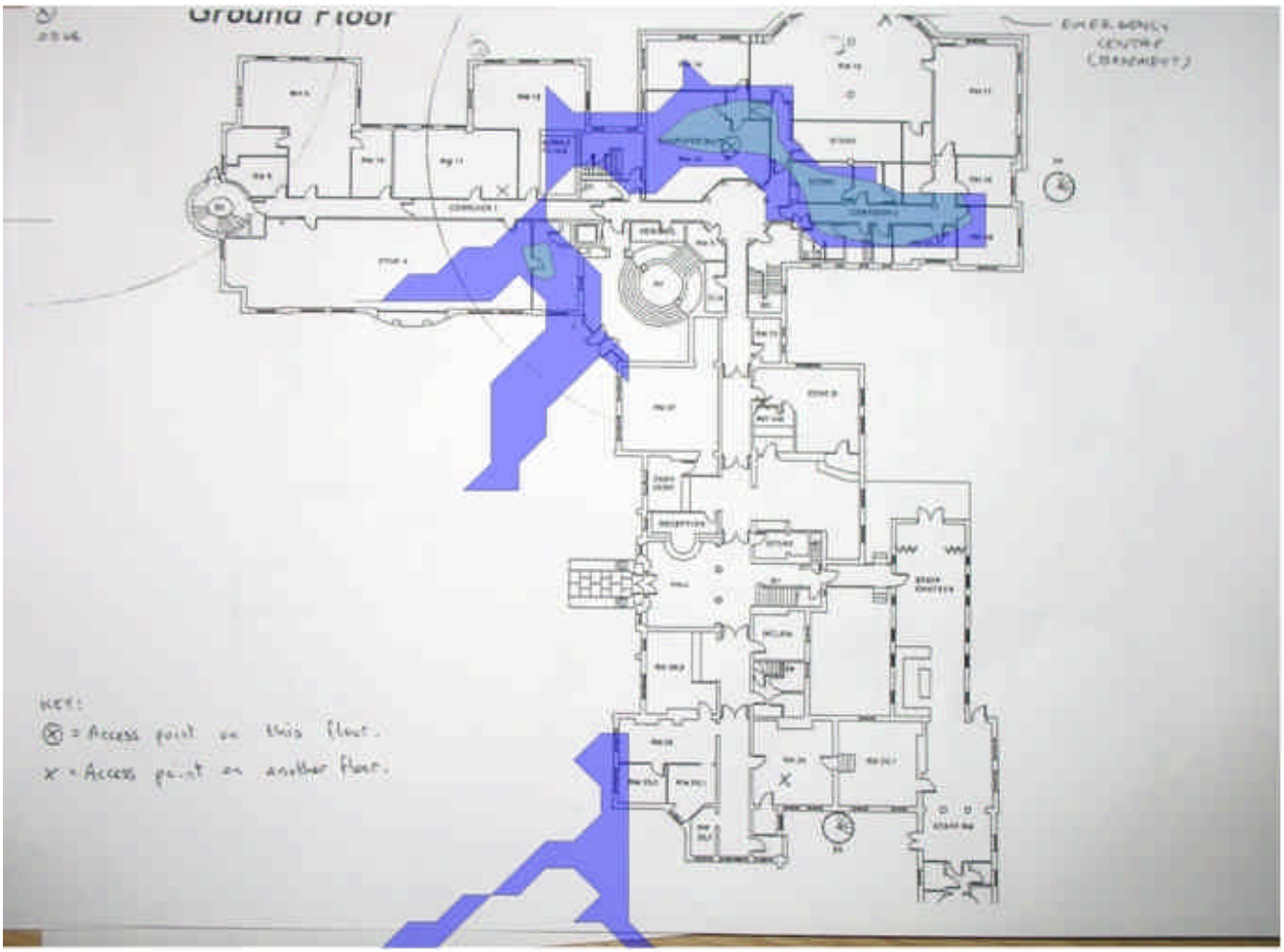


Calculated signal to noise ratio. Simplified formula: SNR = [Signal Strength] - [Interference]

0.0..5.0	5.0..10.0	10.0..15.0	15.0..20.0	20.0..25.0	25.0..30.0
30.0..35.0	35.0..40.0	40.0..45.0	45.0..50.0	50.0..55.0	55.0..60.0
60.0..65.0	65.0..70.0	70.0..75.0	75.0..80.0		

Astro Communications Ltd
Astro House, 41 High Street, Swanley, Kent, BR8 8AE
Tel: 01322 610100 Fax: 01322 610101
Web: www.astro.co.uk & www.classhawk.co.uk

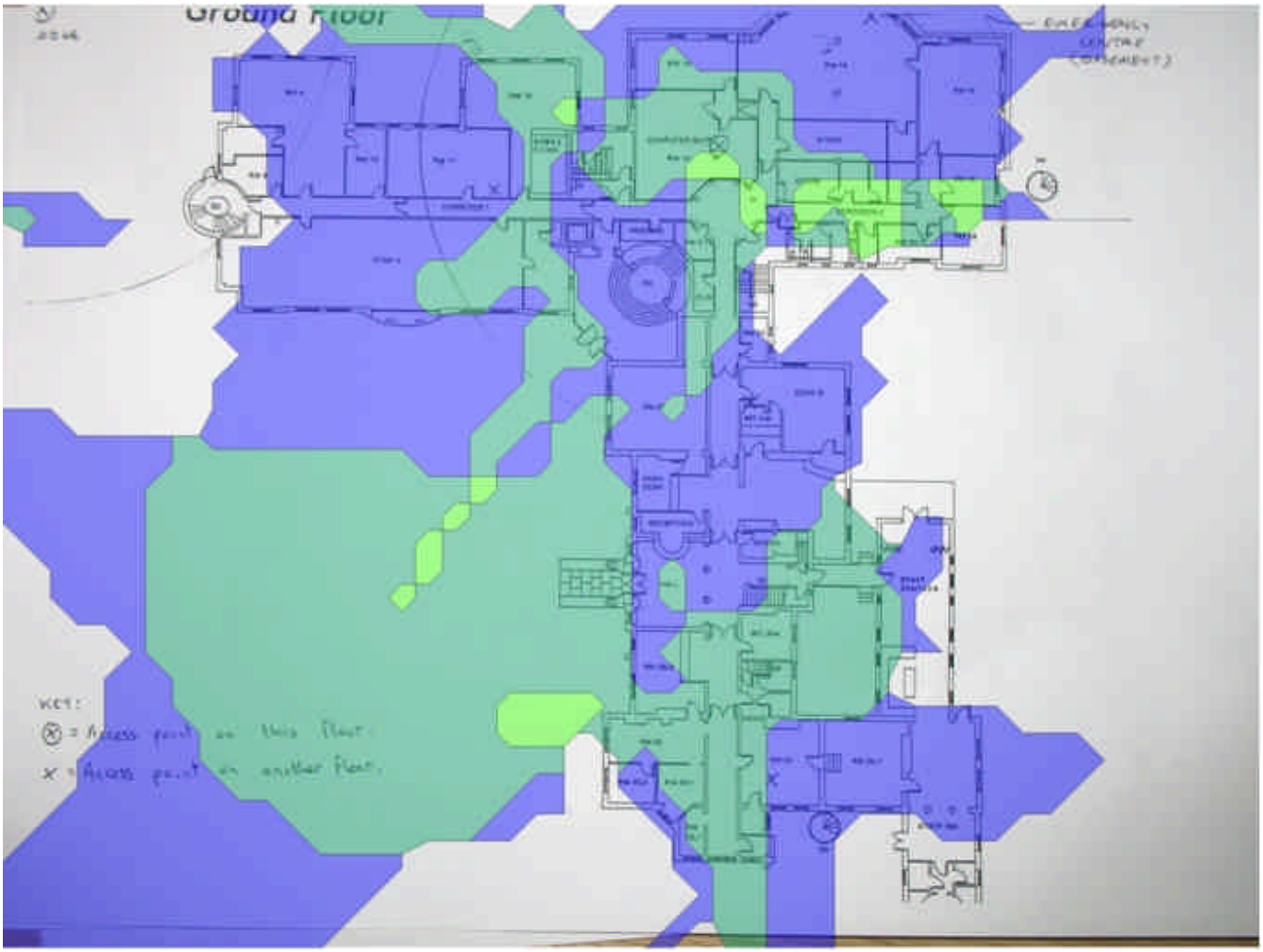
Interference



Calculated interference

-100.0..-90.0	-90.0..-80.0	-80.0..-70.0	-70.0..-60.0	-60.0..-50.0
-50.0..-40.0	-40.0..-30.0	-30.0..-20.0	-20.0..-10.0	-10.0..0.0

