



**NAVAL  
POSTGRADUATE  
SCHOOL**

**MONTEREY, CALIFORNIA**

**THESIS**

**STUDY OF WIRELESS TRANSMISSION PROTOCOL  
TECHNOLOGY FOR USE IN FLIGHT LINE  
ENVIRONMENT TO ASSIST THE DATA UPLOADING  
AND DOWNLOADING ON AIRCRAFT**

by

Ow Keong Meng

March 2004

Thesis Advisor:  
Second Reader:

Bert Lundy  
Donald V. Z. Wadsworth

**Approved for public release, distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

<b>REPORT DOCUMENTATION PAGE</b>			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
<b>1. AGENCY USE ONLY (Leave blank)</b>		<b>2. REPORT DATE</b> March 2004	<b>3. REPORT TYPE AND DATES COVERED</b> Master's Thesis	
<b>4. TITLE AND SUBTITLE:</b> Study of Wireless Transmission Protocol Technology for Use in Flight Line Environment to Assist the Data Loading and Downloading on Aircraft			<b>5. FUNDING NUMBERS</b>	
<b>6. AUTHOR(S)</b> Ow Keong Meng				
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> Naval Postgraduate School Monterey, CA 93943-5000			<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>	
<b>9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> N/A			<b>10. SPONSORING/MONITORING AGENCY REPORT NUMBER</b>	
<b>11. SUPPLEMENTARY NOTES</b> The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
<b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b> Approved for public release, distribution is unlimited			<b>12b. DISTRIBUTION CODE</b>	
<b>13. ABSTRACT (maximum 200 words)</b> Presently, the required data file to be loaded onto the Radar Warning Receiver (RWR) onboard the F-16 aircraft is done manually by the aircraft technicians, two to three hours prior to the actual flight time. This process should be automated. As such there is a need to look into the use of wireless transmission technology to complement or replace the manual method of loading the critical data file from the command station onto every F-16 aircraft. The present wireless technology is relatively mature and stable. In this thesis, the feasibility of incorporating and adapting this technology for use in the flight line environment is examined. The propagation effect in wireless transmission is also studied and recommendations proposed with regards to the installation of wireless facilities in the flight line. In addition, the EDNA, a portable maintenance aid that comes with the F-16 aircraft for loading the data file, has to be upgraded. Hence, a system feasibility study is carried out to adapt or upgrade the present equipment to wireless transmission capability.				
<b>14. SUBJECT TERMS</b>  IEEE 802.11b, EDNA, WLAN, FSO, Wireless Transmission Protocol, Radar Warning Receiver, Aircraft, F-16.			<b>15. NUMBER OF PAGES</b> 141	
			<b>16. PRICE CODE</b>	
<b>17. SECURITY CLASSIFICATION OF REPORT</b> Unclassified	<b>18. SECURITY CLASSIFICATION OF THIS PAGE</b> Unclassified	<b>19. SECURITY CLASSIFICATION OF ABSTRACT</b> Unclassified	<b>20. LIMITATION OF ABSTRACT</b> UL	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)  
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release, distribution is unlimited**

**STUDY OF WIRELESS TRANSMISSION PROTOCOL TECHNOLOGY FOR  
USE IN FLIGHT LINE ENVIRONMENT TO ASSIST THE DATA UPLOADING  
AND DOWNLOADING ON AIRCRAFT**

Ow Keong Meng  
Major, The Republic of Singapore Air Force  
Bachelor of Engineering (Hons), Nanyang Technological University, Singapore, 1995  
Master of Science (Communication and Network Systems), Nanyang Technological  
University, Singapore, 2002

Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF SCIENCE IN SYSTEMS ENGINEERING**

from the

**NAVAL POSTGRADUATE SCHOOL  
March 2004**

Author: Ow Keong Meng

Approved by: Bert Lundy  
Thesis Advisor

Donald V. Z. Wadsworth  
Second Reader

Dan Boger  
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

Presently, the required data file to be loaded onto the Radar Warning Receiver (RWR) onboard the F-16 aircraft is done manually by the aircraft technicians, two to three hours prior to the actual flight time. This process should be automated. As such there is a need to look into the use of wireless transmission technology to complement or replace the manual method of loading the critical data file from the command station onto every F-16 aircraft. The present wireless technology is relatively mature and stable. In this thesis, the feasibility of incorporating and adapting this technology for use in the flight line environment is examined. The propagation effect in wireless transmission is also studied and recommendations proposed with regards to the installation of wireless facilities in the flight line. In addition, the EDNA, a portable maintenance aid that comes with the F-16 aircraft for loading the data file, has to be upgraded. Hence, a system feasibility study is carried out to adapt or upgrade the present equipment to wireless transmission capability.

THIS PAGE INTENTIONALLY LEFT BLANK



# TABLE OF CONTENTS

<b>I.</b>	<b>INTRODUCTION.....</b>	<b>1</b>
<b>A.</b>	<b>BACKGROUND .....</b>	<b>1</b>
<b>B.</b>	<b>OBJECTIVE OF STUDY .....</b>	<b>1</b>
<b>C.</b>	<b>APPROACH.....</b>	<b>2</b>
<b>D.</b>	<b>OVERVIEW .....</b>	<b>3</b>
<b>II.</b>	<b>F-16 AIRCRAFT AND ALR-69 SYSTEMS OVERVIEW.....</b>	<b>5</b>
<b>A.</b>	<b>OVERVIEW OF F-16 AIRCRAFT .....</b>	<b>5</b>
<b>B.</b>	<b>F-16 EVOLUTION .....</b>	<b>6</b>
<b>C.</b>	<b>F-16 C AND F-16 D.....</b>	<b>11</b>
<b>D.</b>	<b>ALR-69 (RADAR WARNING RECEIVER) SYSTEM OVERVIEW .....</b>	<b>15</b>
<b>III.</b>	<b>IEEE 802.11 WIRELESS TECHNOLOGY OVERVIEW .....</b>	<b>21</b>
<b>A.</b>	<b>OVERVIEW .....</b>	<b>21</b>
<b>B.</b>	<b>BRIEF HISTORY OF IEEE 802.11 WIRELESS PROTOCOL.....</b>	<b>21</b>
<b>C.</b>	<b>FREQUENCY SPECTRUM FOR IEEE 802.11 WIRELESS PROTOCOL.....</b>	<b>25</b>
<b>D.</b>	<b>DIFFERENT IEEE 802.11 WIRELESS STANDARDS.....</b>	<b>26</b>
<b>1.</b>	<b>IEEE 802.11 Original.....</b>	<b>26</b>
<b>2.</b>	<b>IEEE 802.11b.....</b>	<b>26</b>
<b>3.</b>	<b>IEEE 802.11g.....</b>	<b>27</b>
<b>4.</b>	<b>IEEE 802.11a.....</b>	<b>28</b>
<b>E.</b>	<b>HOW DOES IT WORK .....</b>	<b>30</b>
<b>1.</b>	<b>Access Points.....</b>	<b>31</b>
<b>2.</b>	<b>Wireless Client Adapter .....</b>	<b>31</b>
<b>F.</b>	<b>WIRELESS LAN CONFIGURATIONS .....</b>	<b>33</b>
<b>1.</b>	<b>Independent Wireless LANs .....</b>	<b>33</b>
<b>2.</b>	<b>Infrastructure Wireless LANs .....</b>	<b>34</b>
<b>3.</b>	<b>Micro Cells and Roaming.....</b>	<b>34</b>
<b>G.</b>	<b>WIRELESS LAN TECHNOLOGY OPTIONS .....</b>	<b>35</b>
<b>1.</b>	<b>Frequency Hopping Spread Spectrum (FHSS) [From 6].....</b>	<b>35</b>
<b>2.</b>	<b>Direct-Sequence Spread Spectrum (DSSS) [From 6] .....</b>	<b>36</b>
<b>3.</b>	<b>Orthogonal Frequency Division Multiplexing (OFDM) [From 8] .....</b>	<b>36</b>
<b>H.</b>	<b>SECURITY IN WIRELESS LAN .....</b>	<b>36</b>
<b>I.</b>	<b>CONSIDERATIONS FOR WIRELESS NETWORKING.....</b>	<b>38</b>
<b>1.</b>	<b>Range and Coverage.....</b>	<b>38</b>
<b>2.</b>	<b>Throughput.....</b>	<b>38</b>
<b>3.</b>	<b>Integrity and Reliability .....</b>	<b>38</b>
<b>4.</b>	<b>Interoperability with Wired Infrastructure .....</b>	<b>38</b>
<b>5.</b>	<b>Interoperability with Wireless Infrastructure .....</b>	<b>39</b>
<b>6.</b>	<b>Interference and Coexistence.....</b>	<b>39</b>
<b>7.</b>	<b>Simplicity and Ease of Use .....</b>	<b>39</b>
<b>8.</b>	<b>Security .....</b>	<b>39</b>

