Chapter 3 – WLAN TECHNOLOGIES

In the early 1970's, the success of the Ethernet project at Xerox's Palo Alto Research Center as well as of other similar digital protocols brings the Local Area Networks (LANs) technology in both the public and corporate sectors. Standard LAN protocols, such as Ethernet, that operate at fairly high speeds bring digital networking to almost any computer. However, LANs are limited to the physical and hard-wired infrastructure of the buildings. The origins of wireless networking standardization can be traced to the late 1980s, motivated by FCC spread spectrum regulations in the 2.4 GHz range. In the 1990's, it has been shown that many network users and, more especially, mobile users in business, medical profession, factories and universities could find benefit from the Wireless LANs (WLAN) capabilities.

The installation of traditional wired LAN is not always practical or feasible (e.g. in old buildings, in factory floors, in trading floors, in trade shows, at conferences…). Therefore, in many cases, WLAN offers the connectivity and the convenience of wired LAN without the need for expensive wiring or re-wiring. Additionally, WLANs present the advantage to combine both the power of the wireless access and the mobile computing delivering high data rates. The major motivation and benefit of WLANs is the increased mobility and flexibility that it is offered to the user.

The primarily application of WLANs as a mean of connecting computers, has been stretched to larger applications. Presently, the market and target segments of the WLANs are seen as being corporate, public access and home/consumer product environments.

As mentioned previously, WLANs are also penetrating the hospital and university environments in which users are highly mobile.

The demand in wireless networks in home, known as Home Networking, is poised for take-off. The homes with multiple computers are looking for ways to communicate among computers and share resources such as files, printers and broadband Internet connections. Consumer oriented electronics devices such as games, phone are being added to home WLANs. The home networks will have to deliver multiple services and support a broad variety of media and computing devices as part of a single network.

In corporate/business environments, WLANs have a big potential. As for example, employees could bring laptop computers together to communicate and share professional information in an ad-hoc network configuration. The ad-hoc network configuration would allow any group of people to connect together without having to be connected via an access point to a wired network (infrastructure network).

More and more, the mobile professionals are looking for:

- Ubiquitous, available wireless public access to the Internet (IP) and to corporate intranets.
- Broadband speeds that could respond to their demand for data-intensive applications.
- Security and Privacy.
- Reasonable access charges.
- Consolidated Internet access billing per trip.

Indeed, the most valuable assets for those users would be to access remotely through the IP backbone, which would require typically high bandwidth (e.g. e-mail attachment downloading). Presently, this large data transmission exceeds the cellular networks capacity and WLANs is a perfect broadband complement for the operator's existing GSM and GPRS services in an indoor environment to answer to the strong demand for public wide-area Internet access. As such, WLANs could be considered as a public wireless

broadband access technology. However, current WLANs products offer limited global user management features as well as modest authentication and roaming capabilities compared to traditional cellular networks. The security and privacy issues are seen as a bottleneck for the realization of public WLANs as well as the ability of public WLAN operators to provide coverage areas for potential users, which would also imply roaming between the operators.

Wireless interworking is also gaining high interest and is of major importance for seamless interoperability between the networks. Recently, Ericsson announced its GPRS-WLAN interworking solution to enable users to roam seamlessly between Wide-Area mobile Networks (Wireless WANs) and WLAN networks without interruption. With their H2U project, Telenor and Ericsson are also active in interworking between UMTS and WLAN. AT&T labs are looking more particularly to Internet Roaming and proposed an IP-based integrated architecture that provides seamless interworking across WLAN and cellular technologies and the IEEE 802.11 study groups (e.g. convergence/interworking on WLANs/WWANs) as well as ETSI HIPERLAN type 2 are addressing the wireless interworking aspects.

Appropriate WLAN architectures still have to be developed to allow all these capabilities. Actually, a high-data rate European standard (ETSI H/2) has been designed in that sense, to enable this interworking. Other working groups (more particularly the IEEE 802.11e working group) are working on proposals to support Quality of Services (QoS) and multimedia in their WLAN specifications. As already mentioned, this interworking is extremely important in the willingness to offer seamless interoperability between business, home and public environments. QoS and multimedia-capable networks are essential ingredients to offer residential customers video-on-demand, voice over IP (multimedia applications) and high-speed Internet access, which are of interest for broadband service providers.

The present and future WLAN terminal penetration creates a high business opportunity for mobile operators to extend their services to cover WLAN access. In the following, a brief presentation of the existing WLAN chipset and products is made and compared to the other wired and not-wired solutions on the market. Afterwards, the future potential services and the market forecast are covered more specifically to present the market potential and to underline the needs for WLAN service deployments by the service providers.

3.1 THE IEEE 802.11 FAMILY OF STANDARDS

The IEEE 802.11 family is an extension of Ethernet to wireless communication. It supports TCP/IP, but also handles other forms of networks like IPv6 for enhanced mobile IP features. There are two physical layer standards: 802.11b operating in the 2.4 GHz radio band and 802.11a operating in the 5 GHz radio band. Products complying with 802.11b go through market in 2001. Products complying with 802.11a started to appear in North America toward the end of 2001. In many other countries, including those in Europe, regulators of radio spectrum block the use of 11a products operating in the 5 GHz radio band. A third physical layer specification, 802.11g, is in the final stages of being defined.

Other 802.11 standards (802.11c, d, e, f, g, h, i) extend the physical layer options, improve security, add quality of service (QOS) features or provide better interoperability. These are discussed below. Vendors proprietary implementations exist, in some cases before the IEEE has finalized the relevant standards.

The set of the IEEE 802.11 protocols and evolution are given below in the context of the layered model.