Access Point Count

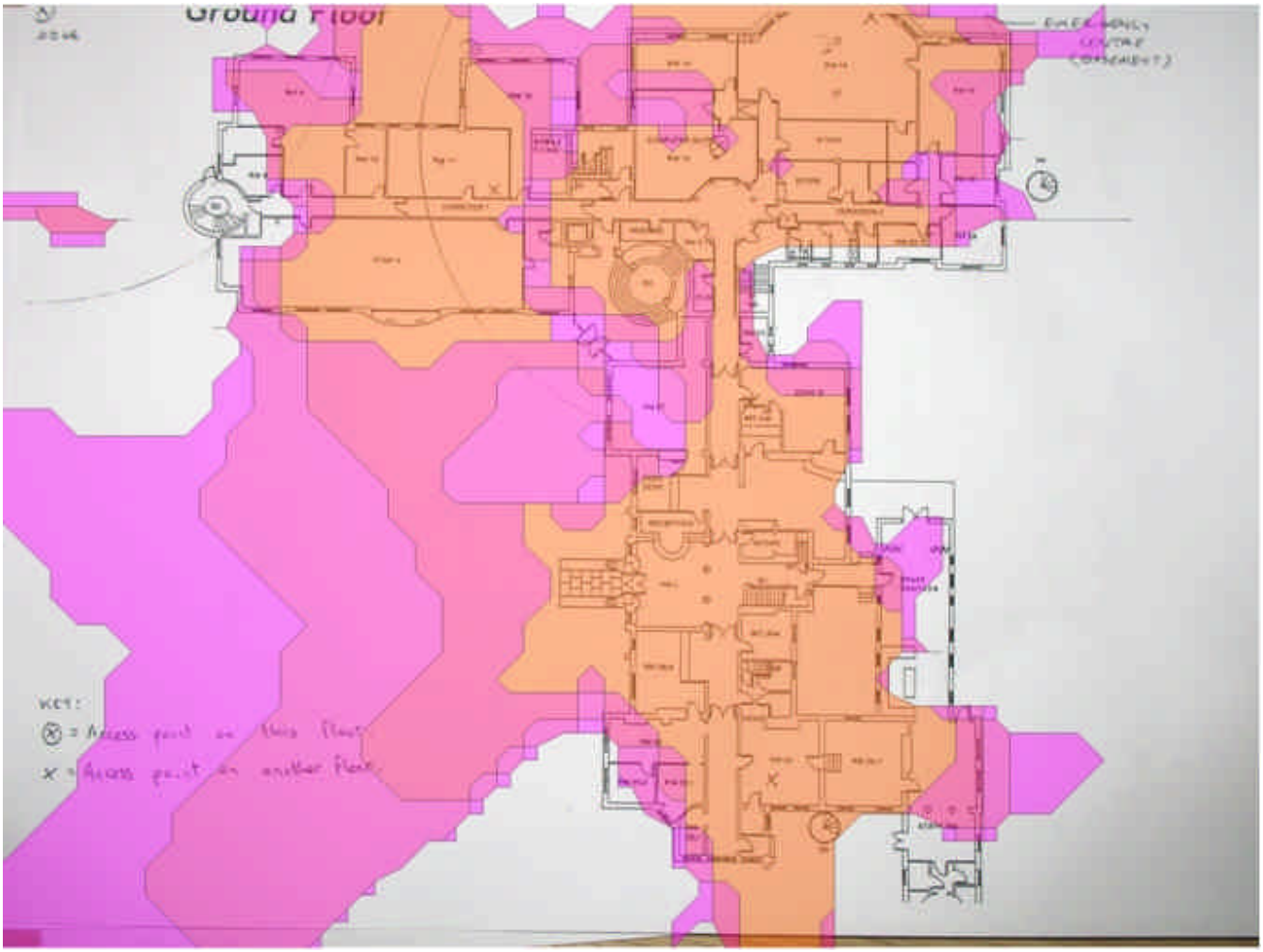


Displays the number of audible access points per location with respect to the selected minimum RSSI requirement.

1	2	3	4	5	6

Astro Communications Ltd
Astro House, 41 High Street, Swanley, Kent, BR8 8AE
Tel: 01322 610100 Fax: 01322 610101
Web: www.astro.co.uk & www.classhawk.co.uk

Data Rate



An estimate of maximum data rate per location, with respect to the selected Signal-To-Noise threshold and the selected wireless network card receiver sensitivity values

1.0	2.0	5.5	6.0	9.0	11.0
12.0	18.0	24.0	36.0	48.0	54.0

Wireless Predictive Survey - First Floor

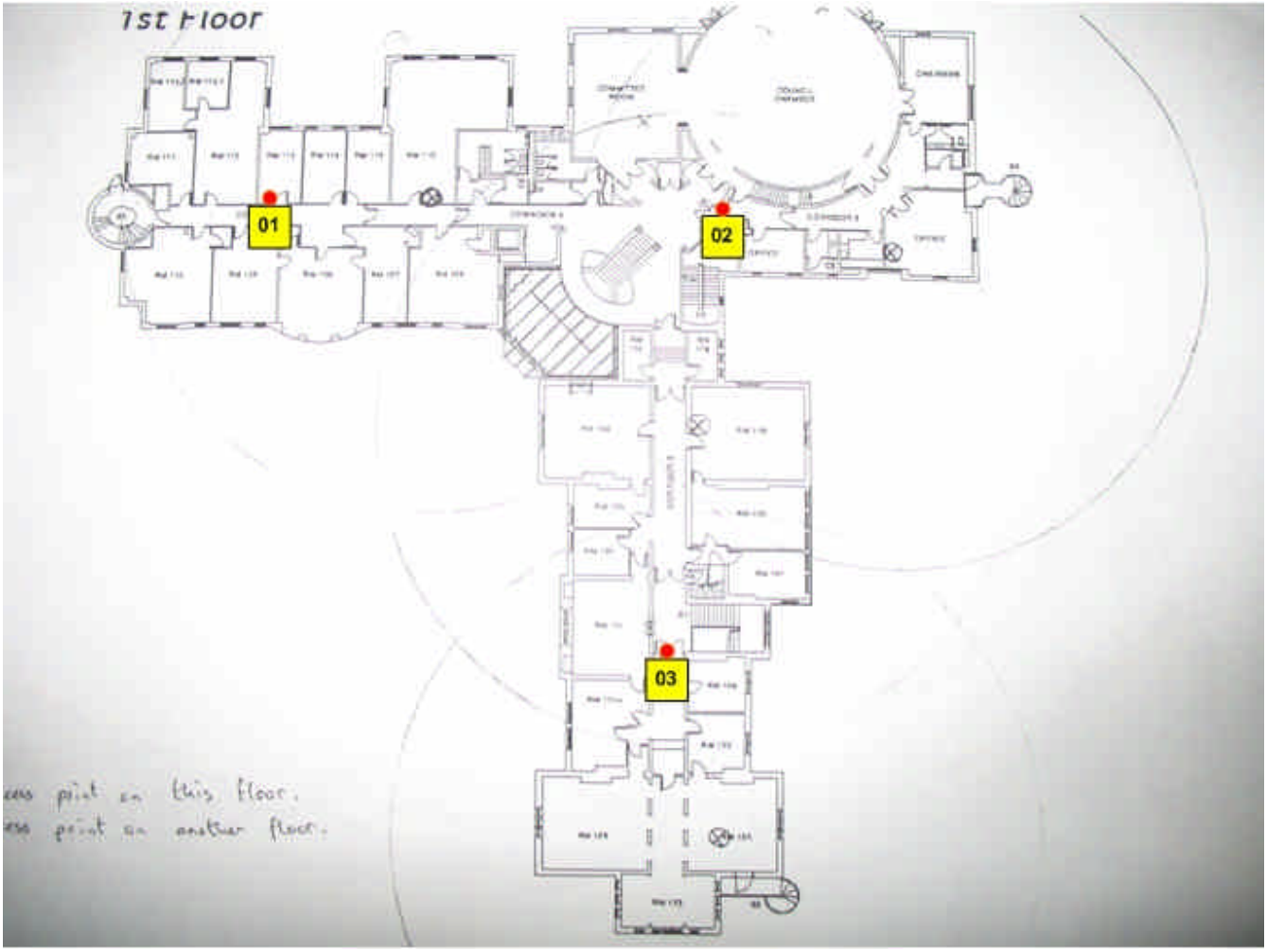
Access Point 802.11b channel allocations

ESSID	Name	Band / Channel	Privacy
Simulated Network	00:00:00:00:00:02	802.11b / 3	
Simulated Network	00:00:00:00:00:01	802.11b / 1	
Simulated Network	00:00:00:00:00:03	802.11b / 6	

Access Point antenna characteristics

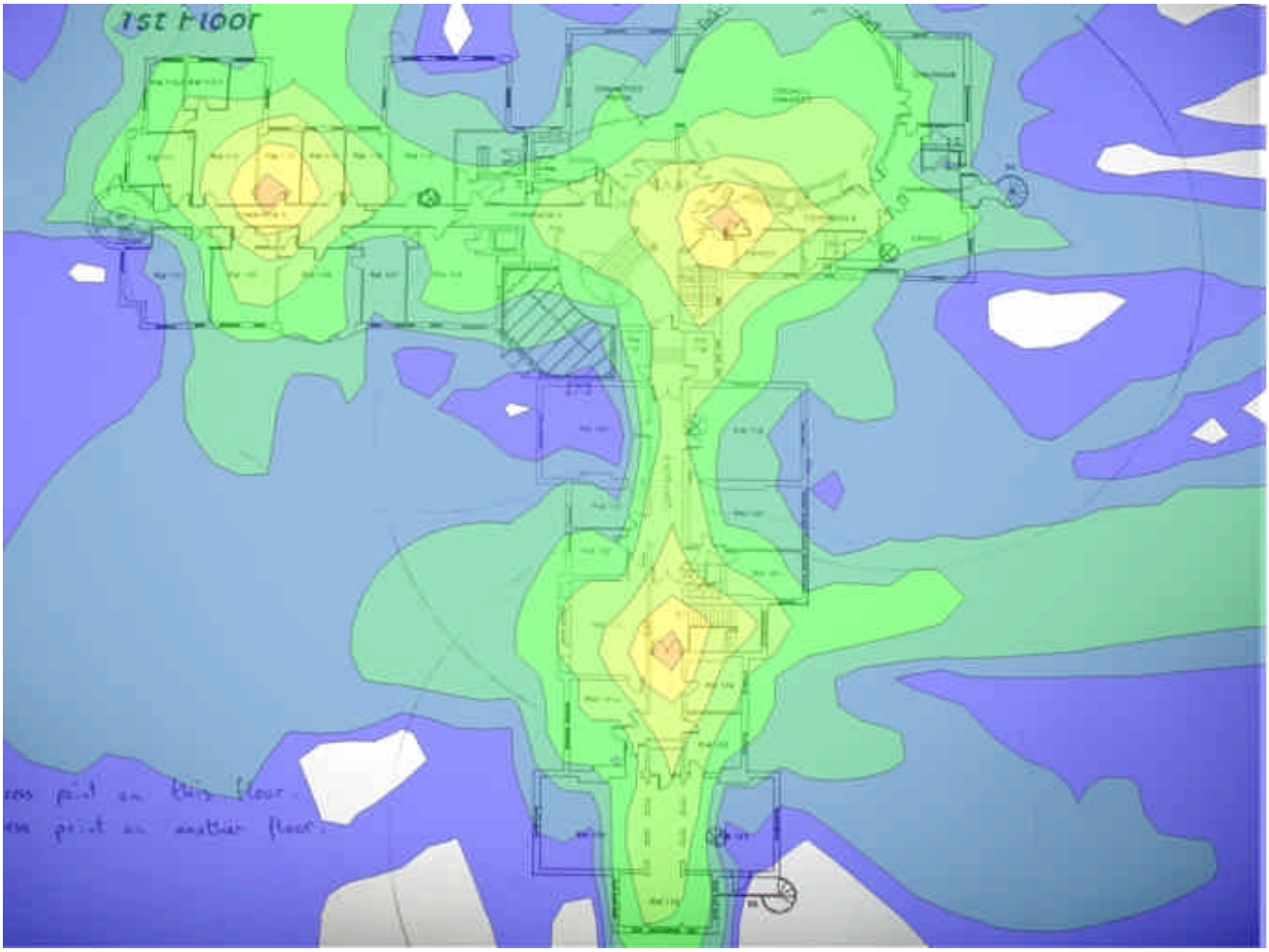
Name	Transmit Power	Antenna	Height	Direction
00:00:00:00:00:02	100	Omni-directional Antenna (2.15 dBi)	2	0
00:00:00:00:00:01	100	Omni-directional Antenna (2.15 dBi)	2	0
00:00:00:00:00:03	100	Omni-directional Antenna (2.15 dBi)	2	0