9.	Implementation Cost .....	40
10.	Scalability.....	40
11.	Battery Life for Mobile Platform .....	40
12.	Safety.....	40
IV.	<b>FREE-SPACE OPTICS TECHNOLOGY .....</b>	<b>41</b>
A.	<b>OVERVIEW .....</b>	<b>41</b>
B.	<b>BRIEF HISTORY OF FREE-SPACE OPTICS .....</b>	<b>43</b>
C.	<b>HOW FSO WORKS .....</b>	<b>44</b>
1.	Operating Frequency Band.....	44
2.	Description of the Transceiver.....	45
D.	<b>FSO IMPLEMENTATION ISSUES.....</b>	<b>47</b>
E.	<b>COUNTERING DIFFICULTIES.....</b>	<b>49</b>
F.	<b>FREE-SPACE OPTICS SECURITY .....</b>	<b>50</b>
G.	<b>ADVANTAGES OF USING FREE-SPACE OPTICS .....</b>	<b>51</b>
1.	High Speed Broadband Access .....	51
2.	Low Cost Bypass of Copper Infrastructure .....	52
3.	Rapid Deployment and Service Provisioning.....	53
4.	Improved Availability and Reliability .....	53
5.	Improved Scalability and Flexibility .....	53
6.	Creation of New Revenue Opportunities for Service Providers and Carriers .....	53
H.	<b>LIMITATIONS OF FREE-SPACE OPTICS .....</b>	<b>53</b>
V.	<b>PRESENT OPERATING CONCEPT AND PRESENT ENCOUNTERED PROBLEMS .....</b>	<b>55</b>
A.	<b>OVERVIEW .....</b>	<b>55</b>
B.	<b>BRIEF HISTORY OF REPUBLIC OF SINGAPORE AIR FORCE (RSAF) .....</b>	<b>55</b>
C.	<b>AIRBASES IN SINGAPORE .....</b>	<b>59</b>
D.	<b>BASIC LAYOUT OF FLIGHT LINE OPERATING ENVIRONMENT.....</b>	<b>60</b>
E.	<b>PRESENT OPERATIONAL CONCEPT (MAINTENANCE CREW'S ASPECTS) FOR LOADING CRITICAL DATA FILE ONTO THE ALR-69 SYSTEM ONBOARD THE F-16 AIRCRAFT.....</b>	<b>62</b>
1.	Operational Scenario of Loading Critical Data to EDNA Prior to ALR-69 System Onboard the F-16 Aircraft.....	65
2.	Timeline for Present Operational Workflow for RWR Uploading Team.....	67
F.	<b>POTENTIAL PROBLEMS IN PRESENT OPERATIONAL WORKFLOW FOR RWR UPLOADING TEAM.....</b>	<b>68</b>
1.	Long Time Required to Complete Uploading of RWR Critical Data File for One Squadron of Aircraft .....	68
2.	Limited Number of EDNA Directly Restricting the Number of RWR Loading Team.....	69
3.	Insufficient Number of EDNA in RSAF Inventory .....	69

4.	Time Wasted on Floppy Diskette Transfer and Traveling to the Aircraft.....	69
5.	Increased Risk of Military Vehicle Accident.....	69
6.	Human Fatigue is Crucial .....	70
7.	Security Considerations.....	70
8.	Insufficient Military Vehicles.....	70
<b>VI.</b>	<b>FEASIBILITY STUDY ON UPGRADING OF PRESENT SYSTEM TO INCLUDE WIRELESS TRANSMISSION CAPABILITY .....</b>	<b>73</b>
A.	SPECIFIC REQUIREMENTS .....	73
1.	User’s Requirements.....	73
2.	Hardware Specifications .....	75
B.	RATIONALE FOR SELECTION OF EITHER IEEE 802.11 OR FSO WIRELESS TECHNOLOGY .....	77
1.	Comparison of Suitability of IEEE 802.11 Wireless Technology Against FSO for the Upgrade in This Thesis Work.....	77
2.	Which IEEE 802.1x Standard to Use .....	78
C.	SELECTION OF EQUIPMENT FOR IEEE 802.11B WIRELESS TECHNOLOGY .....	81
1.	Access Points for the Infrastructure .....	81
2.	Network Interface Card (NIC) for the EDNA .....	83
D.	EMI/EMC OR ANY POSSIBLE INTERFERENCE WITH AIRCRAFT OR ARMAMENT SYSTEMS .....	84
E.	RECOMMENDATION FOR THE SETUP OF IEEE 802.11B WIRELESS CAPABILITY IN THE SQCP.....	85
1.	Recommendation of Mounting Point for Cisco Aironet® 1200 Series Wireless Access Point .....	85
2.	Installation of Cisco Aironet® 350 Series Client Adapter to the EDNA .....	87
3.	Network Diagram of the Newly Installed Wireless Access Point Integrated to the Intranet.....	88
<b>VII.</b>	<b>BENEFITS AFTER IMPLEMENTATION OF IEEE 802.11B .....</b>	<b>89</b>
A.	NEW OPERATIONAL CONCEPT AFTER INCORPORATING IEEE 802.11B WIRELESS TRANSMISSION CAPABILITY .....	89
1.	Sending of New Critical Data File to SQCP Directly .....	90
2.	Transfer of Critical Data File to EDNA Using Wireless Transmission Media Instead of Floppy Diskette.....	91
3.	RWR Uploading Team is Pre-Dispatched to Aircraft.....	91
4.	F-16 Aircraft Can Be Pre-Prepared to Save Time.....	91
5.	Signed-off the Aircraft Logbook for All Aircraft .....	92
B.	SIGNIFICANT TIME SAVING.....	92
1.	Save on Traveling Time.....	93
2.	Aircraft is Pre-Prepared.....	94
3.	Consolidation of Closing Paperwork .....	94
C.	BUDGET REQUIRED FOR NEW HARDWARE REQUIRED FOR THE WIRELESS TRANSMISSION CAPABILITY UPGRADE .....	95

D.	SECURITY [16] .....	95
1.	Change the Default Network Name (SSID).....	97
2.	Disable the SSID Broadcast in the AP Bacon.....	97
3.	Enabled Wired Equivalent Privacy (WEP).....	98
4.	Change Encryption Keys Periodically .....	98
5.	Enable MAC Filtering on APs.....	98
VIII.	CONCLUSION AND FUTURE WORK .....	99
A.	CONCLUSION .....	99
B.	FUTURE WORK.....	99
1.	EDNA Made Redundant .....	99
2.	Replace EDNA With Other COTS Equipment.....	100
3.	Critical Issue of Operational Support.....	100
APPENDIX A:	CISCO AIRONET® 1200 SERIES ACCESS POINT .....	103
A.	KEY FEATURES AND BENEFITS .....	104
B.	HARDWARE SPECIFICATIONS .....	105
C.	POWER REQUIREMENTS.....	108
D.	PHYSICAL AND ENVIRONMENTAL SPECIFICATIONS FOR CISCO AIRONET 1200 SERIES ACCESS POINT.....	109
E.	REGULATORY APPROVALS FOR CISCO AIRONET 1200 SERIES ACCESS POINT .....	109
APPENDIX B:	CISCO AIRONET® 350 SERIES CLIENT FOR THE EDNA.....	111
A.	ETHERNET SPEED AND IMPROVED RANGE .....	112
B.	ENTERPRISE-CLASS WIRELESS LAN SECURITY .....	112
C.	SPECIFICATIONS FOR CISCO AIRONET® 350 SERIES CLIENT ADAPTERS [FROM 16] .....	114
LIST OF REFERENCES	.....	119
INITIAL DISTRIBUTION LIST	.....	121