Table 3-1: WLAN Layered Model

<table>
<tr><td rowspan="3">MAC</td><td rowspan="3">802.11
MAC</td><td>802.11 e
MAC Enhancements – QoS</td><td rowspan="7"></td></tr>
<tr><td>802.11f
Access Point Interoperability</td></tr>
<tr><td>802.11i
Enhanced Security Mechanisms</td></tr>
<tr><td rowspan="4">PHY</td><td>Infrared (IrDA)</td><td>802.11 IrDA (1/2 Mbps)</td></tr>
<tr><td>2.4 GHz (FHSS)
Frequency Hopping Spread Spectrum</td><td>802.11 FHSS (1/2 Mbps)</td></tr>
<tr><td rowspan="2">2.4 GHz (DSSS)
Direct Sequence Spread Spectrum</td><td>802.11 DSSS (1/2 Mbps)</td></tr>
<tr><td>802.11b Extension
(5.5 / 11 Mbps)</td><td>802.11g
>20 Mbps</td></tr>
<tr><td rowspan="2">5 GHz (OFDM)
Orthogonal Frequency Division Multiplexing</td><td rowspan="2">802.11a
6/54 Mbps Extension</td><td>802.11h
Spectrum Management</td></tr>
<tr><td>5 GHz
Globalization</td></tr>
</table>

Main technical 802.11 characteristics are as follows:

- Bandwidth: Originally 1,2 Mbps (BPSK and QPSK), then CCK 5.5 and 11 Mbps.
- Asynchronous, connectionless service.
- Supports both ad-hoc and infrastructure mode operation.
- Spread Spectrum without requiring licensing.
- Three Physical Layer Implementations: **Direct Sequence Spread Spectrum** (DSSS), **Frequency Hopping Spread Spectrum** (FHSS), 915 MHz, 2.4 GHz (Worldwide ISM), 5.2 GHz, and **Diffused Infrared** (850 – 900 nm) bands (see more below).
- Multiple priorities supports.
- Time-critical and data traffic support.
- Power management allows a node to doze off.

3.1.1 IEEE 802.11b

One of the most used WLAN technologies is defined in IEEE 802.11b. The standard was completed in 1999 and a wide range of products exists since 2001. For radio access this standard defines three Frequency Hopping CDMA coded channels in unlicensed 2,4 GHz frequency band. It allows the wireless transmission of approximately 11 Mbps of raw data at distances from tens up to hundred meters. The distance depends on impediments, materials, and line of sight while the transmission rate depends strongly on usage of common unlicensed radio channel. Most wireless LAN installations today comply with 802.11b, which is also the basis for Wi-Fi certification from the Wireless Ethernet Compatibility Alliance (WECA).

The problem with this technology is unsatisfactory security. Many severe weaknesses in Wired Equivalent Privacy (WEP) have been identified, which is supposed to secure WLAN communication but does not deliver what its name implies.

The initial version of the IEEE 802.11b achieves only 1 Mbps with BPSK and 2 Mbps with QPSK over both FHSS (Frequency Hopping Spread Spectrum) and DSSS (Direct Sequence Spread Spectrum). The task group for 802.11b was responsible for enhancing the initial 802.11 DSSS PHY to include 5.5 Mbps and 11 Mbps data rates to finalized the standard (IEEE Std. 802.11b-1999) in late 1999. At present FHSS is not longer used. To provide the higher data rates, 802.11b uses CCK (Complementary Code Keying), a modulation technique that makes efficient use of the radio spectrum.

It utilizes Direct Sequence Spread Spectrum (DSSS).

- Higher-Speed Physical Layer Extension of 802.11 in the 2.4 GHz Band.
- Use High Rate Direct Sequence Spread Spectrum (HR/DSSS).
- HR/DSSS uses the same PLCP preamble and header as DSSS, so both PHYs can co-exist in the same AP.
- Multirate: 1, 2, plus 5.5 and 11 Mbps, rate switching mechanism.
- Use Complementary Code Keying (CCK) modulation with 8 chip for high rates.

The DSSS provides an immunity of the WLAN signal from the noisy ISM band of the 2.4 GHz. The major interferences for the WLAN are the microwave ovens and other industrial applications.

The main DSSS characteristics employed are:

- Spreading factor = Code bits/data bit, 10 – 100.
- Commercial (Min 10 by FCC), 10,000 for military.
- Signal bandwidth >10 × data bandwidth.
- Code sequence synchronization.
- Correlation between codes.
- Signal modulated with a spreading code (11-bit Barker Sequence).
- All 802.11b compliant products use the same spreading code.
- Higher data rates because of “fatter pipe” (about 11 MHz).
- Allows for some single frequency noise and higher wideband noise.
- Only allows for 3 networks in same area.
- Uses higher power to transmit and more expensive to build than FHSS.
- Differential Binary Phase Shift Keying (DBPSK) for 1 Mbps, Differential Quadrature Phase Shift Keying (DQPSK) for 2 Mbps.

The Multiple Access Scheme employed has the following features:

- Two access methods: Distributed and Point Coordination Function.
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).
- Not all stations can hear each other (hidden station problem).

- CA: Listen before you talk. If the medium is busy, the transmitter backs off for a random period. However CA cannot detect collision, hence each packet is acked. If not acked, MAC level retransmission occurs.
- Avoids collision by sending a short message: Ready To Send (RTS), which contains source/ destination addresses and duration of message. Destination then sends Clear To Send (CTS) and all stations receiving RTS and/or CTS set their timer.
- NAV (Network Allocation Vector) for the given duration.

Two Supported Topologies exist: Ad-hoc and Infrastructure.

3.1.2 IEEE 802.11a

IEEE 802.11a defines an updated version of 802.11b standard in order to achieve higher data rates and enhanced security. The standard has been completed in 1999 and products are available now. The 802.11a uses 8 – 12 available radio channels in the low – medium UNII frequency band at 5.2 GHz and achieves data throughput up to 54 Mbps. Products based on the IEEE's 802.11a standard cannot interoperate with slower 802.11b units because they run on different bands. The 802.11a standard is using Orthogonal Frequency Division Multiplexing (OFDM). 802.11a supports data rates ranging from 6 to 54 Mbps.