Sample Points and Access Point Locations



Astro Communications Ltd
Astro House, 41 High Street, Swanley, Kent, BR8 8AE
Tel: 01322 610100 Fax: 01322 610101
Web: www.astro.co.uk & www.classhawk.co.uk

Signal Strength

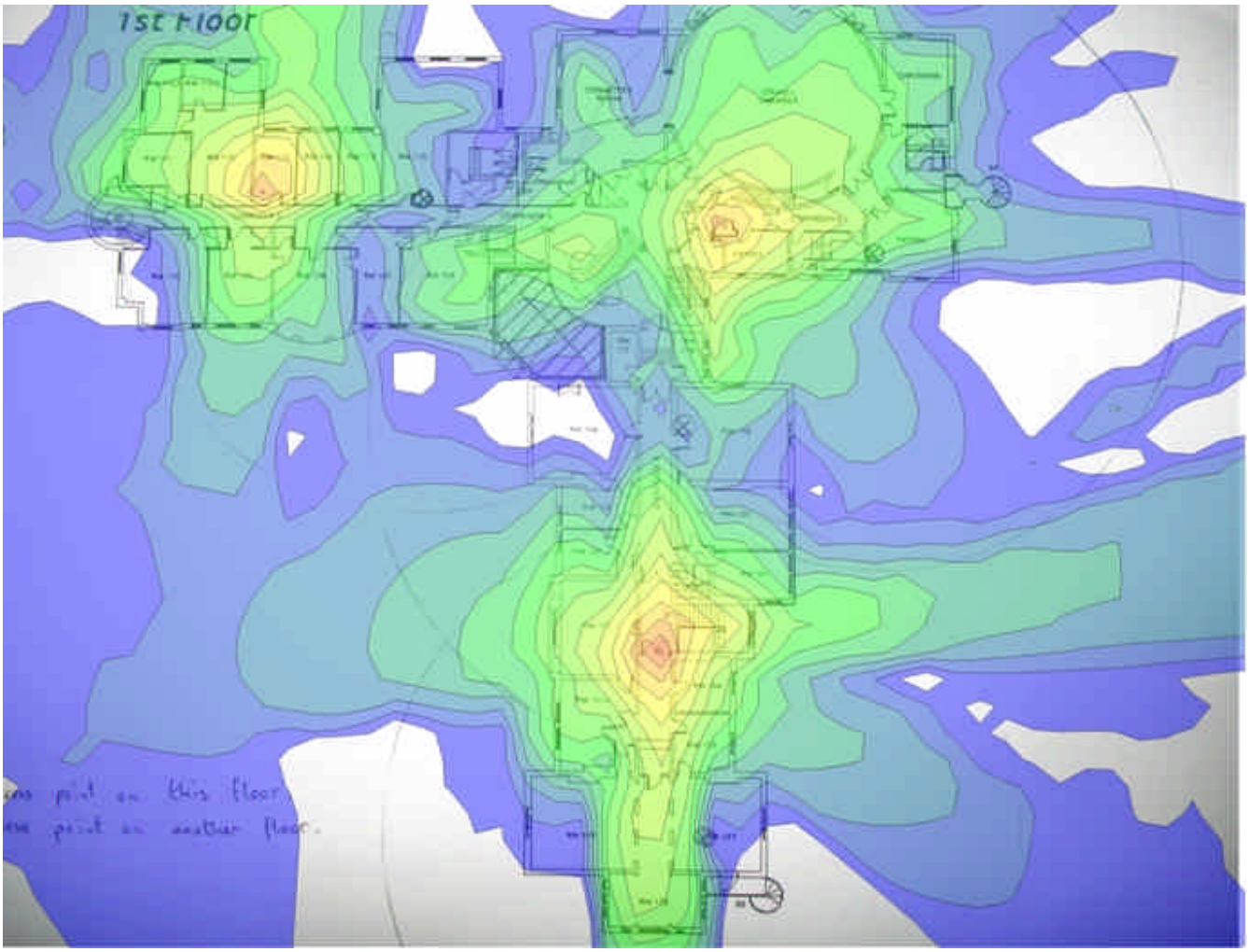


Signal Strength coverage (RSSI) of the selected access points. The strongest RSSI is shown per location.

-100.0..-90.0	-90.0..-80.0	-80.0..-70.0	-70.0..-60.0	-60.0..-50.0
-50.0..-40.0	-40.0..-30.0	-30.0..-20.0	-20.0..-10.0	-10.0..0.0

Astro Communications Ltd
Astro House, 41 High Street, Swanley, Kent, BR8 8AE
Tel: 01322 610100 Fax: 01322 610101
Web: www.astro.co.uk & www.classhawk.co.uk

Signal-to-Noise Ratio

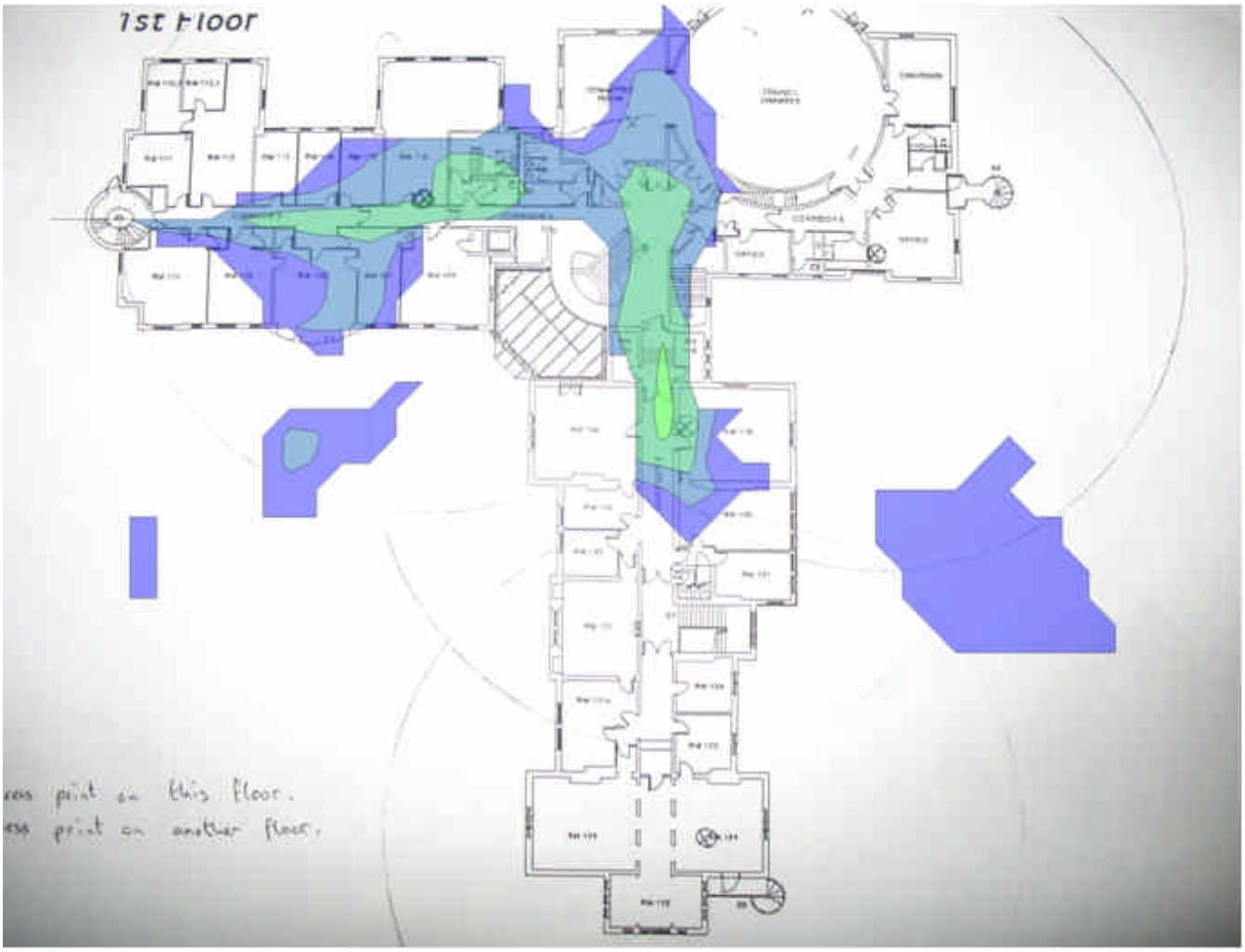


Calculated signal to noise ratio. Simplified formula: SNR = [Signal Strength] - [Interference]

0.0..5.0	5.0..10.0	10.0..15.0	15.0..20.0	20.0..25.0	25.0..30.0
30.0..35.0	35.0..40.0	40.0..45.0	45.0..50.0	50.0..55.0	55.0..60.0
60.0..65.0	65.0..70.0	70.0..75.0	75.0..80.0		

Astro Communications Ltd
Astro House, 41 High Street, Swanley, Kent, BR8 8AE
Tel: 01322 610100 Fax: 01322 610101
Web: www.astro.co.uk & www.classhawk.co.uk