## LIST OF FIGURES

Figure 1 - EDNA Used on the F-16 Aircraft .....	2
Figure 2 - F-16 D Aircraft from the Republic of Singapore Air Force (RSAF).....	5
Figure 3 - General Dynamic’s (Now Called Lockheed Martin) 2 <sup>nd</sup> YF-16 Prototype .....	8
Figure 4 - Northrop YF-17 “Cobra” Prototype Aircraft .....	10
Figure 5 - Components of ALR-69 RWR System Produced by Litton .....	16
Figure 6 - Technical Specifications of EDNA by BAE Systems.....	18
Figure 7 - IEEE 802.11 and ISO Model .....	22
Figure 8 – Electromagnetic Frequency Spectrum.....	25
Figure 9 - DSSS Non-Overlapping Channels .....	27
Figure 10 - Various IEEE 802.11 Standards and Industry Players.....	30
Figure 11 - Typical Wireless LAN Configuration.....	31
Figure 12 - Radio Signals Traveling Over Different Paths [From 4] .....	32
Figure 13 - Independent Wireless LAN Configuration [From 5] .....	33
Figure 14 - Infrastructure Wireless LAN Configuration [From 5] .....	34
Figure 15 - Handing Off Between Access Points [From 5].....	34
Figure 16 – Visible Light Spectrum [From 8] .....	44
Figure 17 - Typical Link Head for FSO [From 9] .....	45
Figure 18 - Diagrammatic FSO Communication Layout [From 10] .....	46
Figure 19 - Impact of Fog and Bad Weather on the Operational Distance of a Free-Space Optics System [From 11] .....	48
Figure 20 - Beam Divergence [From 11].....	49
Figure 21 - Bypassing Copper Wire Infrastructure [From 12] .....	52
Figure 22 - Two of RSAF's Hunter Mk. 47s Taking Off [From 12] .....	56
Figure 23 - Crewmen Posed with a BAC 167 Strikemaster [From 12].....	56
Figure 24 - A Pair of Skyhawks In Formation. Aircraft 687 is a TA-4S Advanced Trainer With a Separate Canopy for the Instructor, a Feature that Makes the RSAF's TA-4 Unique in the World [From 12] .....	57
Figure 25 - RF-5E Tiger [From 12] .....	58
Figure 26 - Airbases in Singapore [From 15] .....	59
Figure 27 - Logo of Paya Lebar and Tengah Airbase Respectively .....	59
Figure 28 - Typical Layout of an Airbase.....	61
Figure 29 - RSAF’s Pilots and Aircraft Technicians Standing in Front of the F-16 Aircraft. Aircraft are Usually Parked Side-By-Side Close to the SQCP .....	62
Figure 30 – Technicians (Non RSAF) Loading Data File to the Aircraft Using EDNA.....	63
Figure 31 - Simplified Network Layout of Higher HQ Command and Various Airbases (a.k.a. Intranet).....	64
Figure 32 - Operational Workflow for RWR Uploading Team.....	66
Figure 33 - Timing Chart for Operational Events for RWR Uploading Team.....	67
Figure 34 - Network Diagram For Wired LAN Within an Airbase.....	76
Figure 35 - Comparison of Wireless LAN Standards – IEEE 802.11a Versus IEEE 802.11b (PC Magazine, May 21 2002).....	80
Figure 36 - Cisco Aironet® 1200 Series Access Point.....	82
Figure 37 - Cisco Aironet® 350 Series Client Adapter .....	84

Figure 38 - Recommended Location for Installing the Access Point in SQCP .....	86
Figure 39 - Cisco Aironet® Lightning Arrestor .....	87
Figure 40 – Cisco Aironet® 350 Series Client Adapter Installed in the PCMCIA Expansion Slot of the EDNA .....	87
Figure 41 - Network Diagram of Newly Installed Wireless Access Point Integrated to the Intranet .....	88
Figure 42 - Present Operational Workflow for RWR Uploading Team.....	89
Figure 43 - New Operational Workflow for RWR Uploading Team After Incorporating the IEEE 802.11b Wireless Technology Upgrade .....	90
Figure 44 - Timing Chart for Present Operational Events.....	92
Figure 45 - New Timing Chart for Operational Events for RWR Uploading Team After Incorporating IEEE 802.11b Wireless Transmission Technology Upgrade....	93
Figure 46 - Cisco Aironet® 1200 Series Access Point.....	103
Figure 47 - Client Devices Equipped With Wireless Client Adapters Can Roam Freely Throughout a Facility Via Communications With Multiple Access Points ..	111
Figure 48 - The Cisco Wireless Security Suite is an Enterprise-Class Security System Based on the 802.1x Architecture.....	113

## LIST OF TABLES

Table 1 - Comparison of Wireless LAN Technologies [From 3] .....	24
Table 2 - Frequencies and Power Output in the UNII 5.2 GHz.....	28
Table 3 - Selection Criteria Scoring Table .....	78
Table 4 - Hardware Cost for IEEE 802.11b Wireless Transmission Capability Upgrade.....	95
Table 5 - Summary of Key Security Mechanism That Can Be Implemented in WLAN .....	98

THIS PAGE INTENTIONALLY LEFT BLANK



## LIST OF ABBREVIATIONS, ACRONYMS & SYMBOLS

AAA	Anti-Aircraft Artillery
ACF	Air Combat Fighter
AF	After-Flight Checks
AI	Airborne Interceptor
AMRAAM	Advanced Medium Range Air-to-Air Missile
AOA	Angle-of-Arrival
AP	Access Point
BF	Before-Flight Checks
BPSK	Binary Phase Shift Keying
CCIP	Common Configuration Implementation Program
CCK	Complementary Code Keying
COTS	Commercial Off The Shelf
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access / Collision Detection
DES	Direct Encryption Standard
DSSS	Direct Sequence Spread Spectrum
EDNA	Enhanced Diagnostics Aid
EW	Electronic Warfare
FCC	Federal Communication Committee
FHSS	Frequency Hopping Spread Spectrum
FSO	Free-Space Optics
HUD	Head-Up Display

IEEE	Institute of Electrical and Electronics Engineers
IR	Infrared
IREDD	Infrared Emitting Diode
ISI	Inter-Symbol Interference
ISM	Industrial, Scientific and Medical
LAN	Local Area Network
LED	Light-Emitting Diodes
MAC	Media Access Control
MIL-SPEC	Military Specifications
NIC	Network Interface Card
NOS	Network Operating System
OFDM	Orthogonal Frequency Division Multiplexing
QoS	Quality of Service
PBCC	Packet Binary Convolutional Coding
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency
RWR	Radar Warning Receiver
SAM	Surface-to-Air Missile
SQCP	Squadron Command Post
UNII	Unlicensed National Information Infrastructure
WAN	Wide Area Network
WECA	Wireless Ethernet Compatibility Alliance
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network

## ACKNOWLEDGMENTS

This thesis is dedicated to my family, especially my loving wife, Puay Chee, my son, Adrian, and my adorable daughter, Alicia, for enduring my stress and absence during my research here at the Naval Postgraduate School. I am forever indebted to them for their love, consideration, and unrelenting support that continually inspired me to visualize reality from a different perspective.

I also wish to dedicate this thesis to my thoughtful and supportive parents who taught me the values of education, diligence and conscientiousness.

I would like to express my sincere appreciation to my advisors, Professor Bert Lundy and Professor Donald V. Z. Wadsworth. Without their support coupled with clear explanations and supervision, this thesis would not have been possible.

Lastly, I must thank my sponsor, the Republic of Singapore Air Force, for providing an opportunity for me to pursue my postgraduate study here in the Naval Postgraduate School.

THIS PAGE INTENTIONALLY LEFT BLANK

# **I. INTRODUCTION**

## **A. BACKGROUND**

Presently, the required data file to be loaded onto the Radar Warning Receiver (RWR) onboard the F-16 aircraft is done manually by the aircraft technicians, two to three hours prior to the actual flight time. In today's environment where human resources are scarce and limited, such manual intensive methods may soon be unsupportable. As such there may be a need to look into the use of wireless transmission technology to complement or if possible replace the manual method (via floppy diskette) of loading the critical data file from the command station to the Enhanced Diagnostics Aid (EDNA) prior to loading the data onto the ALR-69 system onboard every F-16 aircraft. The present wireless technology is relatively mature and stable. It should be feasible to incorporate and adapt this technology for use in the flight line environment. The propagation effect in wireless transmission will also be studied and recommendations be proposed with regards to the installation of wireless facilities in the flight line. In addition, the EDNA, a portable maintenance aid that comes with the F-16 aircraft for loading the data file onto the ALR-69 systems onboard the F-16 aircraft has to be upgraded to cater to the use of wireless transmission technology. Hence, a system feasibility study is to be carried out to adapt or upgrade the present equipment to wireless transmission capability.

## **B. OBJECTIVE OF STUDY**

The objectives of the project are to investigate, perform a feasibility study, and propose a plan for use of the present state-of-art wireless transmission technology to load critical data file from the command center onto the EDNA prior to loading onto the ALR-69 systems onboard the F-16 aircraft in a flight line environment. The investigation shall include the limitation imposed by propagation effects (if any) on wireless transmission and the security aspects of wireless transmission in a typical flight line environment. In addition, the adaptation or upgrade required to the present EDNA to include the wireless transmission capability will be determined. Finally, the total cost for implementing such

wireless technology in the flight line will be determined and a proposal will be drafted for the possible implementation of the wireless transmission technology in the flight line.

### **C. APPROACH**

The Enhanced Diagnostics Aid (EDNA) provides worldwide flight line and back shop support for load/verify of operational flight programs; download of aircraft flight data recorder and subsystem enhanced fault diagnostics. The EDNA is widely used by aircraft technicians to load the required data file to the RWR systems onboard the F-16 aircraft. EDNA is fundamentally a ruggedized laptop with Windows Operating Systems (OS) version 98. The feasibility study was conducted on the EDNA to include the PCMCIA wireless adapter client, the software compatibility on the EDNA OS and the location of the access points to be installed in the flight line.