Because of operation in the 5 GHz bands, 802.11a offers much less potential for radio frequency (RF) interference than other PHYs (e.g. 802.11b and 802.11g) that utilize 2.4 GHz frequencies. With high data rates and relatively little interference, 802.11a does a great job of supporting multimedia applications and densely populated user environments. This makes 802.11a an excellent long-term solution for satisfying current and future civilian requirements.

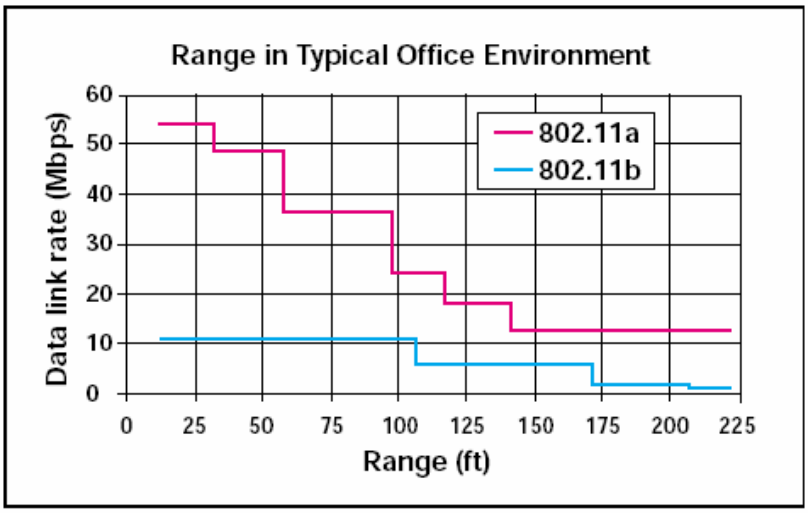
It specifies 8 available radio channels (available radio spectrum in some countries would permit the use of 12 channels – the US 5 GHz Unlicensed Band supports 12 non-overlapping 802.11a networks).

The benefits of 802.11a are:

- Significantly higher data rates, up to 54 Mbps.
- Operating at comparable range and faster speeds than 802.11b.
- Allows users to perform bandwidth intensive applications without sacrificing throughput.
- Increased scalability, better interference immunity.
- 802.11a supports many more channels (8 non-overlapping instead of 3 with 802.11b).
- OFDM modulation scheme.
- Within a channel, the 20 MHz spectrum is divided into 52 "narrowband carriers" each about 300 KHz, based on OFDM technology.
- The high data rate is accomplished by combining many lower-speed subcarriers to create one high-speed channel.

Table 3-2: IEEE 802.111/b Characteristics

Characteristic	*802.11b*	*802.11a*
Spectrum	2.4 GHz	5 GHz
~Max physical rate	11 Mbps	54 Mbps
~Max data rate, layer 3	5 Mbps	32 Mbps
Medium access control/Media sharing	CSMA/CA	CSMA/CA
Connectivity	Wireless	Wireless
Multicast	Yes	Yes
QoS support	(PCF) *	(PCF) *
Frequency selection	DSSS	Single Carrier (OFDM)
Authentication	No	No
WEP Encryption	64-bit RC4	128-bit RC4
Handover support	(NO) **	(NO) **
Fixed network support	Ethernet	Ethernet
Management	802.11 MIB	802.11 MIB
Radio link quality control	No	No



Source: Atheros Communications Inc.

Figure 3-1: WLAN Range.

3.1.3 Bridge Operation Procedures with 802.11c

IEEE 802.11c is a set of instructions named "Support of the Internal Sub-layer Service by Specific MAC Procedures to cover bridge operation with IEEE 802.11 MACs". It will not be published as a separate document.

802.11c provides required information to ensure proper bridge operations. This project is completed, and related procedures are part of the IEEE 802.11c standard. Product developers utilize this standard when developing access points. This standard is not of primary concern to wireless LAN installers.

3.1.4 Global Harmonization with 802.11d

IEEE 802.11d promotes worldwide use of 802.11 WLANs. It will allow access points to communicate information on the permissible radio channels with acceptable power levels for user devices. The 802.11 standards cannot legally operate in some countries; the purpose of 802.11d is to add features and restrictions to allow WLANs to operate within the rules of these countries.

When 802.11 first became available, only a handful of regulatory domains (e.g. U.S., Europe, and Japan) had rules in place for the operation of 802.11 wireless LANs. In order to support a widespread adoption of 802.11, the 802.11d task group has an ongoing charter to define PHY requirements that satisfy regulatory requirements within a group of additional countries. This is especially important for operation in the 5 GHz bands because the use of these frequencies differ widely from one country to another.

In countries where the physical layer radio requirements are different from those in North America, the use of WLANs is lagging behind. Equipment manufacturers do not want to produce a wide variety of country-specific products nor do users accept the need to cope with several country-specific WLAN PC cards. The outcome will be country-specific firmware solutions.

As with 802.11c, the 802.11d standard mostly applies to companies developing 802.11 products.

Work is ongoing, but see 802.11h for a timeline on 5 GHz WLANs in Europe.

3.1.5 Enhancements for QoS with IEEE 802.11e MAC

IEEE 802.11e is a supplementary to the MAC layer to provide QoS support for LAN applications. It will apply to 802.11 physical standards a, b and g. Its purpose is to provide classes of service with managed levels of QoS for data, voice and video applications.

Without strong quality of service (QoS), the existing version of the 802.11 standard is not optimized for the transmission of voice and video. There is a lack of effective mechanism to prioritize traffic within 802.11. As a result, the 802.11e task group is currently refining the 802.11 MAC (Medium Access Layer) to improve QoS for better support of audio and video (such as MPEG-2) applications. The 802.11e group should finalize the standard by the end of 2002, with products probably available by mid-2003.

Because 802.11e falls within the MAC Layer, it will be common to all 802.11 PHYs and be backward compatible with existing 802.11 wireless LANs. As a result, the lack of 802.11e being in place today does not impact a decision on which PHY to use. In addition, the aim is to offer upgrades of existing 802.11 access points to comply with 802.11e through relatively simple firmware add-ons.

