



Northern Territory Government

Department of Employment, Education and Training

Northern Territory Schools

Wireless Network Standards

Version: 1.3 - May 2006



Contents

Policy Approval	2
Overview.....	3
Introduction	3
Scope.....	3
Related Documents.	3
Contacts for policy change	3
Policy statement.....	4
Installing Wireless Networks	5
Planning Considerations.....	5
Fixed Access Points	5
Mobile (Roaming)	5
Bridging.....	5
Building to building networks	5
Installing Wireless Networks	6
Data Transfer speed	6
Control of radiation	6
Technical Support.....	6
Security Requirements.....	7
Security Requirements	7
Wireless Standards	8
802.11a.....	8
802.11b.....	8
Wireless Standards	9
802.11g.....	9
802.11g (Super G or Extreme G).....	9
Summary	9
Future directions	10
Wireless Standards	11

Policy Approval

This policy and the standards were approved by the DEET Information and Technology Management Committee in 8 March 2006 and is effective immediately.



Overview

Introduction

Wireless local area network (WLAN) services provide schools with more flexible and mobile options to connect computers to local area networks. There are two broad classes of wireless networks:

1. Wireless LANs (or wireless office) where devices such as laptop computers and PDAs connect via a radio-enabled network card.
2. Point to point or bridge connections that connect two or more wired (or fixed) networks.

Wireless LAN is not a replacement for wired LANs but rather supplementary to it. Wired networks are more secure, more reliable and offer a higher data transfer speed. Wireless connections generally do not offer the same level of bandwidth as fixed connections and some applications will not work effectively in a wireless environment, e.g. the SAMS database could become corrupted if the wireless connection is lost during database updates. Because this risk is unacceptable, DEET IT Services Division (ITSD) advise that a wireless connection should NOT be used if you are updating SAMS records.

Wireless networks can also pose a significant security risk because by the very nature of the technology, it is possible for people outside of schools premises to gain access to the network and intercept network traffic.

This document establishes the minimum authentication and encryption measures that must be applied to stop unauthorised access to school networks and information.

The intended audience is School Principals, ICT Coordinators and vendors who maybe considering application of WLAN technology within an NT School.

Scope

Sets out the minimum requirements for any new wireless network equipment connected to an NT Government School local area network. It also provides guidance on the considerations that should be taken into account when establishing a WLAN.

Related Documents.

- ◆ NT Government Wireless Office Standards
- ◆ NT Government Wireless Bridge Networks

http://www.nt.gov.au/dcis/it/it_policies/

Contacts for policy change

Changes in technology and school requirements will require ongoing updates to this policy. For queries or recommended changes please contact the DEET ITSD.

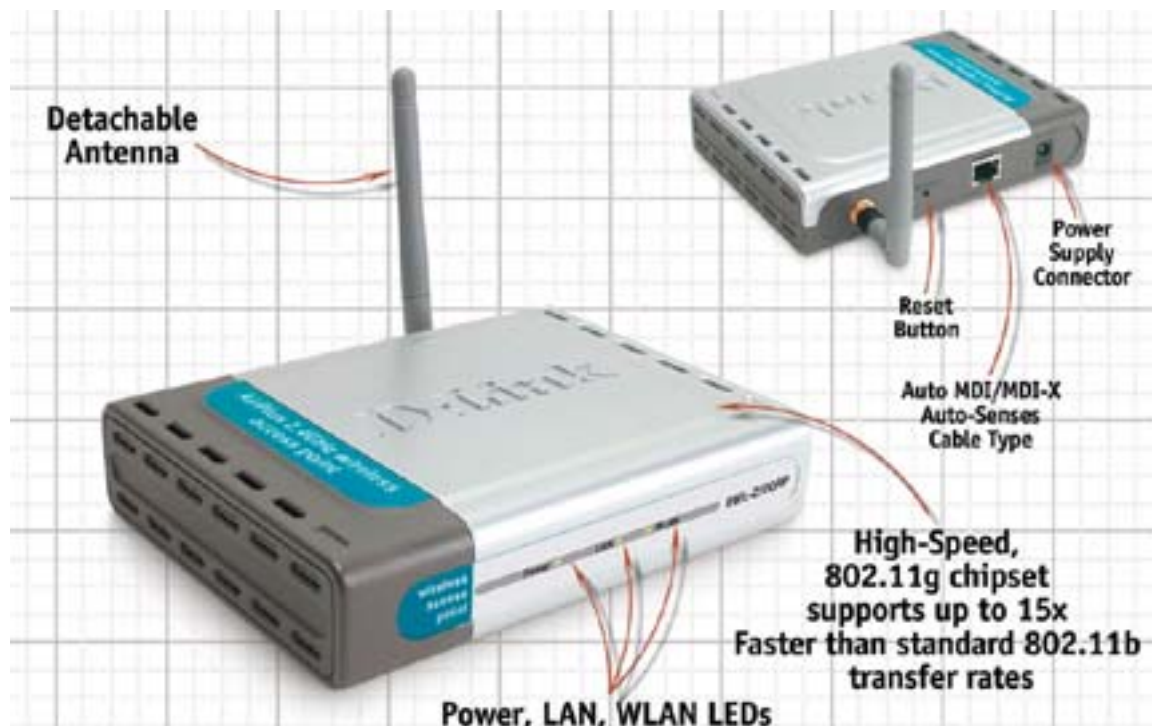


Policy statement

The following standards and configuration settings shall be applied for all new wireless data networks that are connected to NT Government School local area networks.

