Deployment issues in making the transition from 802.11a/g to 802.11a/g/n

Scott Armitage, Loughborough University

9 May 2011

Introduction

802.11n is the latest Wi-Fi standard in wireless networking. Although the standard was only fully ratified in 2009, it is already very well supported in client chipsets. Pre-standard devices began appearing as early as 2007 and by the time of ratification, the vast majority of new laptops being sold had 802.11n-capable wireless adapters. Furthermore, 802.11n has now begun to appear in smart phones.

Whilst there is a large base of clients that support 802.11n, most institutions' infrastructures are still only capable of supporting 802.11a/g (802.11b has now been effectively replaced on campus by the high data rate technologies). This has come about because the investment was made in wireless networks before 802.11n access points were widely available As a result most institutions have large 802.11a/g deployments of hundreds, or even in some cases thousands, of 802.11a/g-only access points. Given the large capital cost associated with upgrading an institutions' whole wireless infrastructure, and the fact that existing 802.11a/g equipment has not reached the end of its expected life, it is unlikely that institutions will replace their whole existing deployment in a single big upgrade.

Typical a/b/g to n migration

The migration to 802.11n is likely to take place take place in a number of ways:

- **New builds.** New building projects will generally have 802.11n access points included as part of the specification. In most cases, there will be little or no overlap between new 802.11n and 802.11a/g domains elsewhere on campus. **Upgrades in areas with high utilization.** Some areas, e.g. libraries, will have many more clients and higher utilisation than other areas. Access points in these areas may be upgraded to 802.11n to support more clients and provide better throughput.
- **Upgrades of existing buildings.** Existing buildings may have a wireless refresh as part regular upgrades.
- **Replacement of faulty access points.** Inevitably in any large deployment eventually an access point will fail. These units may well be replaced with 802.11n equipment.

Co-existence of a/b/g and n

These ad-hoc methods of deployment will lead to 802.11n being deployed in coexistence with

802.11a/g. The mixture of 802.11n and non-802.11.n clients and access points means that often both 802.11n clients and 802.11a/g clients will be associated to the same access point, or will be operating in the same RF space. When 802.11n was created, this situation was anticipated and the standard was designed to permit operation in a mixed environment.

802.11 PHY and Clients

A number of different physical layer (PHY) mechanisms exist within the 802.11 standard; HR/DSSS for 802.11b, ERP for 802.11g, OFDM for 802.11a and High Throughput (HT) OFDM for 802.11n. To ensure that clients, referred to in the IEEE 802.11n standard as stations (STA), can operate properly in mixed environments, the 802.11 standard specifies that STAs which support later amendments, e.g. HT (High Throughput), must also support previous PHY mechanisms. For example this means that an 802.11a/n STA must support OFDM as well as HT mode. 802.11n clients should therefore have no problems connecting to legacy access points and roaming between 802.11n and 802.11a/g domains. However, clients operate as HT STAs when connected via 802.11n, and since non-HT clients cannot detect HT clients (because they don't recognise the HT PHY method) there is the danger of both clients transmitting simultaneously. Therefore, other protections are needed to ensure that clients do not interfere with each other.

Operating Mode

To ensure that HT clients operating in a mixed environment are detectable by non-HT clients, a number of operating modes exist. The operating mode is set by the access point, based upon the types of clients that are identified to it. HT access points advertise information about which types of clients are operating in the environment through setting the 'Operating Mode', 'Non Greenfield STAs Present' and 'OBSS Non-HT STAs Present' fields in the Information Element (IE). The 'Non Greenfield STAs Present' field indicates 802.11a/b/g clients are detected. The 'OBSS Non-HT STAs Present' field indicates a neighbour (overlapping) access point has non-HT clients. The four different operating modes are:

- Mode 0: All STAs are capable of HT (either 20MHz or 40MHz). In this case the HT Greenfield Preamble may be used (i.e. not compliant with non-HT STAs).
- Mode 1 (HT non-member Protection Mode): Non-HT STAs are visible (clients or access points) using either the primary or secondary (for 40 MHz) channels.
- Mode 2: All STAs are capable of HT but some clients are 20MHz capable only.
- Mode 3 (non-HT Mixed Mode): Used when non-HT STAs are connected to the access point.