3.1.6 An Inter Access Point Protocol with IEEE 802.11f

IEEE 802.11f is a “recommended practice” document that aims to achieve radio access point interoperability within a multivendor WLAN network. The standard defines the registration of access points within a network and the interchange of information between access points when a user is handed over from one access point to another.

The existing 802.11 standard does not specify communications between access points in order to support users roaming from one access point to another. The 802.11 WG purposely did not define this element in order to provide flexibility in working with different distribution systems (i.e. wired backbones that interconnect access points). Hence access points from different vendors may not interoperate when supporting roaming. The inter access point protocol is the scope of 802.11f so as to provide the necessary information that access points need to exchange to support the 802.11 distribution system functions

(e.g. roaming). The 802.11f group expects to complete the standard by the end of 2002, with products supporting the standard by mid-2003.

3.1.7 Higher Rate Extensions in the 2.4 GHz Band with IEEE 802.11g

802.11g is an extension to 802.11b. The 802.11g task group aims to develop a higher speed extension (up to 54 Mbps) to the 802.11b PHY, while operating in the 2.4 GHz band. 802.11g will implement all mandatory elements of the IEEE 802.11b PHY standard. For example, an 802.11b user will be able to associate with an 802.11b access point and operate at data rates up to 11 Mbps. In early 2002, 802.11g decided to use OFDM instead of DSSS as the basis for providing the higher data rate extensions. A big issue with 802.11g, which also applies to 802.11b, is considerable RF interference from other 2.4 GHz devices, such as the newer cordless phones.

The transmitted signal uses approximately 30 MHz, which is one third of the band. This limits the number of non-overlapping 802.11g access points to three, which is the same as 802.11b.

The FCC (Federal Communications Commission) still needs to approve the use of OFDM in the 2.4 GHz band. As a result, it will likely take a relatively long period of time before 802.11g products appear on the market.

Because of the earlier time to market and superior performance capacity, 802.11a rather than 802.11g will likely dominate the high performance WLAN market in the near-term and distant future.

Benefits:

- Includes all of 802.11b plus higher speed options based on new baseband;
- Enhanced Speeds 24, 36, 48, 54 Mbps;
- Enhanced Modulation –OFDM (same as 802.11a); and
- Spectrum 2.4 GHz.

3.1.8 Spectrum Managed 802.11a with 802.11h

IEEE 802.11h standard is supplementary to the MAC layer to comply with European regulations for 5 GHz WLANs. European radio regulations for the 5 GHz band require products to have transmission power control (TPC) and dynamic frequency selection (DFS). TPC limits the transmitted power to the minimum needed to reach the furthest user. DFS selects the radio channel at the access point to minimise interference with other systems, particularly radar.

802.11h addresses the requirements of the European regulatory bodies. It provide dynamic channel selection (DCS) and transmit power control (TPC) for devices operating in the 5 GHz band (802.11a). In Europe, there's a strong potential for 802.11a interfering with satellite communications, which have "primary use" designations. Most countries authorize WLANs for "secondary use" only. Through the use of DCS and TPC, 802.11h will avoid interference in a way similar to HiperLAN/2, the European-based competitor to 802.11a. 802.11h hopes to have their standard finalized sometime before the end of 2003.

To implement DCS and TPC, 802.11h is developing associated practices that affect both the MAC and PHY Layers. The inclusion of DCS and TPC will likely enable 802.11h to become the successor to 802.11a. Fortunately, there shouldn't be any issues of non-interoperability between existing 802.11a and 802.11h users and access points. The good news is that 802.11h is enabling sales of 802.11a networks in Europe, which will eventually result in higher sales volumes and lower prices.

A fast-dwindling group will continue to support the alternative HyperLAN standard defined by ETSI. Although European countries such as The Netherlands and the United Kingdom are likely to allow the use of 5 GHz LANs with TPC and DFS well before 11h is completed, pan-European approval of 11h is not expected until the second half of 2003, possibly longer.

The standard is expected to be finalized by the second half of 2002. Products will be available in the first half of 2003 (firmware implementation), with high availability in the second half of 2003 (0.7 probability).

3.1.9 MAC Enhancements for Enhanced Security with 802.11i

IEEE 802.11i is a supplementary to the MAC layer to improve security. It will apply to 802.11 physical standards a, b and g. It provides an alternative to WEP with new encryption methods and authentication procedures.

As a conclusion over IEEE 802.11 standards it should be noticed that wireless communication is always more vulnerable and less reliable than its wired counterpart. Especially when using commonly available unlicensed frequencies the coverage of all possible communicating devices must be considered. Many technological obstacles must be overcome in order to achieve needed throughput with acceptable security. The familiar and widely used WLAN is good example of that. In practical networks many test have shown that actual throughput won't be more than half of promised bit rate. Many security flaws have been found. To enhance the technology to meet the needs for better throughput and security many new additional standards have been introduced.

802.11i is actively defining enhancements to the MAC Layer to counter the issues related to wired equivalent privacy (WEP). The existing 802.11 standard specifies the use of relatively weak, static encryption keys without any form of key distribution management. This makes it possible for hackers to access and decipher WEP-encrypted data on your WLAN. 802.11i will incorporate 802.1x and stronger encryption techniques, such as AES (Advanced Encryption Standard).

It is not expected 802.11i to be available in the near future. The standard will likely not have IEEE ratification before mid-2003. 802.11i updates the MAC Layer, so you should be able to upgrade existing access points with firmware upgrades. The implementation of AES, however, may require new hardware.

For now, stronger forms of security that go well beyond WEP by implementing proprietary security mechanisms available from access points vendors. The problem is that you'll probably need to deploy network cards and access points from the same vendor. As a minimum, utilize WEP.