**Figure 1 - EDNA Used on the F-16 Aircraft**

In addition to the physical hardware feasibility studies the compatibility of the 802.11 wireless frequency spectrum with the frequency spectrum used by other existing systems onboard the aircraft was also investigated. This is crucial to ensure that the 802.11 wireless frequency spectrum is safe for use in the flight line environment.

The thesis includes recommendation for the necessary hardware necessary to implement IEEE 802.11 wireless transmission for use on the RWR system in a flight line environment.

## **D. OVERVIEW**

Chapter II explains the history of F-16 aircraft and the ALR-69 Systems. It includes the push factors for the need of compact and multi-role fighter aircraft by the USAF. The different F-16 blocks and their configuration variances are explained in great detail.

Chapter III presents an overview of the mature IEEE 802.11 wireless technology. In today's military application, the demand for wireless connectivity continues to rise and the demand is similar to those of the domestic market. The convenience and portability of wireless networks, including wireless Internet, e-mail, and network access - make it a popular choice for many organizations, including the military.

Chapter IV presents an overview of another wireless technology - the Free-Space Optics (FSO). This is an alternate technology to the IEEE 802.1x wireless protocol and offers good security protection compared to 802.1x. FSO is gaining in popularity in wireless applications, both in the military and civilian organizations.

Chapter V explains the present operating concept as well as the problems encountered in a typical flight line environment in the Republic of Singapore Air Force (RSAF).

Chapter VI presents the feasibility study on upgrading the present systems to include the IEEE 802.11 wireless systems. It includes investigation of potential Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC) problems with existing systems onboard the aircraft, armament safety concerns, as well as proposed locations for the installation of the IEEE 802.11 access points.

Chapter VII presents the new operational concept after the incorporation of the wireless systems. It presents and account for the reduction in turnaround time, reduction in Man-hour cost. The budget required for the new hardware or software upgrading to include the wireless systems is estimated.

Chapter VIII concludes the findings in the thesis and presents recommendation for future work.

THIS PAGE INTENTIONALLY LEFT BLANK



## **II. F-16 AIRCRAFT AND ALR-69 SYSTEMS OVERVIEW**

### **A. OVERVIEW OF F-16 AIRCRAFT**

The F-16 Fighting Falcon is a compact, multi-role fighter aircraft. It is highly maneuverable and has proven itself in air-to-air combat and air-to-surface attack. It provides a relatively low-cost, high-performance weapon system for the United States and allied nations.

In an air combat role, the F-16's maneuverability and combat radius (distance it can fly to enter air combat, stay, fight and return) exceed that of all potential threat fighter aircraft. It can locate targets in all weather conditions and detect low flying aircraft in radar ground clutter. In an air-to-surface role, the F-16 can fly more than 500 miles (860 kilometers), deliver its weapons with superior accuracy, defend itself against enemy aircraft, and return to its starting point. An all-weather capability allows it to accurately deliver ordnance during non-visual bombing conditions.



**Figure 2 - F-16 D Aircraft from the Republic of Singapore Air Force (RSAF)**

The F-16 is being built under an unusual agreement creating a consortium between the United States and four NATO countries: Belgium, Denmark, the Netherlands and Norway. These countries jointly produced with the United States an initial 348 F-16s for their air forces. Final airframe assembly lines were located in Belgium and the Netherlands. The consortium's F-16s are assembled from components manufactured in all five countries. Belgium also provides final assembly of the F100 engine used in the European F-16s.

USAF F-16 multi-mission fighters were deployed to the Persian Gulf in 1991 in support of Operation Desert Storm, where more sorties were flown than with any other aircraft. These fighters were used to attack airfields, military production facilities, Scud missile sites and a variety of other targets.

The original F-16 was designed as a lightweight air-to-air day fighter. Air-to-ground responsibilities transformed the first production F-16s into multi-role fighters. The empty weight of the Block 10 F-16A is 15,600 pounds. The empty weight of the Block 50 is 19,200 pounds. The A in F-16A refers to a Block 1 through 20 single-seat aircraft. The B in F-16B refers to the two-seat version. The letters C and D were substituted for A and B, respectively, beginning with Block 25. **Block is an important term in tracing the F-16's evolution.** Basically, a block is a numerical milestone. The block number increases whenever a new production configuration for the F-16 is established. Not all F-16s within a given block are the same. They fall into a number of block subsets called mini-blocks. These sub-block sets are denoted by capital letters following the block number (Block 15S, for example). From Block 30/32 on, a major block designation ending in 0 signifies a General Electric engine; one ending in 2 signifies a Pratt & Whitney engine.

## **B. F-16 EVOLUTION**

The air war experience in Vietnam, where the lack of maneuverability of US fighters at transonic speeds provided advantages to nimble enemy fighters, was the stimulus for the Lightweight Fighter program. The United States Air Force and designers

of the Lightweight Fighter therefore placed great emphasis on achieving unprecedented transonic maneuver capability with excellent handling qualities.

In January 1972, the Lightweight Fighter Program solicited design specifications from several American manufacturers. Participants were told to tailor their specifications toward the goal of developing a true air superiority lightweight fighter. General Dynamics and Northrop were asked to build prototypes, which could be evaluated with no promise of a follow-on production contract. These were to be strictly technology demonstrators. The two contractors were given creative freedom to build their own vision of a lightweight air superiority fighter, with only a limited number of specified performance goals. Northrop produced the twin-engine YF-17, using breakthrough aerodynamic technologies and two high-thrust engines. General Dynamics countered with the compact YF-16, built around a single F100 engine.

The evolutions of the YF-16 design at LMTAS included studies of configuration variables such as wing design, maneuvering devices, number and location of engines, control surfaces, number and location of tail surfaces, and structural concepts. As the configuration options matured, two candidate configurations competed for priority. The first configuration was a simple wing, body, and empennage design, while the second design was a twin-tailed, blended-wing body with vertical and horizontal tails on booms. The LMTAS team selected the best features of both configurations for the final YF-16 design. After considerations of performance, stability, and control were addressed, the YF-16 configuration incorporated a rather wide, blended forebody that produced strong vortices at moderate angles of attack. LMTAS had attempted to weaken the strength of the vortices by promoting attached flow, but these attempts were not successful.



**Figure 3 - General Dynamic's (Now Called Lockheed Martin) 2<sup>nd</sup> YF-16 Prototype**

In the early 1960's worldwide interest in the phenomenon known as "vortex lift" increased as a result of aerodynamic studies of highly swept configurations such as the Concorde supersonic transport. The favorable effects of vortex on lift were demonstrated during development of the Swedish Viggen canard configured aircraft. The favorable effects of the canard-trailing vortex on the lifting capability of a close-coupled wing might also be extended to higher angles of attack by the strong leading-edge vortex flow of a slender lifting surface. The leading edge of the blended fore body is sharpened to increase (rather than decrease) the strength of the vortices, which could be exploited for additional lift. This modification allowed the fore body vortices to dominate and stabilize the flow field over the aircraft at high angles of attack, improve longitudinal and directional stability for the single-tail configuration, and stabilize the flow over the outer wing panels. In addition, the sharpened strake significantly reduced buffet intensity at transonic maneuvering conditions. The wing-body strake of the F-16 is regarded as a key contribution to its success as a maneuvering fighter.

When the YF-16 team analyzed the effects of deflected leading- and trailing-edge flaps and the sharp-edged wing-body strake on directional stability at high angles of

attack, they found that the stability contributions of a single vertical tail were significantly enhanced. However, the contributions of twin vertical tails were markedly degraded. As a result of this analysis, the YF-16 was configured with a single vertical tail. Thus, the Langley recommendation for a sharpened wing-body strake favorably impacted other configuration features of the aircraft.

Increased maneuverability for the YF-16 necessitated extended flight at high angles of attack where aerodynamic deficiencies caused by separated airflow can result in sudden decreases in stability and controllability. Therefore, special emphasis was placed on tests to insure that the YF-16 could provide the pilot with “care-free” maneuverability. To provide superior handling characteristics at high angles of attack, any undesirable handling characteristics were pushed out of the operating envelope of the aircraft and the flight envelope was limited with an advanced fly-by-wire flight control system by LMTAS. This concept has proven to be highly successful and has been used in all variants of the F-16.