If mode 1 or 3 is selected by the access point, and 802.11 (DSSS) or 802.11b (HR/DSSS) are present, the 'Use_Protection' field is set in the ERP Information Element. This means that HT clients must use RTS/CTS or CTS-to-self protection to prevent inference with legacy clients. The protection frames must be sent at 802.11 / 802.11b PHY rates.

When mode 3 is selected, HT transmissions are protected. If mode 3 is selected and the 'Use_Protection' field is not set (i.e. there are no 802.11 or 802.11b clients), the HT STA can use 1 of 5 different protection mechanisms:

- RTS/CTS

- CTS-to-self
- L-SIG TXOP
- Initial TXOP then (upon response) HT Greenfield and/or RIFS
- HT mixed format preamble: transmit a frame that requires a response.

The selected mechanism depends upon what is supported by the STAs. All of these protection methods will cause reduced throughput due to the overhead of the protection frames, some more so than others. The use of L-SIG TXOP can result in overheads of as little as <0.5%. However, use of RTS/CTS and CTS-to-self results in particularly high overheads and reductions in throughput. The overheads for these methods, depending upon the PHY rate and other factors such as aggregation, could be between 7-88% (see http://www.nle.com/literature/Airmagnet_impact_of_legacy_devices_on_80211n.pdf [1])

Deployment Considerations

20MHz or 40MHz

When deploying 802.11n a decision needs to be made whether or not to use 40MHz wide channels. In the 5GHz part of the 802.11a/n spectrum the use of 40MHz channels does not pose a problem, given the large number of available channels (in Europe there are nine non-overlapping 40MHz channels). However, it should be noted that most of these channels are in the UNII 2 extended range, which is subject to interference from RADAR i.e. the access point will stop using a channel if RADAR is detected.

In the 2.4GHz part of the 802.11g/n spectrum, however, it is recommended that only 20MHz wide channels be used due to the limited number of non-overlapping channels. Using 40MHz channels would inevitably lead to channel clashes when attempting to design a WLAN to provide wireless coverage in all but the simplest buildings.

Using 40MHz channels in the presence of 20MHz-only clients should not pose a problem, as access points will automatically change to mode 2 when required.

WPA2/AES

To support 802.11n HT clients wireless network must be either open access or WPA2/AES. WPA/TKIP is not supported within 802.11n. For sites which currently have a mixed mode (WPA/TKIP, WPA2/AES) environment this is an important consideration. Some clients may need to have their wireless drivers updated to support WPA2.

Gigabit Switches

As 802.11n provides greater bandwidth to clients, access points require gigabit connections to the wired infrastructure. This needs to be taken into consideration when planning an 802.11n deployment. Previously with 802.11a/g deployments, many sites purchased specific Power over Ethernet (PoE) switches for their access points. This could mean that a single switch, with a gigabit uplink, supported 10 access points before becoming over subscribed, as each access point only required 100Mbit/s. However, as each 802.11n access point can potentially require up to 444.4Mbit/s (g/n client and a/b both at MCS 15), a single 1Gbit/s uplink becomes over subscribed after two access points are connected. In new build situations, or in areas of

heavy usage, access points can be distributed over multiple switches, or switches could be uplinked at 10Gbit/s. However, in many instances it may not be economically viable to upgrade switches to eliminate oversubscription. In these instances it may be pragmatic to accept the over subscription, particularly in areas where the access point utilisation is expected to be low.

Site Surveys

The characteristics of 802.11n wireless signal propagation are quite different from that of 802.11a/g. This is due to a number of different techniques such as MIMO technology, beam forming and different MCS rates. This means that the number and location of 802.11n access points may vary in comparison to traditional 802.11a/g deployments. Therefore, it is vital that when surveying an area for 802.11n networking, the survey equipment is also 802.11n. Additionally the survey access points should be of the same type as will form the installation. This is due to variation between 802.11n access points caused by differences such as the number and type of antennas e.g. 3x2 vs. 3x3. Also when upgrading areas with existing 802.11a/b/g deployments, it is most beneficial to resurvey the area using 802.11n access points to ensure that the desired coverage will be achieved.

Links
[1] http://www.nle.com/literature/Airmagnet_impact_of_legacy_devices_on_80211n.pdf