The 11i specification is part of a set of security features that should address and overcome these issues by the end of 2002. Solutions will start with firmware upgrades using the Temporal Key Integrity Protocol (TKIP), followed by new silicon with AES (an iterated block cipher) and TKIP backwards compatibility.

Finalization of the TKIP protocol standard is expected in the first half of 2002. Firmware will be available in the second half of 2002 (0.8 probability). The second half of 2003 expects new silicon with an AES cipher.

3.2 A BACKUP WIRELESS LAN FOR THE CZECH ARMY

3.2.1 Introduction

This chapter describes development steps on the way from the decision to the realization of new LAN communication facilities in the battlefield environment. These steps were made by Military Technical

Institute of Electronics in Prague ("VTÚE Praha") during 2000 – 2001 years and were made in the frame of the giant and long-term project dedicated to the Czech Ground Forces Tactical Command and Control System (GF-TCCS).

One of the sub-task was find solution how to use the latest communication technologies on behalf of the modernization of the current Theater Operation Centers (TOC) on the Battalion level. The final goal was to design and realize one prototype of TOC using new LAN/WLAN technology.

These TOCs are designed on the base of shelters (topologically relatively isolated) on mobile platform (in vehicles). Each TOC consists of four (or more, max. 7) shelters (vehicles), which should be logically (one IP address space) connected together with versatile LAN by using fiber optics (FO), metallic cables and wireless technology (as a "warm" backup of FO). The fifth vehicle has special function and serves as an access node to support the communication to the upper operation level (to the Brigade via IP routers with ISDN/BRI interfaces).

Projected LAN is base on basic~~s~~ NATO standards (for example STANAG 4290 – NATO Multi-channel Tactical Digital Gateway – Cable Link (Optical) Standards) – to ensure interoperability and to fulfill high transfer rates for all possible types of data transfers (primary data, voice only in the case of using FO segments). These requirements led to the structure described below.

The structure of LAN consists of two types of LAN segments: internal LAN segments and external LAN segments. Internal segments of LAN are based on UTP or STP (twisted pairs) cables (10BaseT or 100BaseT) and are located inside the shelters. External LAN segments are FO (100(1000) Base FX, or 10Base FL) or WLAN and must be weather resistant. In the case of external LAN segments we decided to use FO (Fiber Optics) technology (base on STANAG 4290) with combination of WLAN (IEEE 802.11b).

Main requirements to the external LAN segments are following:

- FO LAN should be primary communication medium and should have the highest "communication" priority.
- Wireless technology should serve as "warm" backup of FO cables.
- WLAN "segments" should maintain rapid functionality of LAN after taking positions of shelters in terrain.
- FO and wireless technology must coexist and switching between them must be automatic.

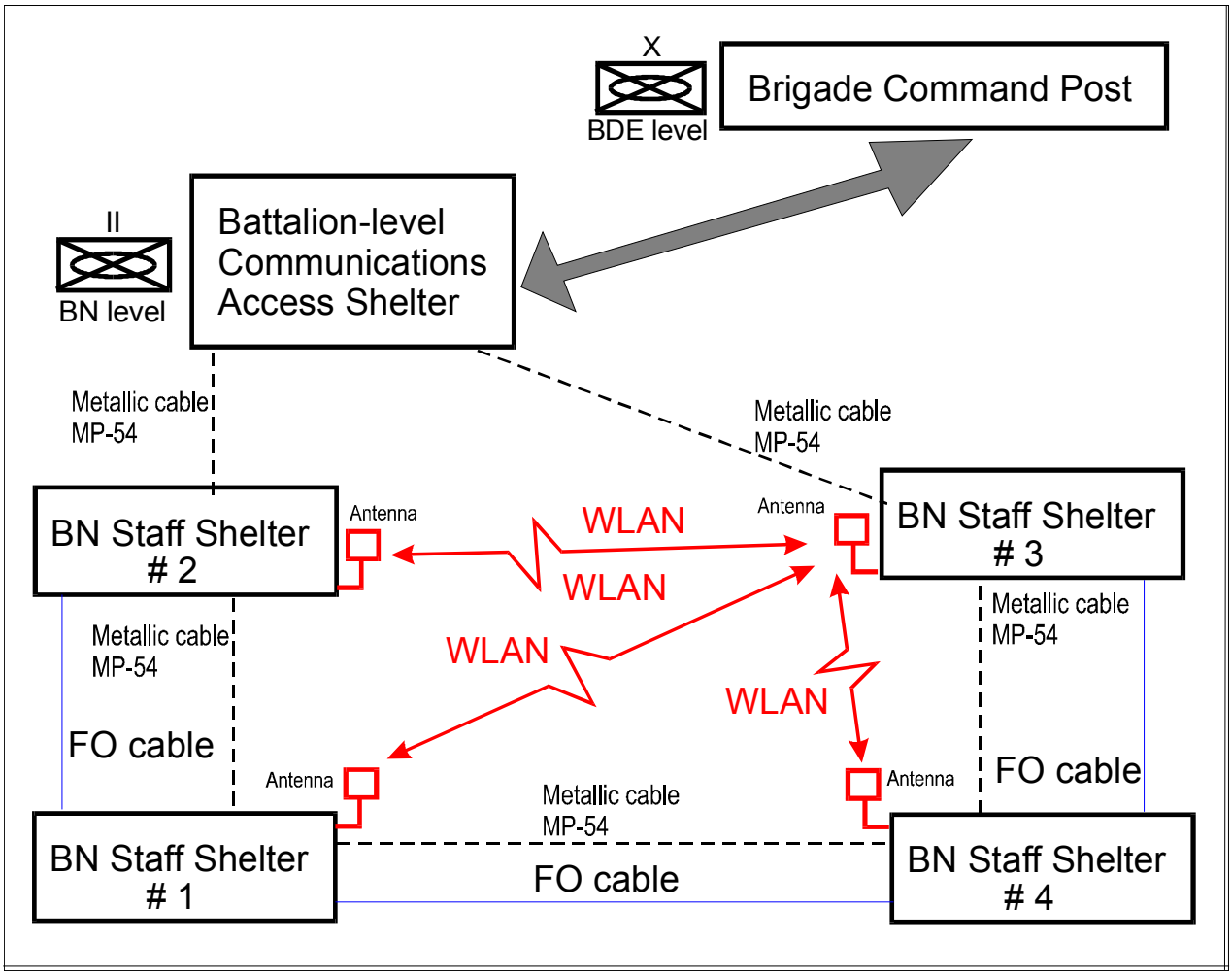


Figure 3-2: Battalion TOC LAN External Segment Layout (Simplified).