Reliance on the flight control system to insure satisfactory behavior at high angles of attack required research on the ability of fly-by-wire control systems to limit certain flight parameters during strenuous air combat maneuvers. The F-16 employs the concept of “relaxed static stability” in which the aircraft is intentionally designed to be aerodynamically unstable while the flight control system provides integrated stability by sensing critical flight variables and making the control inputs required to stabilize the aircraft. Of particular concern was the ability of the horizontal tails and longitudinal control system to limit the aircraft’s angle of attack during maneuvers with high roll rates at low airspeeds. Such maneuvers are critical because rapid rolling maneuvers produce large nose-up trim changes due to inertial effects, whereas the aerodynamic effectiveness of the horizontal tails becomes significantly reduced at low airspeeds and high angles of attack.

Early on, tests of a YF-16 model indicated that if angle of attack was not limited by the flight control system, the aircraft could pitch up and attain an undesirable trimmed condition at very high angles of attack with insufficient nose-down aerodynamic control to recover normal flight. NASA Langley researchers viewed this “deep” stall as a

serious problem that would require significant research for resolution. High-angle-of-attack test results obtained on models of the early production version of the F-16 configuration showed the same deep-stall trimmed condition that was noted in the YF-16 results. In subsequent high-angle-of-attack flight evaluations at Edwards Air Force Base, an F-16 that had been subjected to rapid rolls at diminishing airspeeds in vertical zoom climbs suddenly entered a stabilized deep-stall condition and the pilot was unable to recover the aircraft with normal aerodynamic controls. Fortunately, the test aircraft was equipped with an emergency spin recovery parachute that was deployed to recover the aircraft to normal flight conditions. This event brought all high-angle-of-attack flight tests of the F-16 to a standstill while a solution to the deep stall could be found. The ultimate fix for the problem (which also improved takeoff performance) was increasing the size of the horizontal tail about 25 percent. This solution has been incorporated in all F-16 production aircraft.



**Figure 4 - Northrop YF-171 “Cobra” Prototype Aircraft**

---

1 Engines: Two General Electric YJ101-GE-100 turbojets, 15,000 lb.s.t. each with afterburning. Performance: Maximum speed: Mach 2.0 (1320 mph) at 40,000 feet. Service ceiling 60,000 feet. Maximum range 2800 miles. Weights: 21,000 pounds empty, 23,000 pounds gross, 30,630 pounds maximum takeoff. Dimensions: Wingspan: 35 feet 0 inches, length 55 feet 6 inches, height 14 feet 6 inches, wing area 350 square feet. Armament: One 20-mm M61A1 cannon. One AIM-9 Sidewinder infrared-homing air-to-air missile could be carried at each wingtip. Stores could be carried on one ventral and four under wing pylons.

When the Lightweight Fighter competition was completed early in 1975, both the YF-16 and the YF-17 showed great promise. The two prototypes performed so well, in fact, that both were selected for military service. On 13 January 1975 the USAF announced that the YF-16's performance had made it the winner of its Air Combat Fighter (ACF) competition. This marked a shift from the original intention to use the two airplanes strictly as technology demonstrators. General Dynamics' YF-16 had generally shown superior performance over its rival from Northrop. At the same time, the shark-like fighter was judged to have production costs lower than expected, both for initial procurement and over the life cycle of the plane. At the same time, the YF-16 had proved the usefulness not only of fly-by-wire flight controls, but also such innovations as reclined seat backs and transparent head-up display (HUD) panels to facilitate high-G maneuvering, and the use of high profile, one-piece canopies to give pilots greater visibility. Thus, the USAF had its lightweight fighter, the F-16.

### **C. F-16 C AND F-16 D**

The **F-16C and F-16D** aircraft, which are the single- and two-place counterparts to the F-16A/B, incorporate the latest cockpit control and display technology. All F-16s delivered since November 1981 have built-in structural and wiring provisions and systems architecture that permit expansion of the multi-role flexibility to perform precision strike, night attack and beyond-visual-range interception missions. All active units and many Air National Guard and Air Force Reserve units have converted to the F-16C/D, which is deployed in a number of Block variants.

**Block 25** added the ability to carry AMRAAM<sup>2</sup> to the F-16 as well as night/precision ground-attack capabilities, as well as improved radar, the Westinghouse (now Northrop-Grumman) AN/APG-68<sup>3</sup>, with increased range, better resolution, and more operating modes.

---

<sup>2</sup> AIM-120 AMRAAM (Advanced Medium Range Air to Air Missile) is a high-supersonic, day/night/all weather Beyond Visual Range (BVR), fire-and-forget air-to-air missile. It has a high-explosive warhead and relies on active radar homing for the final stages of flight, being launched on inertial mid-course guidance without the need for the fighter to keep the target illuminated.

<sup>3</sup> Northrop Grumman AN/APG-68 fire control radar for the F-16 fighter is the USAF's most reliable fighter radar. It provides multiple modes, including long-range, all-aspect detection and tracking, simultaneous multiple target tracking and high-resolution ground mapping. The AN/APG-68 and its predecessor, the AN/APG-66, are two of the most successful fire control radars ever built.

**Block 30/32** added two new engines. Block 30 designates a General Electric F110-GE-100 engine, and Block 32 designates a Pratt & Whitney F100-PW-220<sup>4</sup> engine. Block 30/32 can carry the AGM-45 Shrike and the AGM-88A HARM, and like the Block 25, it can carry the AGM-65 Maverick.

**Block 40/42** (F-16CG/DG) gained capabilities for navigation and precision attack in all weather conditions and at night with the LANTIRN<sup>5</sup> pods and more extensive air-to-ground loads, including the GBU-10, GBU-12, GBU-24 Paveway laser-guided bombs and the GBU-15. Block 40/42 production began in 1988 and ran through 1995. Currently, the Block 40s are being upgraded with several Block 50 systems: ALR-56M threat warning system, the ALE-47 advanced chaff/flare dispenser, an improved performance battery, and Falcon UP structural upgrade.

**Block 50/52** Equipped with Northrop Grumman APG-68 (V) 7 radar and a General Electric F110-GE-129 Increased Performance Engine, the aircraft are also capable of using the Lockheed Martin low-altitude navigation and targeting for night (LANTIRN) system. Technology enhancements include color multifunctional displays and programmable display generator, a new Modular Mission Computer, a Digital Terrain System, a new color video camera and color triple-deck video recorder to record the pilot's head-up display view, and an upgraded data transfer unit. By mid-1999 Block 50/52 (also known as Block 50 Plus) F-16s will carry the CBU-103/104/105<sup>6</sup> Wind-Corrected Munitions Dispenser, the AGM-154<sup>7</sup> Joint Standoff Weapon, and the GBU-31/32<sup>8</sup> Joint Direct Attack Munition.

---

<sup>4</sup> The F100 is an axial-flow turbofan with a bypass ratio of 0.7:1. There are two shafts, one shaft carrying a three-stage fan driven by a two-stage turbine, the other shaft carrying the 10-stage main compressor and its two-stage turbine. For the F100-PW-200 version, normal dry thrust is 12,420 pounds, rising to a maximum thrust of 14,670 pounds at full military power. Maximum afterburning thrust is 23,830 pounds.

<sup>5</sup> LANTIRN is a system consisting of two pods, which allow aircrew to fly their aircraft by day or night and in adverse meteorological conditions. It provides Terrain-Following Radar (TFR), Forward-Looking Infra-Red (FLIR), targeting information for the aircraft's on-board fire control system and target laser illumination. LANTIRN is currently deployed on F-16C/D, F-15E/I/S and F-14 platforms. Over 1,400 pods are currently in service with 10 countries.

<sup>6</sup> These weapons provide accurate, multiple-kill capability from high-altitude release.

<sup>7</sup> All-Weather Standoff Weapons and provides precision capability with GPS guidance.

<sup>8</sup> Joint Direct Attack Munitions (JDAM) is a guidance tail kit that converts existing unguided free-fall bombs into accurate, adverse weather "smart" munitions. With the addition of a new tail section that contains an inertial navigational system and a GPS guidance control unit, JDAM improves the accuracy of unguided, general-purpose bombs in any weather conditions.



**Block 50D/52D Wild Weasel** F-16CJ (CJ means block 50) comes in C-Model (1 seat) and D-Model (2 seat) versions. It is best recognized for its ability to carry the AGM-88 HARM<sup>9</sup> and the AN/ASQ-213 HARM Targeting System<sup>10</sup> (HTS) in the suppression of enemy air defenses (SEAD<sup>11</sup>) mission. The HTS allows HARM to be employed in the range-known mode providing longer-range shots with greater target specificity. This specialized version of the F-16, which can also carry the ALQ-119 Electronic Jamming Pod for self protection, became the sole provider for Air Force SEAD missions when the F-4G Wild Weasel was retired from the Air Force inventory. The lethal SEAD mission now rests solely on the shoulders of the F-16 Harm Targeting System. Although F-18s and EA-6Bs are HARM capable, the F-16 provides the ability to use the HARM in its most effective mode. The original concept called for teaming the F-15 Precision Direction Finding (PDF) and the F-16 HTS. Because this teaming concept is no longer feasible, the current approach calls for the improvement of the HTS capability. The improvement will come from the Joint Emitter Targeting System (JETS), which facilitates the use of HARM's most effective mode when launched from any JETS capable aircraft.