Interference

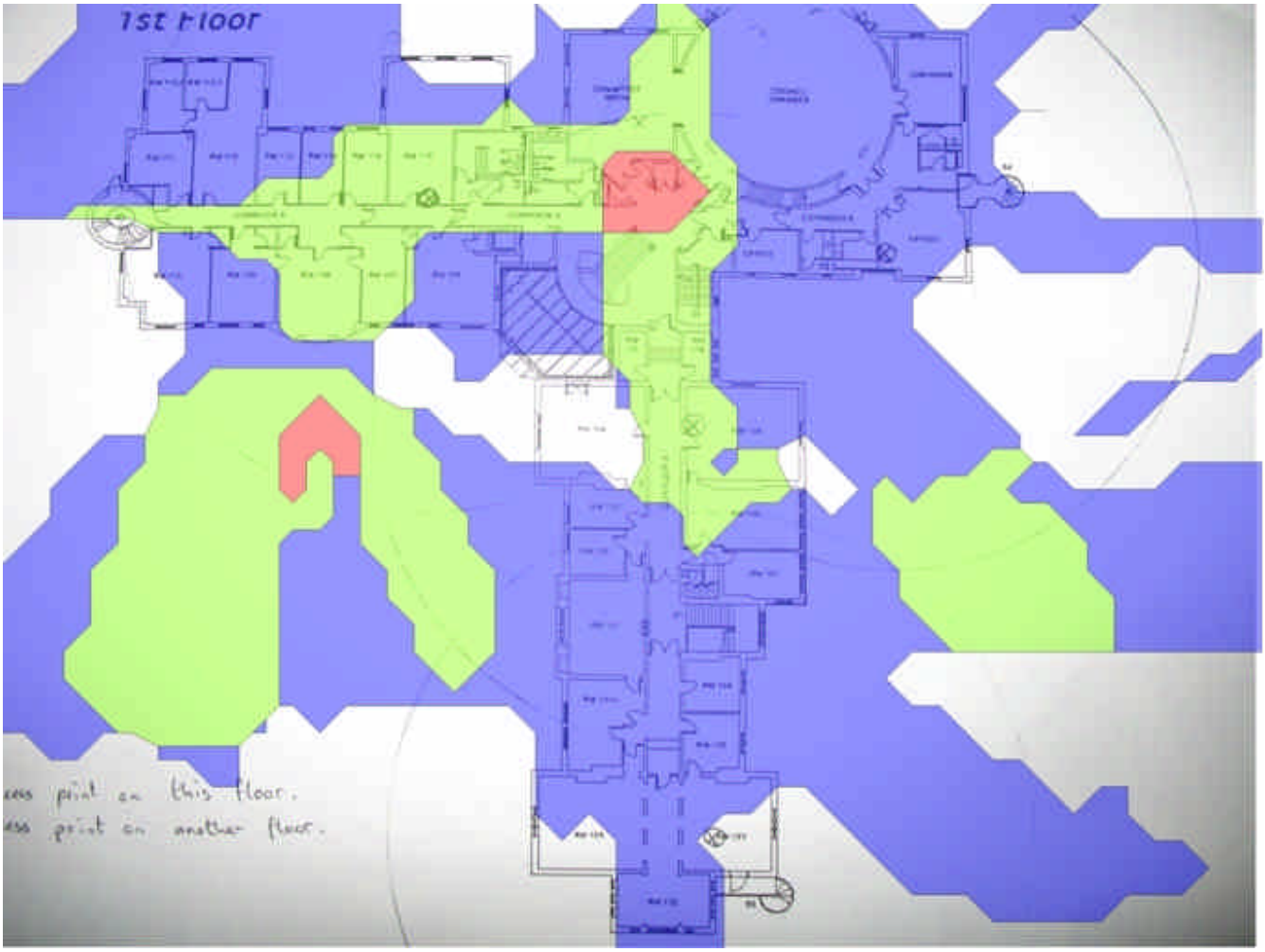


Calculated interference

-100.0..-90.0	-90.0..-80.0	-80.0..-70.0	-70.0..-60.0	-60.0..-50.0
-50.0..-40.0	-40.0..-30.0	-30.0..-20.0	-20.0..-10.0	-10.0..0.0

Astro Communications Ltd
Astro House, 41 High Street, Swanley, Kent, BR8 8AE
Tel: 01322 610100 Fax: 01322 610101
Web: www.astro.co.uk & www.classhawk.co.uk

Access Point Count

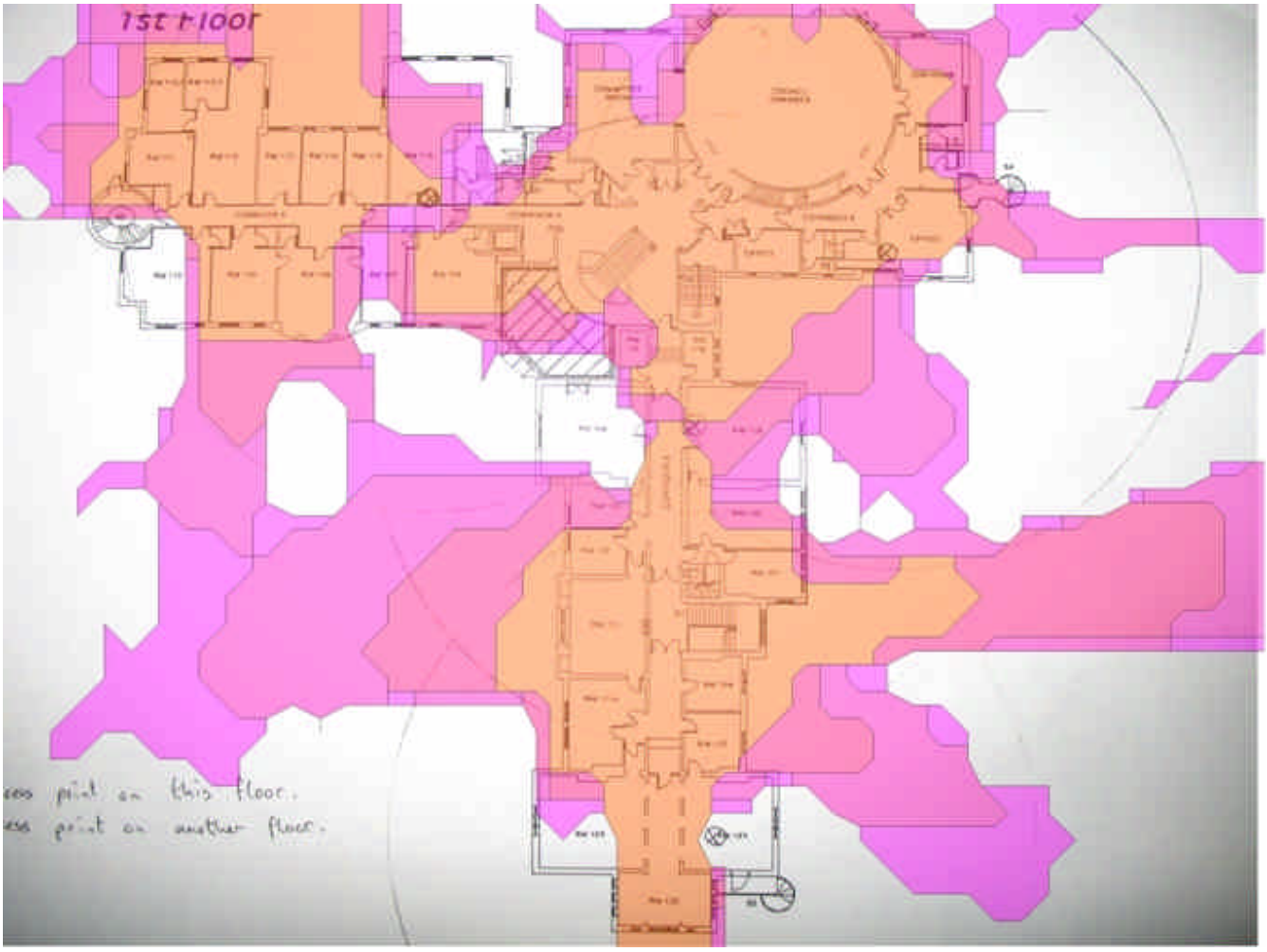


Displays the number of audible access points per location with respect to the selected minimum RSSI requirement.

1	2	3

Astro Communications Ltd
Astro House, 41 High Street, Swanley, Kent, BR8 8AE
Tel: 01322 610100 Fax: 01322 610101
Web: www.astro.co.uk & www.classhawk.co.uk

Data Rate



An estimate of maximum data rate per location, with respect to the selected Signal-To-Noise threshold and the selected wireless network card receiver sensitivity values

1.0	2.0	5.5	6.0	9.0	11.0
12.0	18.0	24.0	36.0	48.0	54.0

Astro Communications Ltd
Astro House, 41 High Street, Swanley, Kent, BR8 8AE
Tel: 01322 610100 Fax: 01322 610101
Web: www.astro.co.uk & www.classhawk.co.uk

