Disabling 802.11b

IEEE 802.11b is one of the oldest WiFi standards still in use and is beginning to show its age. IEEE 802.11b products first started to appear in 1999. Now, more than a decade since its first appearance, the time is approaching for IEEE 801.11b to be turned off, for the reasons detailed below. As this may not be immediately possible for some sites, possible transition and migration strategies are also described below.

Throughput

The 802.11b standard was developed many years before 802.11g and consequently there are some interoperability issues. The main problem stems from the different physical (PHY) mechanisms used to connect to the network. The PHY mechanism for 802.11g is ERP-OFDM (Orthogonal Frequency Division Multiplexing) whereas DSSS (Direct Sequence Spread Spectrum) is used for 802.11b. This means 802.11b clients are unable to recognise any data, management or control traffic of 802.11g clients operating in the same frequency space. Therefore, to allow both 802.11b and 802.11g clients to operate in the same space, 802.11g has to implement backwards compatibility through protection mechanisms. If an 802.11b client connects to an 802.11g access point, the access point will set the “Use_Protection” field in the ERP Information Element (IE). This means that any 802.11g clients connecting to the access point will use Request-to-Send/Clear-to-Send (RTS/CTS) or CTS-to-self, over DSSS, before transmitting data. Unfortunately using RTS/CTS and CTS-to-self adds a significant amount of overhead to client data transmission; this in turn reduces throughput. An 802.11g client connecting in a pure 802.11g environment can expect a throughput of between 22–36Mbps. In comparison an 802.11g client using CTS-to-self will achieve approximately 12–13 Mbps and an 802.11g client using RTS/CTS will achieve 8 Mbps.

Security

Throughput, although important, is not the only consideration when supporting 802.11b clients. There are also security considerations. Use of encryption and authentication is commonplace at most sites. Most sites will use WPA or WPA2 for encryption and 802.1X authentication for wireless clients. When 802.11b was developed, WEP was the only encryption scheme available for wireless networking. As WEP was based on the RC4 encryption algorithm, 802.11b devices don’t support AES encryption and WPA2. Some older adapters may not even be WPA/TKIP capable. It is also likely given the age of 802.11b devices (at least 5 years old) that manufacturers may have stopped updating drivers, leading to a lack of support for WPA and 802.1X. This means that many 802.11b clients are incapable of connecting to WPA/WPA2 protected networks and network access services such as eduroam.

Is disabling 802.11b feasible?

Given the age of the protocol and the limitations arising from legacy support, site

administrators should therefore seriously consider whether they need to

support 802.11b clients. The replacement for 802.11b, 802.11g, was first standardised in 2003. The number of 802.11b devices at a site is likely to be very low and any remaining devices in use are likely to be close to or past their usable lifespan. Given that the vast majority of client devices should now be 802.11a/g/n, the disadvantages of supporting 802.11b outweigh the need for legacy support.

To gauge whether it is feasible to drop legacy support, individual institutions should conduct surveys to see how many 802.11b clients exist on their wireless networks. Based upon the results, a strategy on how to proceed can be planned.

The ultimate aim should be to remove support for 802.11b. However, there may be an interim support period while remaining 802.11b clients are replaced with newer 802.11a/g/n equipment. Sites with legacy 802.11b devices which can’t be immediately upgraded can implement migration schemes to balance 802.11g performance versus 802.11b support. Meanwhile sites with a large number of access points could remove support for 802.11b from sections of the network. For example if particular buildings or areas never have any 802.11b clients connected, their 802.11b support could be turned off. In areas where 802.11b clients are known to operate, support for 802.11b could be removed from half of the access points. As long as the 802.11g-only access points are operating on different, non-overlapping channels to the access points which still support 802.11b, there should be no problems. Eventually a point should be reached when all remaining 802.11b devices can be removed from the network and support for 802.11b can be removed fully.