**Block 60** - In May 1998 the UAE announced selection of the Block 60 F-16 to be delivered between 2002 to 2004. The upgrade package consists of a range of modern systems including conformal fuel tanks for greater range, new cockpit displays, an internal sensor suite, a new mission computer and other advanced features including a new agile beam radar.

The Mid-Life Update (MLU) is an avionics modification program for the F-16 Block 15 A/B and is based primarily upon common requirements of the European

---

<sup>9</sup> AGM-88 HARM (high-speed anti-radiation missile) is an air-to-surface tactical missile designed to seek and destroy enemy radar-equipped air defense systems.

<sup>10</sup> AN/ASQ-213 HARM Targeting Systems (HTS) Pod has opened up a whole new mission for the F-16. With HARM/HTS, the F-16 picked up the demanding mission of suppression of enemy air defenses (SEAD), once performed primarily by the F-4G Wild Weasel aircraft. The F-16 is truly a multiple unit; in addition to the primary SEAD mission, it also flies air superiority, defense counter air, and air interdiction missions. Originally developed by Texas Instruments under a program to provide new modular targeting systems for USAF aircraft, it is the key to USAF's effort in SAM hunting now and in the 21st century. The pod is 8 inches in diameter, 56 inches long and weighs 85 pounds. Most important of the HTS' capabilities is the ability to rapidly generate ranges to target radars, as well as to provide greater discretion between different types of enemy radars.

<sup>11</sup> That activity which neutralizes, destroys, or temporarily degrades surface-based enemy air defenses by destructive and/or disruptive means. Also called SEAD. See also electromagnetic spectrum; electronic warfare.

Participating Governments (EPG) through the F-16 Multinational Fighter Program (MNFP) Steering Committee. The members of the F-16 MNFP are the Belgian Air Force (BAF), the Royal Danish Air Force (RDAF), the Royal Netherlands Air Force (RNLAf), the Royal Norwegian Air Force (RNoAF), and the United States Air Force. The MLU program evolved from the Agile Falcon/MLU pre-development stage, which began in January 1988. Transition to MLU Engineering and Manufacturing Development (EMD) began in January 1990. The EPG elected during EMD to develop and buy aircrew trainers, Unit Level Trainers (ULTs) and Weapon System Trainers (WSTs). In October 1992, the US announced its withdrawal from the production phase of the MLU; and, in 1995, Denmark announced its withdrawal from the MLU trainer program with the intent to purchase directly from Hughes Training, Inc. (now Raytheon Training, Inc.). The MLU trainer program was established to support the remaining European Participating Air Forces (EPAF). The MLU trainer contract was awarded in June 1995 to Lockheed Martin Tactical Aircraft Systems (LMTAS) in Fort Worth, Texas, with the majority of the effort for both hardware and software development and integration being done by LMTAS's prime sub-contractor, Thomson Training and Simulation, Ltd. (TT&SL) in Crawley, England. The contract calls for a total of 12 trainers to be delivered to the EPAF, and one Training System Support Center (TSSC) at LMTAS. European participating industries competed equally for subcontracts on the F-16 Mid-Life Update Program. European participating industries were awarded a total of \$303.3 million of the \$380 million available for foreign manufacture on the F-16 Mid-Life Update Program. Contractors complied with the Federal Acquisition Regulation and the Defense Federal Acquisition Supplement in the solicitation, source selection, and award process for subcontracts on the F-16 aircraft Mid-Life Update Program. European participating industries who were not awarded subcontracts: had smaller production bases than U.S. companies; did not have nonrecurring costs subsidized by their respective European

governments; could not overcome U.S. companies' technical advantages; or did not receive follow-up contracts for research and development on the F-16 Mid-Life Update Program.

The Common Configuration Implementation Program (CCIP) for the USAF's F-16C/D fleet will provide significant avionics upgrades to Block 40 and 50 F-16s, ensuring their state-of-the-art capability well into the 21st century. A key element of the upgrade is a common hardware and software avionics configuration for these two blocks that will bring together the Block 40/42 and 50/52 versions into a common configuration of core avionics and software. The avionics changes consist of the following systems: Link 16 Multifunctional Information Distribution System (MIDS), Joint Helmet-Mounted Cueing System (JHMCS), commercial expanded programmable display generator, color multifunction display set, modular mission computer, MUX loadable data entry display set and an electronic horizontal situation display. This package contains a number of systems being incorporated into European F-16s in the F-16 A/B Mid-Life Update program.

#### **D. ALR-69 (RADAR WARNING RECEIVER) SYSTEM OVERVIEW<sup>12</sup>**

The ALR-69 Class IV Radar Warning Receiver (RWR<sup>13</sup>) system provides the following functional capabilities: RF threat situational awareness, threat signal processing, reprogrammability, associated defensive support equipment and training equipment, and future Electronic Warfare (EW) interfaces to other avionics defensive/offensive equipment. The RWR system detects, identifies, processes and displays airborne interceptor (AI), surface-to-air missile (SAM) and anti-aircraft artillery (AAA) weapon systems. Situation awareness provides the crew with threat type, emitter

---

<sup>12</sup> Information on ALR-69 RWR obtained from <http://www.fas.org/man/dod-101/sys/ac/equip/an-alr-69.htm> accessed on October 1, 2003.

<sup>13</sup> RWR (Radar Warning Receiver) shows the signals received by the ALR-69 TWS (Threat Warning System). These signals can be originated from other aircraft or from ground units. The ALR-69 registers and processes these radar-signals and provides type of radar, intensity and direction of them. Threats with high priority are shown with their bearing and intensity. As intensity increases, the signal is shown nearer to the center of the display. The TWS consists of the RWR, Threat Warning Prime Panel, the Threat Warning Aux Panel and the Chaff/Flare Panel.

mode and threat angle-of-arrival (AOA) information. The RWR system integrated diagnostics provide the crew and maintenance personnel system diagnostics data.



**Figure 5 - Components of ALR-69 RWR System Produced by Litton**

The AN/ALR-69 continuously monitors the radar environment to alert the pilot of any hostile or foreign activity that may be taking place. When it receives a radar signature it compares that signature to its database of threats and displays a graphical symbol of that radar so the aircrew can see what kind of radar is "painting" their aircraft; whether it be friend or foe. If the system determines the radar is an immediate threat it will give a distinctive audible warning. The system is updated continuously as new threats are encountered or to improve system operation. Litton manufactures the system.

The AN/ALR-69 RWR has been installed on Air National Guard (ANG), United States Air Force (USAF) and USAF Reserve F-16 (except Block 50), A-10, AC-130, MC-130H Combat Talon II, and the HH-53 aircraft. The AN/ALR-69 RWR is a mature system and has been in continuous service since the mid 1970s.

The AN/ALR-69 represented early-1970s technology. As such, by the early 1990s, the system had become non-supportable because of obsolete components and saturated embedded memory. As a result, Center and contractor engineers and technicians designed and developed a Reliability and Maintainability (R&M) modification for the system. In turn, Air Force personnel conducted a Qualification Operational Test and Evaluation (QOT&E) on the production hardware from June to August 1993.

In FY94, AN/ALR-69 engineers, supported by contractor personnel, undertook software changes to the Mission Data (MD) and Operational Flight Program (OFP), in conjunction with the hardware upgrade. The software effort involved the conversion of the software from 9445 to 1750 computer language and the incorporation of over 120 Operational Software Change Requests (SCRs). This proved to be an extraordinary modification since system programmers normally incorporates only 20-30 software changes at one time. The effort was worth the trouble since these software changes incorporated the latest threat data information.

The hardware and software changes to the system provided numerous benefits including improved reliability of the system from about 110 hours to about 244 hours and elimination of obsolete components and the inclusion of adjustable components from the Signal Processor LRU which had experienced numerous support problems. This also meant that the maintenance time for this LRU decreased by half improving Center personnel's ability to process assets in support of user requirements.

Other improvements entailed providing for a 1553B<sup>14</sup> data bus interface with other ECM and avionics systems on the aircraft and total flight line programming of the system with MD and OFP software updates. This resulted in about \$500,000 savings annually due to the use of Electronically Erasable Programmable Read Only Memory (EEPROM) hardware kits. Systems programmers increased embedded memory capacity from 12K Random Access Memory (RAM) and 40K EEPROM in the old system to 128K RAM and 256K EEPROM in the modified system. They also enhanced the BIT system which allowed the user to detect LRU failures on the aircraft within one minute, and which meet the requirements for two levels of maintenance on the system. Programmers improved processing speeds for threat information received by the system, and they ameliorated the system's threat detection capability through the incorporation of over 293 Operational Software changes.