Wireless local area networks must meet the following requirements:

- Meet either the IEEE 802.11 Wi-Fi or 802.16 Wi-Max standards
- Wi-Fi Protected Access (WPA) using Pre-Shared Key mode.
- SSID broadcast disabling.
- Secure management through the use of Secure HTTP (HTTPS) or Secure Shell (SSH).
- Access Point management filtering (to ensure management connections are not possible from the wireless network).
- Clear channel select (automatic channel selection).
- Variable power output.
- Client limit of at least 256 clients.
- The use of multiple VPN's, using 802.1x / 802.1q.
- Antennae used for cellular connectivity should be restricted where possible to cover only the necessary areas. External antennae are not permitted.



Picture courtesy of D-Link Australia

Parts of a Wireless Access Point



Installing Wireless Networks

Planning Considerations

Design of the network is critical for effective wireless installation. Access Points are provided with software to perform a "site survey" where the best position with the strongest signal can be located and documented. Considerations when locating APs include such things as mounting APs high enough to cover up to three floors in buildings with wooden floors, installing APs away from steel surroundings such as portables or filing cabinets and selecting the correct wireless channels to enable roaming profiles and load share.

Wireless networks can suffer from radio-interference from other devices (like microwave ovens, and cordless telephones, etc.), and performance can collapse when too many users attempt to use the same access point.

Equipment has to be located to provide 'line of sight' to a base station.

The DEET Infrastructure Services Group must be consulted for and building alterations required to install fixed access points.

Fixed Access Points

The fixed access point provides and base station or "Hotspot" which connects the mobile devices to the fixed network. Several fixed access points can be link together to form a larger network that allows "roaming".

Fixed access points can be placed in the room of inside wall or roof cavities. Multiple access points can be installed with overlapping ranges to support larger numbers of users and allow roaming from one base station to the next. This is more expensive and requires careful planning.

Mobile (Roaming)

The mobile access point is installed on the computer, laptop or PDA and connects the device to the fixed access point. These can be provided with a network or USB card and are standard on all new laptops. The optima laptops provided to teachers have a 802.11b wireless capacity.

Bridging

Wireless bridges are used for connecting two or more physically separate network segments.

Building to building networks

Wireless bridges can be used in two types of implementation, they are point to point link or point to multi point.

To set up bridge networks all the bridges must be set on the same service set identifier (SSID), radio channel and WAP or other authentication mechanism.



Installing Wireless Networks

Data Transfer speed

Data transfer speeds will typically not be as good as in a wired network. All users of the same base station have to share the bandwidth (typically 11Mb/s or 54Mb/s) whilst those wired to a switch typically get almost the full 100Mb/s. Also, wireless data rates degrade rapidly with signal strength/interference.

If a low speed mobile device (i.e. a laptop with a 11Mb/s wireless card) connects to a high speed fixed access point (e.g. 54Mb/s) the connection will run at the lower speed.

Control of radiation

A site survey should be used to establish the actual coverage of the access points to minimise interference to and from other nearby wireless services based on the survey findings. While the security of the network should not depend on an attacker's inability to intercept the wireless signal, the steps mentioned should also help to minimise the opportunity for electronic eavesdropping.

Technical Support

Support for wireless networks will be a school's responsibility. All access points must be managed by either the school ICTC, by CSM Technology or by another service provider.

IT Services Division can provide advice to schools when they are looking to implement a wireless solution and we encourage all schools to contact us for advice in this area.



Security Requirements

Security Requirements

- All new wireless access points shall comply with the TKIP/WPA or standard or higher, preferably 802.11i.
- Access Points shall have WPA encryption turned on with a minimum of a 20 character Pre-Shared key. This key should be changed once a year.
- WPA keys are to be documented and held securely by and administered only by the local authorised contact.
- Broadcast of the SSID must be disabled for all access points. This measure adds an extra layer of obstruction for potential intruders to penetrate.
- MAC address filtering shall be implemented for access points that cannot support WPA or TKIP encryption.
- Wireless bridge networks must be installed and managed by a qualified service provider.



Wireless Standards

802.11a

IEEE 802.11a was designed to operate in the 5GHz spectrum enabling it to avoid much of the interference in the 2.4GHz spectrum produced by other wireless devices and consumer electronics. It provided a higher throughput than previously available, 54Mbps, with an actual throughput of 27Mbps.

It also had the advantage of providing 13 non-overlapping channels for clear transmissions. 802.11a suffered from problems with wireless coverage and the lack of an upgrade path between cheaper 802.11b equipment using 2.4GHz spectrum to the 802.11a equipment using the 5GHz spectrum.