Wireless Predictive Survey - Second Floor

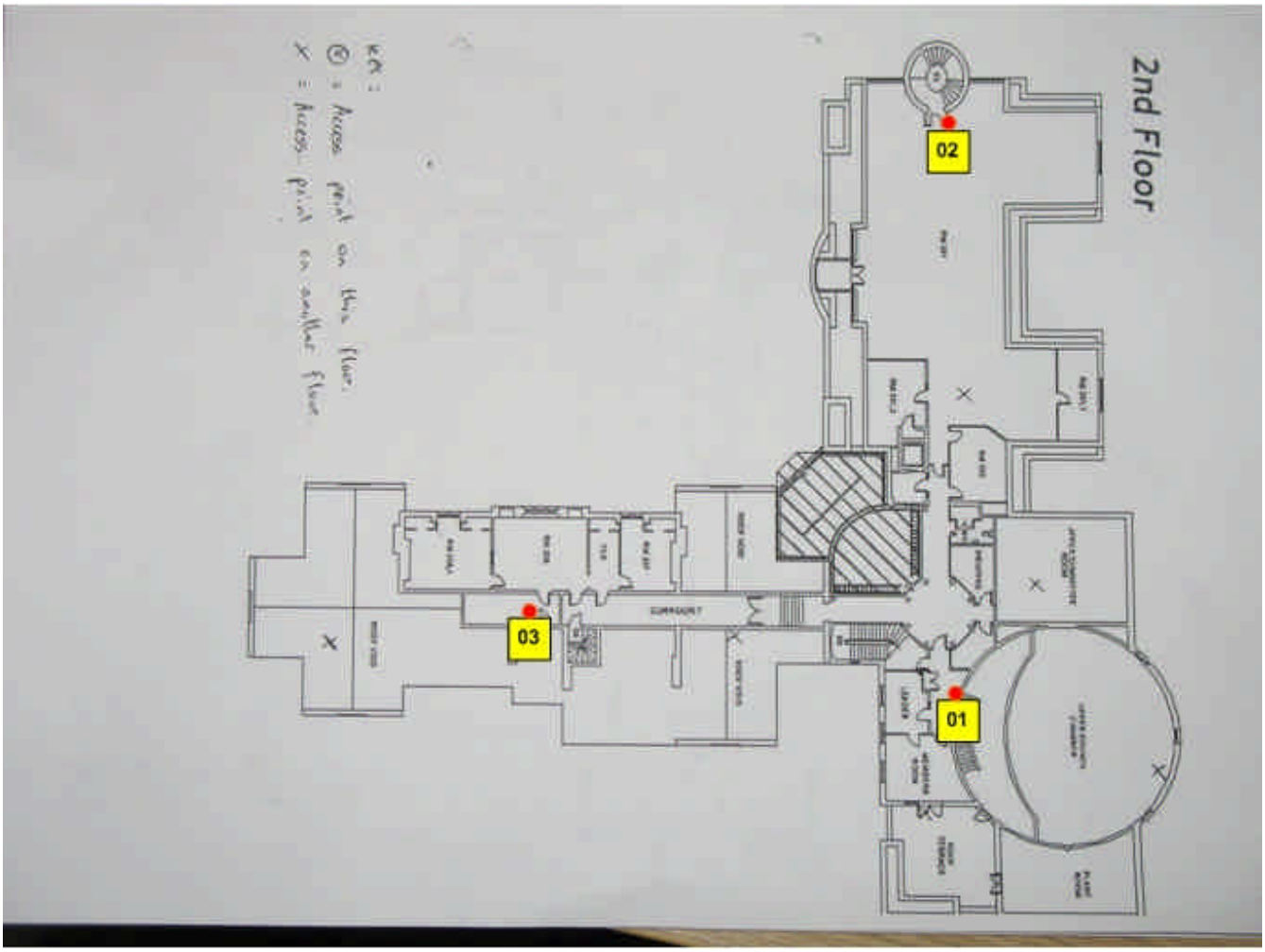
Access Point 802.11b channel allocations

ESSID	Name	Band / Channel	Privacy
Simulated Network	00:00:00:00:00:03	802.11b / 6	
Simulated Network	00:00:00:00:00:01	802.11b / 1	
Simulated Network	00:00:00:00:00:02	802.11b / 3	

Access Point antenna characteristics

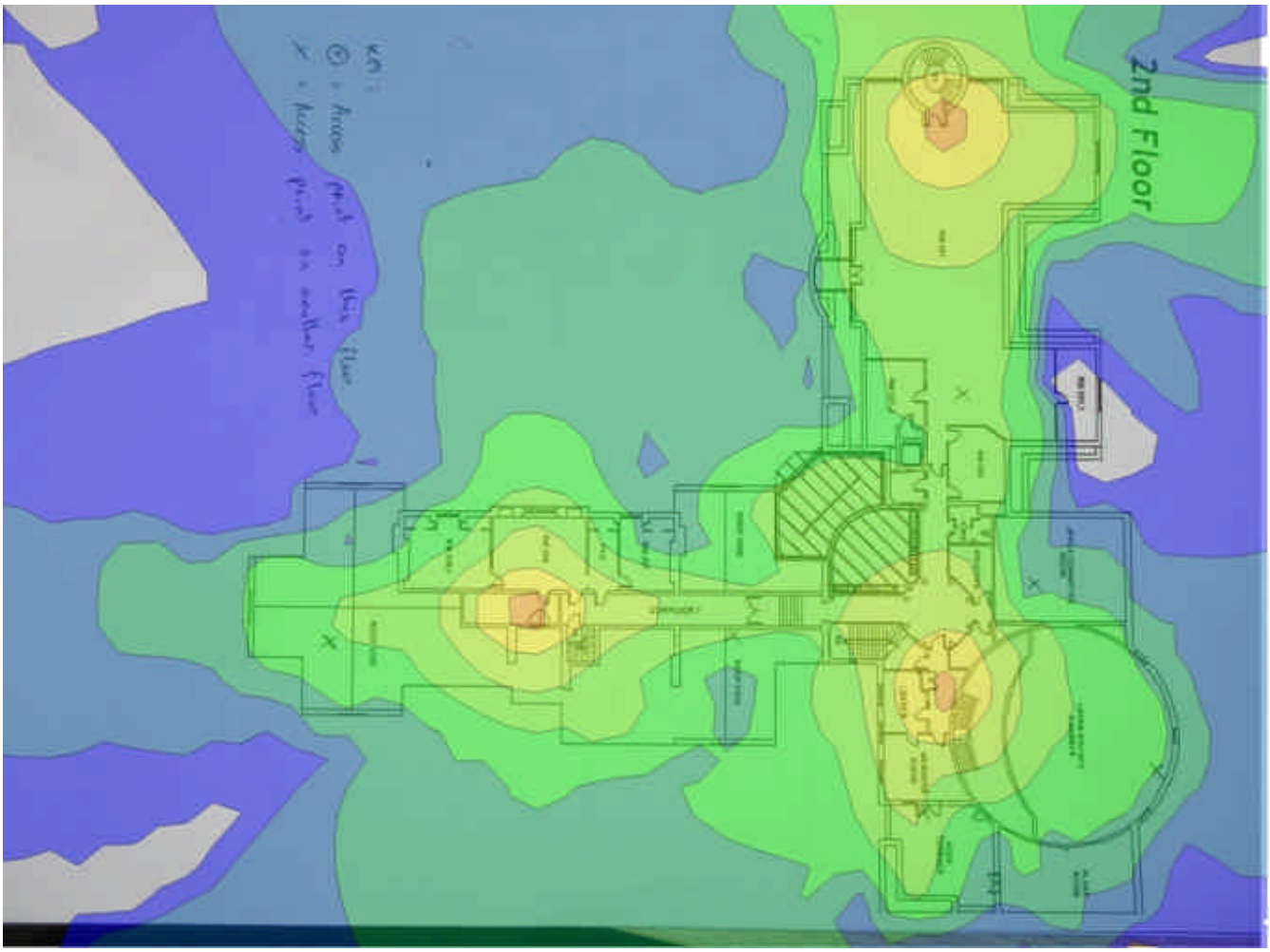
Name	Transmit Power	Antenna	Height	Direction
00:00:00:00:00:03	100	Omni-directional Antenna (2.15 dBi)	2.5	0
00:00:00:00:00:01	100	Omni-directional Antenna (2.15 dBi)	2.5	0
00:00:00:00:00:02	100	Omni-directional Antenna (2.15 dBi)	2.5	0

Sample Points and Access Point Locations



Astro Communications Ltd
Astro House, 41 High Street, Swanley, Kent, BR8 8AE
Tel: 01322 610100 Fax: 01322 610101
Web: www.astro.co.uk & www.classhawk.co.uk

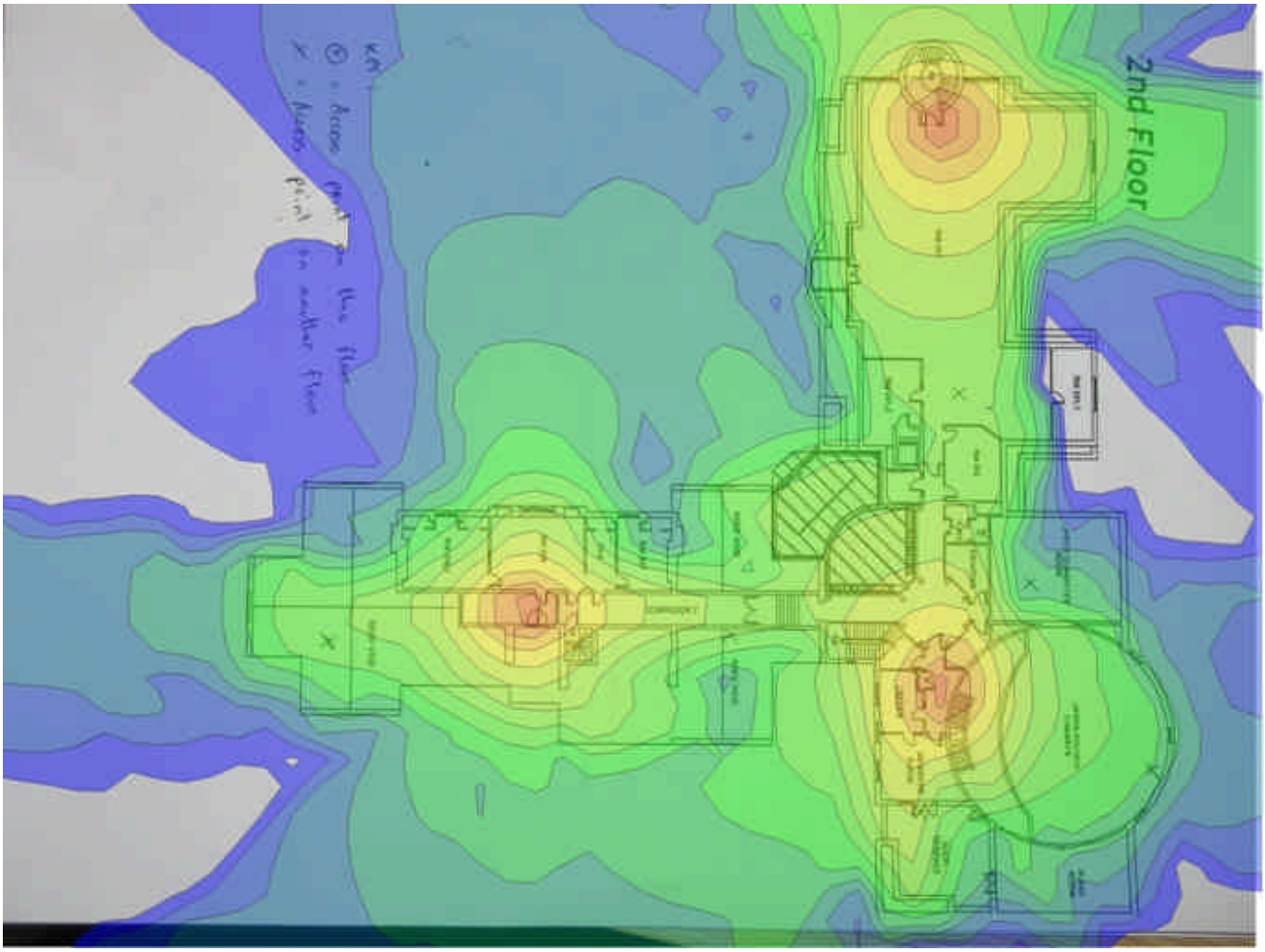
Signal Strength



Signal Strength coverage (RSSI) of the selected access points. The strongest RSSI is shown per location.