---

<sup>14</sup> The digital data bus MIL-STD-1553 was designed in the early 1970's to replace analog point-to-point wire bundles between electronic instrumentation. The latest version of the serial local area network (LAN) for military avionics known as MIL-STD-1553B was issued in 1978. After 20 years of familiarity and reliable products, the data bus continues to be the most popular militarized network.

From June 4, 1993 through July 23, 1993 the Air National Guard Air Force Reserve Test Center (AATC) conducted a qualification operational test and evaluation (QOT&E) for the AN/ALR-69 reliability and maintainability (R&M) modification. The R&M modification was necessary at the time to avert support problems. More specifically, the R&M modification entailed the replacement of the aging AN/ALR-69 system processor and controller with more modern supportable components. Following successful completion of the QOT&E for the R&M modification, the ALR-69 Product Improvement Program (PIP) was initiated in 1993 to replace the current ALR-69 receiver with an advanced crystal video receiver. The first platforms scheduled to receive the ACVR equipped ALR-69s include the HH-60 PAVEHAWK Air Force Combat Search and Rescue Helicopter and F-16 fighter aircraft.

**EDNA Portable Maintenance Aid Technical Characteristics**

**Electronics Unit**

**Processor**

- Pentium MMX, 266 MHz

**Memory**

- 64 MB DRAM
  - Expandable to 192 MB
- 2 GB Removable Hard Disk Drive
  - Expandable to 8 GB
- Two PCMCIA 2.0 Type I, II or III Card Slots
  - Supports Commercial RAM, Flash, and Interface Cards

**Display**

- 9.5" Backlit Sunlight Readable Active Matrix
- 640 × 480, 64 Grayscale

**Keyboard**

- Full-Travel, Sealed QWERTY Keyboard
- Separate Alphanumeric and Function Key Pad
- Integrated Mouse

**Physical**

- 15.75"W × 10.5"H × 4"D
- 40.0W × 26.7H × 10.2D cm
- 16 pounds

**Environmental and EMI**

- Fully Flightline Qualified
  - Tailored MIL-STD-810 and -461

**BAE SYSTEMS**

---

**EDNA Portable Maintenance Aid Technical Characteristics**

**Electronics Unit (Continued)**

**Interfaces**

- Programmable for Peculiar Bus Protocols
- Serial RS-232, -422, Centronics Parallel
- Five Channel MIL-STD-1553
- IEEE-488
- Ethernet

**Power**

- 12-48 Vdc
- 110-240 Vac, 50/400 Hz
- Removable Batteries
  - Standard Commercial Nicad or Alkaline D Cells
- External Batteries
  - Supports Standard Issue BB-390/U, -590/U

**Software**

- MS-DOS 6.0
- Windows 95, NT
- SCO Unix
- Built-in-Test, Self-Test
- Application Specific Diagnostic and MLV Implementations for F-16, B-2, F-117

**Remote Control Unit**

- 6" Backlit Multiplexed, Transflective Touch Screen and Pen-based LCD
- 2048 × 2048 Resolution
- 3.5 pounds

For further information, contact:  
 Information & Electronic Warfare Systems  
 P.O. Box 868, NCA1-4241  
 Nashua, NH 03061-0868  
 Tel: (603) 885-6065  
 Fax: (603) 885-9068

**BAE SYSTEMS**

PIES/01C1310-002

**Figure 6 - Technical Specifications of EDNA by BAE Systems**

The Advanced Crystal Video Receiver (ACVR) upgrade contributes to *full-dimensional protection* by improving individual aircraft probability of survival through improved aircrew situation awareness of the radar guided threat environment. The ACVR

consist of radio frequency (RF) Triplexer, Extended Range Dual Log Video Amplifier (ERDLVA) and Logic Board. The ACVR will replace the existing preamplifier of the ALR-69 Radar Warning Receiver (RWR). The ACVR will provide increased receiver sensitivity, increased dynamic range, and increased pulse density and signal processing capability. Additionally, the ACVR will reduce maintenance costs through improved reliability and maintainability and enhanced Built-In-Test (BIT).

The ACVR upgrade is designed to increase the types of threats that the ALR-69 can detect and classify and should improve detection range and direction finding accuracy. More specifically, the ACVR upgrade should enable the ALR-69 to process both airborne and ground pulse Doppler threat emitters. RF pulse density processing requirements for ACVR are necessarily increased by orders of magnitude over previous emitter environments tested against.

THIS PAGE INTENTIONALLY LEFT BLANK



### **III. IEEE 802.11 WIRELESS TECHNOLOGY OVERVIEW**

#### **A. OVERVIEW**

The previous chapter discussed F-16 aircraft and ALR-69 systems overview. This chapter discusses the IEEE 802.11 wireless protocol which could be used to complement the transfer of data file from the control station, located in the command centre, to the EDNA prior to the uploading to the ALR-69 systems onboard the F-16 aircraft in flight line environment. The evolution of 802.1x protocols (namely 802.11 Original, 802.11b, 802.11a and 802.11g), comparison of various classes of 802.11 protocol, how 802.11 wireless protocol works, 802.11 wireless configuration, 802.11 wireless technology options, security aspects in using 802.11 wireless protocol and conclude with considerations for 802.11 wireless implementation.

In the past decade, wireless has grown from an obscure and expensive curiosity into a practical and affordable networking technology. Today's most common wireless standards are 802.11b, a, and g Ethernet, also called Wi-Fi (Wireless Fidelity). The IEEE 802.11 standard is fast enough to be practical and affordable enough for home networks.

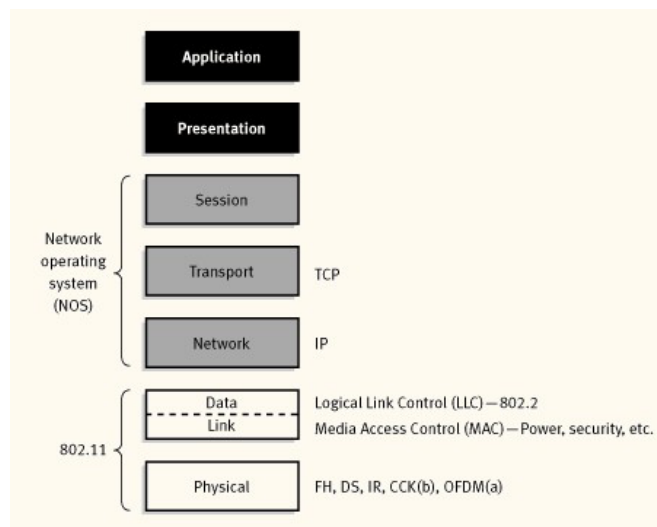
The convenience of wireless is the freedom of computers to move anywhere and still be connected to the network. Wireless is especially suited for use with laptop or notebook computers, offering users great freedom of movement. Wireless has shortcomings that make it ill suited for many networks. Yet its popularity and ongoing efforts to improve the technology make it a promising option in the future.

#### **B. BRIEF HISTORY OF IEEE 802.11 WIRELESS PROTOCOL**

IEEE 802.11 is an IEEE (Institute of Electrical and Electronics Engineering) standard for wireless networking. IEEE 802.11 added new physical and data-link layers to the ISO model to provide Ethernet over a radio frequency (RF). Though the concept started in the mid-1990s, the standard was only established in 1999. The first 802.11, some called IEEE 802.11-Original, supported speeds of only up to 2 Mbps. It supported two entirely different methods of encoding - Frequency Hopping Spread Spectrum

(FHSS) and Direct Sequence Spread Spectrum (DSSS) - leading to confusion and incompatibility between equipment. FHSS and DSSS will be explained in later sections of this chapter.

Reference to the ISO’s OSI model (refer to Figure 7), the data link layer within 802.11 consists of two sub layers: Logical Link Control (LLC) and Media Access Control (MAC). 802.11 uses the same 802.2 LLC and 48-bit addressing as other 802 LANs, allowing for very simple bridging from wireless to IEEE wired networks, but the MAC is unique to WLANs.



**Figure 7 - IEEE 802.11 and ISO Model**

The 802.11 MAC is similar in concept to 802.3, in that it is designed to support multiple users on a shared medium by having the sender sense the medium before accessing it. For 802.3 Ethernet LANs, the *Carrier Sense Multiple Access with Collision Detection* (CSMA/CD<sup>15</sup>) protocol regulates how Ethernet stations establish access to the wire and how they detect and handle collisions that occur when two or more devices try to simultaneously communicate over the LAN. In an 802.11 WLAN, collision detection is not practical due to what is known as the “near/far” problem: to detect a collision, a

<sup>15</sup> WLAN with CSMA/CA protocol works by a “listen before talk” scheme. The collision avoidance portion of CSMA/CA protocol is performed by such a procedure that let some randomly chosen users talk and the others listen, so that the users who hear somebody talking will refrain from talking. However, in spite of using the “listen before talk” scheme, packet collisions can still occur because the process to select speakers and listeners is random.

station must be able to transmit and listen at the same time, but in radio systems the transmission drowns out the ability of the station to “hear” a collision.