Since 802.11a allows for a greater number of operating clear channels, and is not common in iterated wireless devices, it is recommended this technology be used for infrastructure or building to building mode of operation. This will allow for reliable links connecting either wired or wireless devices in a target location.

802.11b

IEEE 802.11b allows a raw transmission rate of up to 11Mbps and is able to select the best data rate ranging from 1, 2, 5.5 or 11Mbps depending on signal strength.

In an ideal scenario the raw frame rate of 11Mbps corresponds to a data throughput rate of 5-6 Mbps.

802.11b provides three non-overlapping channels which provide space for transmissions that do not interfere with each other. It is also the default component of many personal computers, laptops and Personal Digital Assistants.

This may eventually limit some of the usefulness of the technology. With the increase in the number of consumer devices (microwaves, portable phones, etc.) which use the same wireless frequency (2.4GHz), the ability to get long range transmissions without significant loss of signal strength may become increasingly difficult.



Wireless Standards

802.11g

IEEE 802.11g had the main advantage of being able to provide the same speed as 802.11a (54Mbps) but operated in the 2.4GHz frequency range and was also backward compatible with the current 802.11b 11Mbps hardware.

Any 802.11b client can connect to a 802.11g Access Point. 802.11g is limited by the overcrowding and interference from other devices in the 2.4GHz spectrum and the limit of three overlapping channels.

Due to its compatibility with 802.11b, 802.11g is recommended for cellular and wireless client access networks.

802.11g (Super G or Extreme G)

Super G is a group of performance enhancement features that increase the speed of data transfer in an 802.11b/g and 802.11a/g network. These features include Dynamic Packet Bursting, Fast Frames, Hardware Compression and Encryption, and Multi-channel 108 Mbps Mode.

The four features operate independently to enhance the rate of data transfer in a network.

Performance will vary according to the network environment, but the delivered performance should be significantly better than designs that implement any single performance feature, such as bursting-only.

Extended Range transmission technology is designed to provide increased wireless signal range as well as fewer dead spots. It is compatible with all IEEE802.11g and IEEE802.11b products.

In order for the technology to work, all devices on the network must support this standard.

Summary

The following is a summary of the levels of performance expected from each of wireless standards:

Standard	Over the Air estimates	Actual through Put
802.11a	54Mbps	25Mbps
802.11b	11Mbps	5Mbps
802.11G	54Mbps	25Mbps
802.11N	200+ Mbps	100Mbps



Future directions

802.11n

The wireless 802.11n isn't an official standard as yet. The 802.11n committee are in the final stages of voting in a standard.

The main difference between this new proposed standard and the current 802.11b will be faster speed and better coverage.

One of the main aims of the 802.11n standard is to have 100Mbps through put after all the Wireless overheads. So this will be a true 100Mbps speed

Other major differences will be more antennae. Currently the 802.11a/b/g standard uses just one antenna. A second antenna is added for diversity configuration which is used to improve the reception, not double the bandwidth.

Using three antennae enable the signal to be broken up into three and transmitted more efficiently. Each antenna will be capable of transmitting and receiving. This technology is known as MIMO (Multiple-Input/Multiple-Output).

One of the proposed wireless standards will support backward compatibility with 802.11b/g.

At the moment there are many vendors selling pre N standard wireless devices. There is a risk that the pre N standard equipment not being compatible with the final N standard hardware.

For large scale deployments, many companies are holding off until the official standard has been approved, and evening waiting until the price of such equipment comes down in price. When 802.11n becomes the official standard , it will be affordable for everyone, whereas 802.11a and b was well out of everyone's reach when they first hit the market.

Wireless USB (WUSB)

Currently there are over 2 Billion wireless USB devices used in the world. The USB standard was made popular by Apple. USB is faster than the serial connectors and enables more than one device to be connected at the same time.

First came USB1, then later USB2 and Wireless USB. Wireless USB is faster than USB2 and doesn't require physical connectors.

Wireless USB will work like Bluetooth technology. It is not designed for running over long distances like 802.11a/b/g/n , but for short range. Approximate speed will be 480Mbps at 10 meters. This is very fast compared to any other wireless standards, and will enable users to transfer video/audio and data at much faster speeds than before.

Wireless USB will be low power device and only run when it's actually needed.



Wireless Standards

Additional Information

The documents supplied with the equipment are an essential guide, however further information regarding wireless technology and how to set up a wireless network can be obtained from many sources, but some that we recommend are:

Queensland Department of Education

<http://education.qld.gov.au/corporate/doem/commuman/cm-20000/wireless.html>

Victorian Department of Education and Training

<http://www.sofweb.vic.edu.au/ict/lan/wireless.htm>

Vicomsoft

<http://www.vicomsoft.com/knowledge/reference/wireless1.html>

Netcomm

http://www.netcomm.com.au/Wireless/about_wireless.php

PC World

<http://www.pcworld.idg.com.au/index.php/id;1395397229>