-100.0..-90.0	-90.0..-80.0	-80.0..-70.0	-70.0..-60.0	-60.0..-50.0
-50.0..-40.0	-40.0..-30.0	-30.0..-20.0	-20.0..-10.0	-10.0..0.0

Signal-to-Noise Ratio

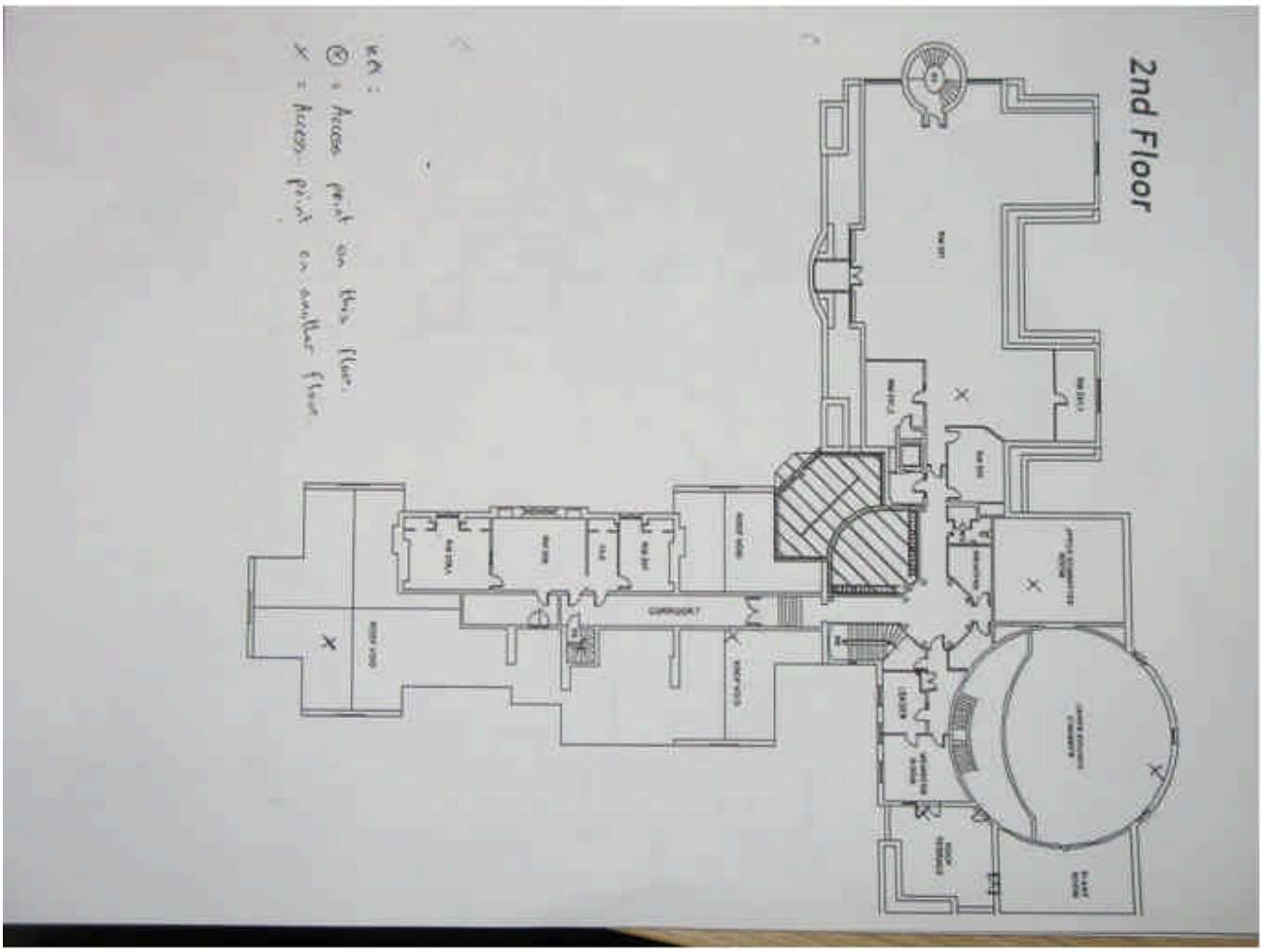


Calculated signal to noise ratio. Simplified formula: SNR = [Signal Strength] - [Interference]

0.0..5.0	5.0..10.0	10.0..15.0	15.0..20.0	20.0..25.0	25.0..30.0
30.0..35.0	35.0..40.0	40.0..45.0	45.0..50.0	50.0..55.0	55.0..60.0
60.0..65.0	65.0..70.0	70.0..75.0	75.0..80.0		

Astro Communications Ltd
Astro House, 41 High Street, Swanley, Kent, BR8 8AE
Tel: 01322 610100 Fax: 01322 610101
Web: www.astro.co.uk & www.classhawk.co.uk

Interference

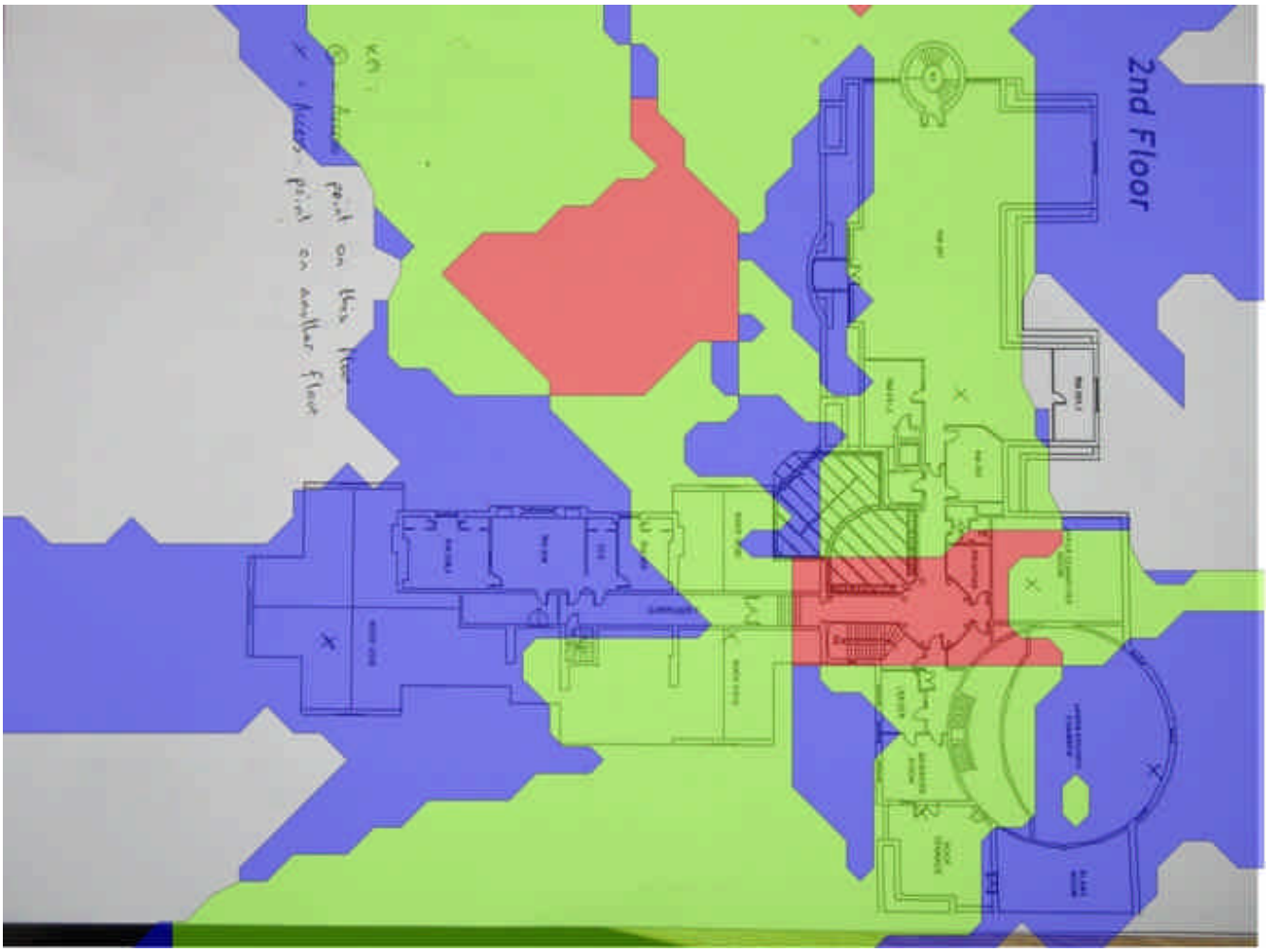


Calculated interference

-100.0..-90.0	-90.0..-80.0	-80.0..-70.0	-70.0..-60.0	-60.0..-50.0
-50.0..-40.0	-40.0..-30.0	-30.0..-20.0	-20.0..-10.0	-10.0..0.0

Astro Communications Ltd
Astro House, 41 High Street, Swanley, Kent, BR8 8AE
Tel: 01322 610100 Fax: 01322 610101
Web: www.astro.co.uk & www.classhawk.co.uk