Remark: Metallic cables MP-54 between staff shelters (#1 – #2, #1 – #4, #3 – #4) serve to the analog telephones and as a transport medium for another legacy communication means.

In the case of communication between staff shelter #2 and communications access shelter (or between staff shelter #4 and communications access shelter) is the situation quite another. Here are metallic cables MP-54 used for two independent ISDN/BRI interfaces between Cisco routers (located in staff shelters #2, #3) and ISDN PABX (located in communication access shelter).

3.2.2 WLAN Step 1 – What is Available on the Market? Choosing COTS (Commercial Off The Shelf) Technology

The system architect and communication designer first considered to use the COTS technology "Bluetooth", but the too short range (less then 10 m) was against the usage of it. (Staff shelters on Battalions TOCs could be more distant, the typical theoretical distance is approx. 500 m, but as will describe later, this factor wasn't been fulfilled).

The second possibility was to use "pure" IEEE 802.11b standard WLAN technology in spite of the fact, that typical range is from tens up to hundred meters and depends on environment (trees, bushes, etc.) and materials in line of sign visibility.

Cisco Aironet WLAN appliances of series 340/350 (wireless bridge and wireless workgroup bridge) has been chosen for the experiments, but it was necessary to test the range (with directional and omni-directional antennas) in the real terrain before using of Aironet bridges in the field.

3.2.3 WLAN Step 2 – Distance and Reliability Measurement of Chosen Technology

The measurement should discover affect of bush and trees to the effective range of Aironet 340 with external antennas (omni-directional or directional).

Following three criteria of measurement were appointed:

- Criterion A: Level of signal measured by diagnostic utilities of Aironet system.
- Criterion B: Reliability of data transfers during transmission of 20 Mbytes long files.
- Criterion C: Error rate and average effective data rate.

Following equipment were used to the measurement:

- 2 pieces of WLAN bridges Cisco Aironet 340.
- 2 pieces of notebooks with Ethernet port 10 Mbit (10BaseT).
- 2 pieces of omni-directional antennas S24003BP (3 dB).
- 2 pieces of directional antennas HGY-15 (11,3 dB/30°).
- Antenna cables (6 m and 15 m).

There were chosen one common “typical” type of vegetation during spring season (without leaves) with following description:

- Wild leafy wood (hornbeam, beech).
- Quite dense (but person can go through).
- Dense branches in the height approx. 2 m above the earth.
- Diameter of trunks from 5 to 15 cm.

The testing place was prepared in a following manner:

- Both antennas (directional and omni-directional) were mounted on poles 2.5 m high to imitate the roof of vehicles.
- One place was used as **stationary measurement point** (with presence of experimentalists).
- The second place was used as **mobile point** with the notebook with hard disc (mapped as shared).
- Transmit rate was fixed at 11 Mbit/s.

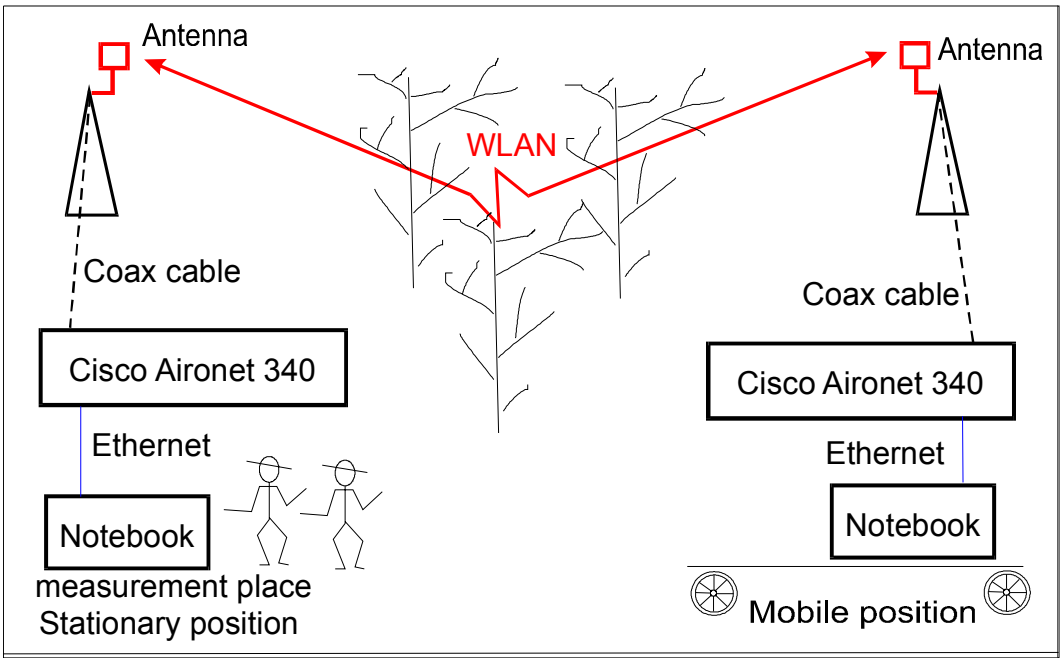


Figure 3-3: Diagram of Apparatus in the Terrain.

First measurement of range was done **in free space** (in the terrain without impediments of vegetation). Both points (stationary and mobile, **distance 160 m**) were equipped by **omni-directional antennas**. Results are here:

- Criterion A: with 50 mW output level of signal – without noticeable loss of signal.
- Criterion A: with 5 mW output level of signal (on both sides) – loss of signal to 50%.
- Criterion B: transfer of file (by 5 mW) was always successful.
- Criterion C: error factor = several dozens of bytes / 20 Mbytes, effective transfer rate 470 Kbytes/s.

Second measurement of range was done in the terrain **"through" the vegetation**. Both points (stationary and mobile) were equipped by **omni-directional antennas** too. Results are here:

- Criterion A: with 20 mW output level of signal by distance 30 m was noticeable loss of signal, with 50 mW by distance 40 m was loss of signal to 50%.
- Criterion B: Unstable file transfer with drop outs, transfer was very often timed out due to loss of synchronization of radio parts of Aironets.
- Criterion C: error factor was approximate 3% from 20 MB file, effective transfer rate around 100 kbytes/s.

Third measurement of range was done in the terrain **"through" the vegetation**. Both points (stationary and mobile) were equipped by **directional antennas** and by using **full output power 50 mW**. Results are here:

- Criterion A: loss of signal 50% in distance of 120 m.
- Criterion B: transfer of file was always successful.
- Criterion C: error factor = several hundreds of bytes / 20 Mbytes file, effective transfer rate around 450 kbytes/s.

Fourth measurement of range was done in the terrain "through" the **vegetation (sporadic bush)**. Both points (stationary and mobile) were equipped by **omni-directional antennas** and by using **full power 50 mW**. Results are here:

- Criterion A: loss of signal 50% in distance of 40 m.
- Criterion B: transfer of file was always successful.
- Criterion C: error factor = several hundreds of bytes / 20 Mbytes file, effective transfer rate around 450 kbytes/s.

The measurements (described above) led to following conclusions:

- Vegetation has drastic impact on range especially by using omni-directional antennas.
- Range of omni-directional antenna is influenced much more by trunks of trees then by thin branches of bush (difference is in accidental drop outs not in the level of signal).
- Range of directional antennas in density vegetation is more then 100 m.
- If vehicles (shelters) are grouped to the close quarters – is using of omni-directional antennas more practical (especially by the central vehicle).
- For standalone vehicles (shelters) would be good to use mechanical robust directional antennas.

In spite of the fact, that the range of WLAN (based on Cisco Aironet series 340/350) was in ideal case (free terrain without vegetation) about 160 m and in the worse case (vegetation) about 40 m, system architect and communication designer decided to use WLAN on technological platform IEEE 802.11b for prototype of TOC on battalion level. The advised tactical distance about 500 m between staff shelters wasn't been fulfilled, but there wasn't another technical solution (how to do the WLAN backup of FO) in that time.

3.2.4 WLAN Step 3 – Realization Details

All LAN and all segments (internal and external) of prototype of TOC were build on the base of following components (basic building blocks):

- **Ethernet switches Catalyst 3500XK**. Each staff shelter was equipped by this switch. This switches were a hearts of Ethernet LAN 100Base-T in each shelter and built so internal LAN segments. On this LAN segments where connected two servers (in shelter #1 and #3) and a lot of PCs (notebooks) Compaq Armada (or notebooks Getac A-760). External FO cables as well as the Aironet bridges 340/350 were connected to these switches. The "warm" backup logic of switching from FO to WLAN (and vice versa) was built in these switches.
- **TCP/IP routers Cisco 2620** with ISDN/BRI interface were install in staff shelters #2, #3 to establish communication from command post to higher level via communication access point.
- **WLAN Cisco Aironet components** (standard IEEE 802.11b), 3 pieces of Cisco Aironet 340/350 **wireless workgroup bridges with antennas**, 1 piece of Cisco Aironet 340/350 **multi-functional bridge (access point) with antenna.**
- **FO cables for distances up to 500 m** (100 Mbit/s, 100BaseFX, standard IEEE 802.3).
- **FO cables for distances up to 2 km** (10 Mbit/s, 10BaseFL).
- Another special equipment inside the staff shelters:
    - two PC dedicated as **graphics workstations** (in shelters #1 and #3);
    - **color laser printer** (format A3) in shelter #1;

- three **monochromatic laser printers** (A4 format) in shelters #2, #3, #4;
- **data projector** – (operable in external or internal space) of shelter #2; and
- **interactive Smart Board** (in shelter #2).

All of shelters were equipped by **standard telephones** (2 pieces), **cable cross-connects** and **external cable panels.**

3.2.5 Conclusion

All above described experiments and measurements tried to answer to the basic question: "Is WLAN (following "pure" standard IEEE 802.11b) usable in military field environment (in real terrain) as an backup of FO cables?". The indisputably true answer is **No** (without some reasonable changes).

One problem is the **carrier frequency** (around 2.4 GHz, band of "microwave ovens") that is not a true military frequency band. Much more convenient would be to use the WLAN in military VHF/UHF bands around 225 – 380/400 MHz.

Another problem is the **maximal usable range** of IEEE 802.11b that is typically around 100 m. Some experts advise to use **lower frequency** – typically around 300 MHz. In this band (with the same output power of transmitter) we can prolong the range approximately ten times.

From tactical point of view it is necessary to consider that the distance of staff shelters should be around 500 m. In the ideal case the field "military" WLAN should have the typical range around 1000 m or a little bit more in the terrain with vegetation effects.

To prolong the range of WLAN we can **slow down the bit rate** from 11 Mbit/s to 1 Mbit/s and this bit rate is still sufficient for some modest military applications (but it is too little as an full backup of FO bit rate capacity).

Another way to prolong the range of "military" WLAN is to use **more HF output power** of transmitters. To use not only 50 mW or 100 mW, but 1 W or more.

Protection of military information in the point of security is another topic that is necessary to consider in the WLAN in field environment. But it goes above the frame of this testbed description.