Access Point Count

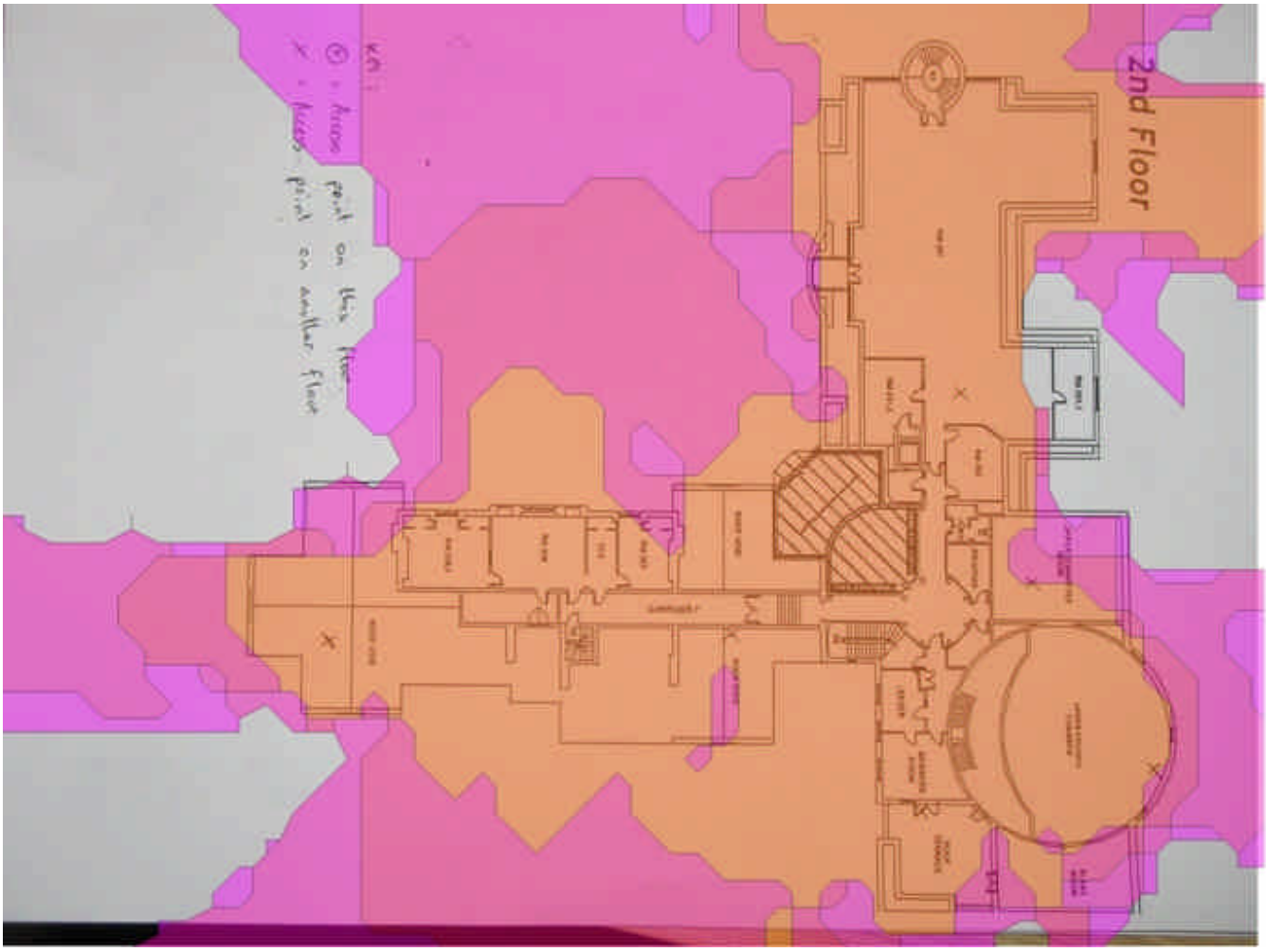


Displays the number of audible access points per location with respect to the selected minimum RSSI requirement.

1	2	3

Astro Communications Ltd
Astro House, 41 High Street, Swanley, Kent, BR8 8AE
Tel: 01322 610100 Fax: 01322 610101
Web: www.astro.co.uk & www.classhawk.co.uk

Data Rate



An estimate of maximum data rate per location, with respect to the selected Signal-To-Noise threshold and the selected wireless network card receiver sensitivity values

1.0	2.0	5.5	6.0	9.0	11.0
12.0	18.0	24.0	36.0	48.0	54.0

Enterprise Wireless Network Configuration Options
In the minimum wireless cover configuration, the network will support around 10 users per Access Point for normal office type applications and Corporate and Guest Internet services. If the wireless network is to support Voice over Wireless LAN the Access Point density will need to be increased to accommodate the increase in traffic and the demands of prioritised voice traffic over the wireless network. The actual density of wireless Access Points can only be determined when detailed traffic requirements are known or estimated. This is especially important when dealing with Voice over IP over Wireless LAN as any shortfalls in wireless bandwidth will result in telephone calls failing to connect or being dropped mid connection. Bandwidth shortfall will also affect the overall voice quality and in turn will rapidly lose the confidence of users.

The frequencies and power levels of wireless networks can be configured manually following radio surveys such as the predictive survey we carried out as part of this project. Manual configuration has its limitations in that the radio spectrum or wireless environment will change and can be very unpredictable over a period of time. There are a number of factors that affect the stability of the wireless environment, most of these can be classified as interference/noise (any external signal affecting the frequency band of the wireless network), typically from surrounding Access Points within and from outside Uttlesford District Council's premises. In addition to this, failure of one Access Point can place the nearby surviving Access Points under severe strain and can cause problems beyond the area covered by the faulty Access Point.

The alternative to a manually configured wireless network, is an automatically configured wireless network of which there are two common sub-configurations. The first involves the wireless network going through the automatic configuration process at installation time. When the automatic configuration process has completed, the configuration can be locked. Auto-configuration can be taken to the next stage by allowing the wireless system to dynamically re-configure to accommodate changes in the wireless environment. For example, if one of the Access Points fail, the controller can increase the power to the surrounding Access Points.

Manually configured wireless networks with many Access Points are very difficult to scale due to the complexities of multiple APs with overlapping cells. For Uttlesford District Council, we recommend deploying an automatic solution for anything other than our recommended minimum solution of eleven Access Points (five on the ground floor and three on each of the first and second floors). However, if it is anticipated that demand for the wireless network will grow in the near to medium future, it is advisable to deploy an automatic solution from the outset.

Client Wireless Supplicant
We advise the use of the wireless supplicant provided by the wireless chipset manufacturer where possible; e.g. if the device is a laptop and comes with the Centrino chipset, download the supplicant from Intel and disable the Microsoft supplicant. The benefit of running the supplicant from the chipset manufacturer is that it is purposely written for the chipset and will normally have many more supported authentication types; tuneable parameters and have more recent updates than the windows supplicant.

Using the chipset supplicant can cause management and support issues if Uttlesford District Council run a range of client PC manufacturer types with different chip sets and supplicants. If this is the case, the Windows supplicant can be of benefit as it is generic across all wireless devices. An update is available for the Microsoft supplicant that will provide WPA II and also contains a fix for some wireless networks not being recognised when the SSID is suppressed in beacon frames. Details can be found under Microsoft article number 893357.

Authentication, Encryption and related security techniques
802.1X - Authentication and Encryption are two different features of the client and wireless network. Authentication is provided with either a PSK (aka Personal Authentication) or via the 802.1X framework using an EAP type (aka Enterprise Authentication). Moving to the encryption scheme of WPA II (aka 802.11i) using AES-CCMP (Advanced Encryption Standard-Counter Mode CBC-MAC Protocol – see Notes 4) is advisable.

Using PSK for authentication for small wireless systems is useable (with a strong key) but can cause problems if the PSK is compromised (more likely by human factors rather than a hack) as all wireless devices have to have their PSK changed. For large numbers of clients this is not a scalable solution and can become administratively costly.

In large enterprise environments a central RADIUS server can be used to provide AAA (Authentication, Authorisation and Accounting) facilities. The RADIUS server can provide authentication facilities via a user database locally or can back end onto a Primary Domain Controller or NetWare Directory Services or any other user database. Using RADIUS it is easier to create, manage and delete clients from the wireless network. The users are authenticated via a username/password combination, but authentication could also involve secure ID, certificate exchange or other criteria. Not only can certificates be used for client authentication but the client can also authenticate the wireless network, to ensure that it hasn't attached to a rogue AP a hacker has set up nearby to trap user credentials or install rogue software on the client.

The RADIUS server can also return other attributes (Authorisation) to the APs such as the SSID the client can attach to and how regularly the client has to be re-authenticated.

Using the 802.1X framework is certainly more scalable and more manageable but requires initial investment in time and money to commission and test new infrastructure components.

WEP - Under no circumstances should WEP be used due to security issues associated with the protocol (weak WEP headers/initialization vectors). This applies to both variants of WEP.

MAC Address Filtering - is generally agreed not to be scalable and can be administratively costly. In addition to this, MAC addresses can be sniffed and faked so filtering offers limited security benefit. The administration overhead is due to all APs having to be kept up to date with MAC addresses of allowable clients. While this can be achievable in a small scale wireless environment it can become a major task once there are many access points. Also as clients are added, changes or removed these changes have to be reflected in the configuration in every access point. Manual MAC address entry is notoriously unreliable due to human error, this is exacerbated when the MAC addresses must be duplicated across all Access Points.

MAC address filtering can become feasible as a supplementary security measure if the 802.1X framework is supported and the APs support the MAC address as a return attribute from a RADIUS server. In this scenario the RADIUS server can store the allowable MAC addresses with the user credentials. This is more scalable as there is only one entry for each MAC address. The administration overhead and reliability problems remain as the RADIUS server must be kept up to date with MAC addresses as clients are added and changed.

Radio Management – some enterprise wireless management systems offer advanced features to manage the radio environment. These might include:

- Rogue Access Point detection, including the rogue device's IP and MAC addresses & SSID
- Client tracking to identify the access point to which each client device is associated
- Automatic counter measures in the event of a rogue device being detected

It is important to note, management facilities offered by manufacturers are only useful if the information is logged and audited to discover problems as they arise.

Network Management - SNMP can be used to obtain traps and gather statistics from Access Points. The SNMP process must be protected on the APs to maintain security. Use of the latest SNMP standard is recommended and the APs should only talk SNMP to listed devices. In addition to this, non-standard community strings should be used. This should only be used if the information gathered is of use and is going to be processed, otherwise, there is no benefit for the cost of a reduction in security.

Channel Assignment - using 802.11b/g there are three non-overlapping channel. ETSI specifies non-overlapping channels 1, 7 and 13. Although this can cause problems if you have a guest in using FCC specification hardware as their channel range will only go up to channel 11. The FCC recommends the use of non-overlapping channels 1, 6 and 11. There is also the potential problems associated with systems that dynamically auto-tune, where the AP will use the best channel in its air space and may change the channel over time as radio conditions change. This is as much a business decision as it is technical. If Uttlesford District Council decide on a frequency range for the installation then this becomes the standard and clients must adhere to this standard to access the network.