Almost all here mentioned technical adaptations of WLAN for military application were proposed and described in Paper A-23: "Wireless Tactical Local Area Network" by Prof. Torleiv Maseng (Norway).

Figure 3-4: Detail View of Omni-Directional Antenna for WLAN on the Roof of Staff Shelters.

Figure 3-5: External Cable Panel with Connected FO Cable (on the reel).

Figure 3-6: External Cable Panel – Detailed View.

Figure 3-7: Connection of External Notebook GETAC with Data Projector to Shelter Cable Panel.

3.3 AN 802.11B RELATED EXPERIMENT AT FFI IN NORWAY

The purpose of the experiment was to increase the range of the WLAN cards.

In order to gain experience with the IEEE 802.11b cards, we made some small changes to a commercial card:

- We fixed the data rate to 1 Mbit/s. These cards are designed to work at 1, 2 5.5 and 11 Mbit/s adaptively depending on link propagation conditions. Ideally, we would like to reduce the rate, but this turned out to be tricky. We expect the coverage results to be improved and the rate to be increased if we had managed to reduce the rate.
- By disabling the diversity switch between two antennas on the card, we were able to convert the input and output frequency to around 300 MHz by an external oscillator and mixers.
- We increased the output power from 50 mW to 3 Watts.

Figure 3-8: WLAN Experiment in FFI.

The WLAN card was equipped with two antenna connectors to provide diversity. These were used to transpose the carrier frequency from 2.45 GHz to 300 MHz. The adaptive bit rate was disabled and locked to 1 Mbit/s. The connectors on the left provide Ethernet and power. Extra equipment containing power, frequency converters and power amplifier is not visible.

Figure 3-9*:* FFI Experiment.

On the figure two antennas can be seen. The white was used for experiments at 2.45 GHz and the green whip antenna (hardly visible in the center roof of the car) was used for 300 MHz.

3.3.1 Measurements

Measurements were made 17/4-2001 with two cars. One was acting as a transmitter and the other as a receiver. The link-analysis was done using a software computing package error rate (PER). The packages were send-using UDP (which is connectionless).

3.3.2 Specifications

Measured sensitivity at receiver: -99 dBm.

Output power: 3 W (35 dBm)

Data rate: 1 Mbit/s.

Package length: 1000 bytes.

Packages/second = 62

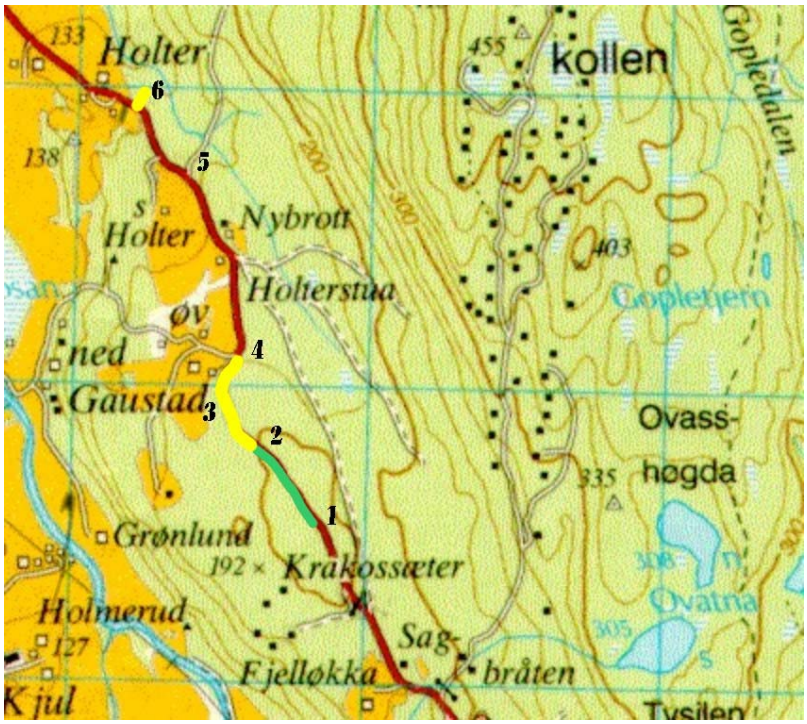


Figure 3-10*:* FFI Experiment – Route.

PT. 1: This position is just before the top of a small hill. The second car remained at Pt. 1 until Pt. 5.

PT. 2: The second car with the receiver drove from 1 to 2. Result: PER < 1% (green). Signal strength was better than -56 dBm. The distance between 1 and 2 is about 300 m with fairly dense wood.

PT. 3: From 2 and 3 is downhill. While signal strength is well above sensitivity limit since it was better than -73 dBm, the PER is varying between 0 and 100% (yellow), which indicates multipath problems. Maximum altitude difference was about 10 m.

PT. 4: Between 3 and 4 PER varies between 80 and 100%. Signal strength was –75 dBm and the distance between transmitter (at PT. 1) and receiver (at PT. 4) was now up to 600 m.

PT. 5: The measurements between PT. 5 and 6 in very dense wood. The second car was now stationary at PT. 5. The distance between the vehicles was now all the time around 200 m (indicated by yellow). Signal strength = -60 dBm. PER varies between 0 and 100%.

These measurements indicate that this system is very sensitive to multipath. With a rate reduction by a factor 8 this should be less of a problem.

Most of the features above are acceptable and even attractive in a tactical LAN, but not all. Assuming that an external crypto unit performing authentication and encryption can improve the security features, and the ESM and jamming threat can be accepted, it is still desirable to increase the range. Reducing the bit rate of IEEE 802.11b by a factor of 8, will improve the power budget and make the system able to handle longer multipath which otherwise would be a problem when the range is increased. Reducing the carrier frequency from 2.435 to 300 MHz will improve the range, in particular in forest. Besides, it is for many applications no problem to increase the transmit power. The result will be an increase in range by a factor of 10!

A continuation of this project is carried out by several nations. Some of the effort is reported at http://www.nc3a.nato.int/mwlan.html.