Interference
Interference can be controlled to a certain extent if the device causing the interference is controlled by a single organisation. Power of wireless devices can be controlled and the type and position of antennas can control the foot print of wireless networks. The control and selection of other technology such as DECT and Bluetooth can have an impact on the interference on the wireless network. Mobile telephones can also cause interference if adjacent to the access point or wireless unit of the PC.

Unfortunately, interference from third parties is not totally controllable unless the site is completely shielded from radio frequencies.

If third party interference or interference from devices within the organisation is severe enough then this could result in lower wireless throughput and many lost frames due to corruption. Measures can be taken within the configuration of the access points to try and compensate for noisy radio environments. These are as follows:

- RTS (Ready to Send)/CTS (Clear to Send) – This is used when many radio clients are connected to the same access point and simultaneously transmit. RTS/CTS can reduce the quantity of collisions. A frame threshold length is set on the access point that indicates when the clients have to use the RTS/CTS mechanism. The client will send an RTS packet to the AP telling it how long it wishes to occupy the air space while sending a frame, the length of occupation also includes the time for the access point to acknowledge the packet. The access point will respond with a CTS frame which all other clients pick up. From the CTS frame the other clients can see how long they must remain quiet for. RTS/CTS is also used when there are 802.11b and 802.11g clients sharing an AP. If the AP has a single 802.11b client on it the AP inserts a flag in its beacon frames. This indicates to other clients that they must use RTS/CTS mechanisms. This is due to 802.11b and 802.11g using incompatible radio access techniques. 802.11b uses DSSS (Direct Sequence Spread Spectrum) and 802.11g uses OFDM (Orthogonal Frequency Division Multiplexing). Using mixed radio access techniques on an AP can reduce throughput by 30% as a result of this mechanism.

- Fragmentation – This technique is used when there is general RF interference, such as from other APs, clients or other devices such as DECT phones, Bluetooth, mobile phones, microwaves etc. A frame size threshold is set and any frames bigger than the threshold get fragmented. Each frame will have its own 802.11 header that will indicate that it is a fragment of a bigger frame. Smaller frames have much more chance of being transmitted and received as they occupy the air space for a shorter space of time. This mechanism again slows down throughput because of the 802.11 frame overhead on each of the fragments.

Both of the above mechanisms can increase throughput, but both also decrease throughput. Somewhere there is a happy medium that can be achieved with regard to throughput and corrupted frames. These mechanisms are normally disabled by default on APs or set to high enough thresholds that they are not used. If they are used it is normally trial and error in configuring them. A change is made and then the effects are monitored to see if there are improvements.

Notes

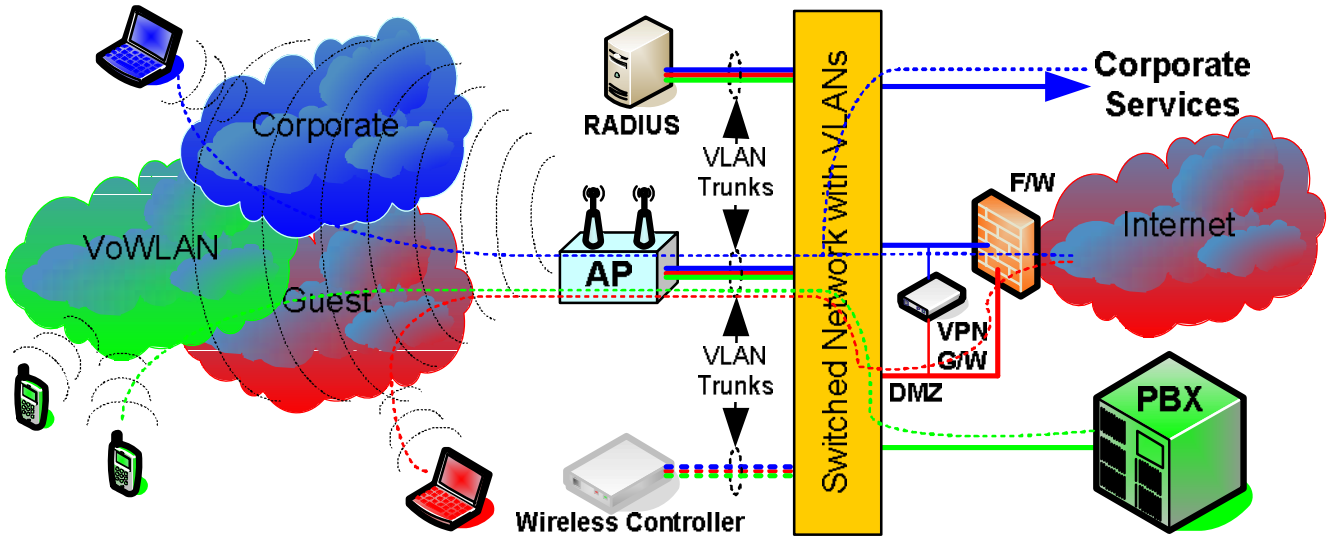
1. PSK solutions rely on all clients to be manually configured with an authentication key that matches the wireless infrastructure equipment. If the key becomes compromised it would mean all clients and access points require configuration changes. With a large amount of APs and clients this can become very costly in terms of administration.

2. WPA II which is the full 802.11i standard is now available for use. WPA II is supported on most enterprise class wireless Access Points. It is important to note that their may be some software client issue and some operating systems may not support this. It is possible on most enterprise class APs to run multiple security profiles on the same SSID or use wireless VLANs each with a separate security profile. This can provide the facility to use different client types, i.e. internal laptops could be upgraded to WPA II but visitor's clients may only be able to support WPA.

3. Current best practice dictates that a PSK for use with WPA and WPA II must be at least 20 characters in length and contain non-standard characters and not be a dictionary word.

4. AES-CCMP (AES-Counter Mode CBC-MAC Protocol) is the encryption algorithm used in the 802.11i security protocol. AES-CCMP incorporates two sophisticated cryptographic techniques (counter mode and CBC-MAC) and adapts them to Ethernet frames to provide a robust security protocol between the mobile client and the access point. AES itself is a very strong cipher, but counter mode makes it difficult for an eavesdropper to spot patterns, and the CBC-MAC message integrity method ensures that messages have not been tampered with.

Example of Operation



The diagram above shows a Wireless LAN connectivity scenario with three VLANs. A single Access Point is shown in this diagram, in practice the Wireless media will be provided by multiple APs. There may be a fourth VLAN for management and authentication.

All users accessing the wireless network are directed to the RADIUS Server. The RADIUS Server determines the users rights and allows access to the specific VLAN dictated by the clients credentials.

Corporate clients – are connected to the Corporate Wireless VLAN. This enables full access to the Corporate services controlled by Directory Services within the Corporate network (as per any other fixed connection client). Access to the Internet is via the Corporate firewalls.

Guest clients – are connected to an un-trusted Wireless VLAN with almost no restrictions to the Internet. Typically this would either connect to the Internet via a DMZ on the Corporate firewalls or it would be provided with a dedicated Internet connection e.g. ADSL.

VoWLAN clients – are connected into the VoWLAN Wireless VLAN where the clients enjoy high priority traffic flow and handover between APs to ensure voice quality and connection is maintained while moving around the building.

Wireless networks with automatic management and configuration require Wireless Controller equipment to manage the APs. These provide a more effective solution for VoWLAN services due the Controllers ability to monitor all APs and adjust the wireless network environment accordingly. Also, handover from one AP to another during cordless phone roaming is more effective. The APs in this environment are referred to as Lite APs as the intelligence is within the Controller.

For manually configured wireless networks each AP has to manage the relationship between itself and other APs.

Internal VPN Client option – removes the need for a Corporate Wireless VLAN as the laptop users access the Corporate Network as if they were working at home via the Internet – which in this case is the un-trusted VLAN. If the laptop is already equipped with VPN client software and the user is familiar with remote access then this provides a solution that is as secure as existing VPN users.

Solution Budgetary Costs
There are several enterprise class wireless systems that could be deployed within Uttlesford District Council offices to satisfy the requirements of our recommendations. We have selected the Siemens HiPath Wireless solution as a model for the budgetary costs as a potential future Voice over IP over Wireless LAN (VoWLAN) solution will be fully compatible with the Siemens telephone switch. This does not preclude Uttlesford District Council from deploying other manufacturers' systems provided any compatibility issues between the telephone system and a potential future VoWLAN implementation are taken into consideration.

The Siemens HiPath wireless solution is a centrally controlled dynamic auto configuration system. Once installed, the APs communicate with each other and manage the air space between them. They can take action against rogue Access Points and will automatically adjust power and frequencies to recover from an AP failure (applies to options 2 and 3 in this budgetary proposal only). Several cost options are provided in two categories:

- Non-resilient Solution
- Resilient Solution

Within each of these categories there are three options of Access Point density:

- Minimum Density – 11 APs to support equivalent of existing users in Corporate and Guest VLANs
- Medium Density – 24 APs to support medium number of users in Corporate, Guest and VoWLAN VLANs
- High Density – 39 APs full support high number of users in Corporate, Guest and VoWLAN VLANs

With the exception of the 'Minimum Density' option, these are hypothetical configurations to provide budgetary costs. The actual number of users for medium and high depends on the balance of voice and data and the amount of roaming involved. For example, if voice users are roaming between APs, assumptions must be made such as a reasonable spread of users across APs.

Non resilient options – budgetary costs for supply, installation and commissioning:

Option 1	£32,000.00
Option 2	£42,000.00
Option 3	£54,000.00

Resilient options – budgetary costs for supply, installation and commissioning:

Option 1	£52,000.00
Option 2	£62,000.00
Option 3	£74,000.00

Notes

1. The budgetary prices include RADIUS server in the non resilient option and two RADIUS servers in the resilient option. This includes the price of the PC hardware to host the RADIUS service.

2. If Uttlesford District Council wish to use VPN technology to access the Corporate network via the un-trusted wireless network, additional VPN and firewall hardware may be required if an existing VPN gateway and firewall is not available or not suitable.

3. It is possible to deploy a wireless network for considerably less but this may restrict development in the longer term and may also introduce security vulnerabilities that are difficult to overcome.