To account for this difference, 802.11 uses a modified protocol known as *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA) or the Distributed Coordination Function (DCF). CSMA/CA attempts to avoid collisions by using explicit packet acknowledgment (ACK), which means an ACK packet is sent by the receiving station to confirm that the data packet arrived intact.

CSMA/CA works as follows. A station wishing to transmit senses the air, and, if no activity is detected, the station waits an additional, randomly selected period of time and then transmits if the medium is still free. If the packet is received intact, the receiving station issues an ACK frame that, once successfully received by the sender, completes the process. If the ACK frame is not detected by the sending station, either because the original data packet was not received intact or the ACK was not received intact, a collision is assumed to have occurred and the data packet is transmitted again after waiting another random amount of time.

CSMA/CA thus provides a way of sharing access over the air. This explicit ACK mechanism also handles interference and other radio-related problems very effectively. However, it does add some overhead to 802.11 that 802.3 does not have, so that an 802.11 LAN will always have slower performance than an equivalent Ethernet LAN.

Another MAC-layer problem specific to wireless is the “hidden node” issue, in which two stations on opposite sides of an access point can both “hear” activity from an access point, but not from each other, usually due to distance or an obstruction. To solve this problem, 802.11 specifies an optional Request to Send/Clear to Send (RTS/CTS) protocol at the MAC layer. When this feature is in use, a sending station transmits an RTS and waits for the access point to reply with a CTS. Since all stations in the network can hear the access point, the CTS causes them to delay any intended transmissions, allowing the sending station to transmit and receive a packet acknowledgment without any chance of collision. Since RTS/CTS adds additional overhead to the network by

temporarily reserving the medium, it is typically used only on the largest-sized packets, for which retransmission would be expensive from a bandwidth standpoint.

Finally, the 802.11 MAC layer provides for two other robustness features: CRC checksum and packet fragmentation. Each packet has a CRC checksum calculated and attached to ensure that the data was not corrupted in transit. Packet fragmentation allows large packets to be broken into smaller units when sent over the air, which is useful in very congested environments or when interference is a factor, since larger packets have a better chance of being corrupted. This technique reduces the need for retransmission in many cases and thus improves overall wireless network performance. The MAC layer is responsible for reassembling fragments received, rendering the process transparent to higher-level protocols.

Generally, the IEEE 802.11 standard employs the CSMA/CA protocol at the Media Access Control (MAC<sup>16</sup>)/data link layer and there are four signal encoding techniques at the physical layer, namely: direct sequence spread spectrum (DSSS), frequency hopping spread spectrum (FHSS), orthogonal frequency division multiplexing (OFDM) and infrared (IR). Refer to Table 1 for comparison between the signal coding techniques.

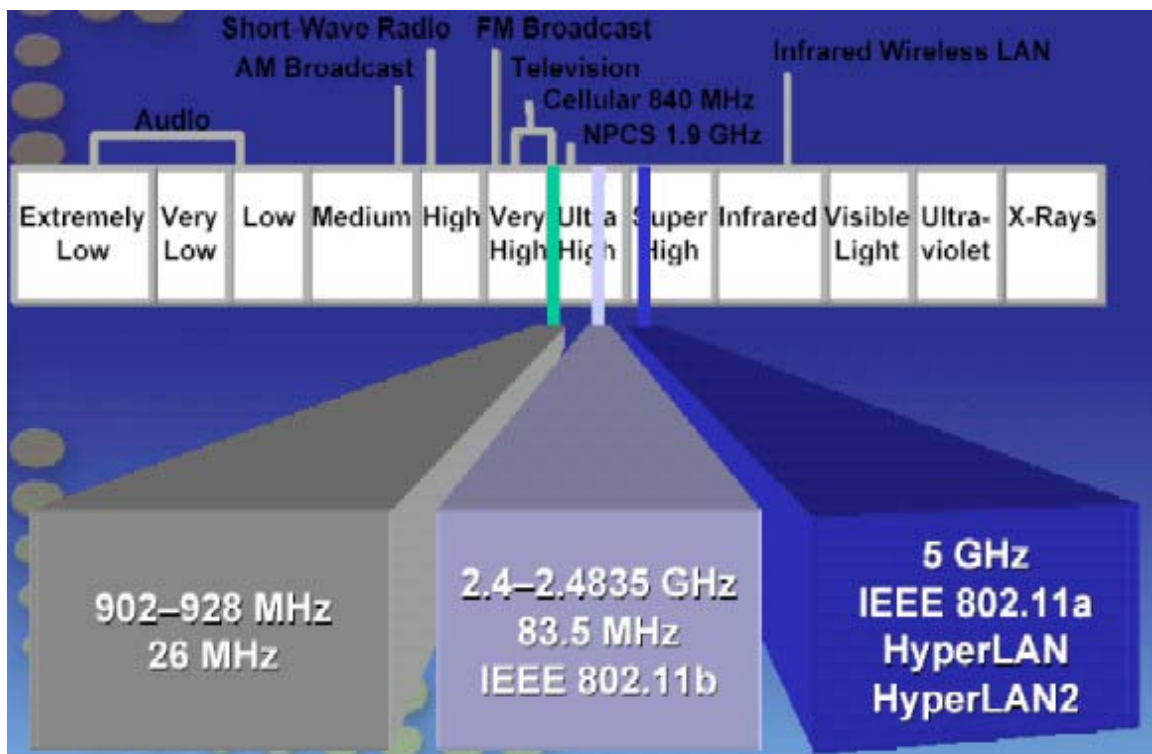
	Infrared		Spread Spectrum		Narrowband Microwave
	Diffused Infrared	Directed Infrared	Frequency Hopping	Direct Sequence	
<b>Data Rate</b>	1 to 4	1 to 10	1 to 3	2 to 20	10 to 20
<b>Mobility</b>	Stationary/mobile	Stationary with LOS	Mobile	Stationary/mobile	
<b>Range (m)</b>	15 to 60	25	30 to 100	30 to 250	10 to 40
<b>Detect ability</b>	Negligible		Little		Some
<b>Wavelength/frequency</b>	$\lambda$ : 800 to 900 nm		902 to 928 MHz 2.4 to 2.4835 GHz 5.725 to 5.85 GHz		902 to 928 MHz 5.2 to 5.775 GHz 5.275 to 5.8 GHz
<b>Modulation Technique</b>	ASK		FSK	QPSK	FS/QPSK
<b>Radiated power</b>	-		<1W		25mW
<b>Access method</b>	CSMA	Token Ring, CSMA	CSMA		Reservation ALOHA, CSMA
<b>License required</b>	No		No		Yes unless ISM

**Table 1 - Comparison of Wireless LAN Technologies [From 3]**

<sup>16</sup> MAC is the second layer of the protocol stack.

### C. FREQUENCY SPECTRUM FOR IEEE 802.11 WIRELESS PROTOCOL

Standard IEEE 802.11 equipment operates in the unlicensed frequency band called the instrument, scientific and medical (ISM) band that ranges from 2.4 to 2.4835 GHz and the Unlicensed National Information Infrastructure (UNII) 5.2 GHz. It is important to note that household equipment like the microwave ovens and some cordless telephones are also operating in the 2.4 GHz bands, which means there is a potential interference problem. Figure 8 shows the radio frequency spectrum and the electromagnetic frequency characteristics.



**Figure 8 – Electromagnetic Frequency Spectrum**

The standard will allow unconnected client devices to communicate with an Ethernet network through a radio frequency (RF) transmitter that is physically connected to the wired Ethernet. As long as the client is within the transmitter's range, the client is connected (associated) to the network and hence, able to send and receive data. The motivation of IEEE 802.11 is to allow mobility of network hosts in a network. The hosts can be anywhere within the transmitter's range.

Being mobile would incur flexibility in the network topology and hence making the network architecture less dependent of building structure. With IEEE 802.11, extending an existing network is easy. New network hosts can be added as long as the wireless network interface card (NIC) is able to pick up the signal from the access point.

#### **D. DIFFERENT IEEE 802.11 WIRELESS STANDARDS**

With the establishment of the IEEE 802.11, several different specifications were developed. As briefly described, the 802.11 works in different transmission technologies (i.e. IR, DSSS and FHSS), and hence, there is a need for a more precise standard. It leads to the introduction of IEEE 802.11b, which works only in the DSSS modes and it offers a throughput rate up to 11 Mbps. As the predominant standard currently, it is widely supported by vendors such as Cisco, Lucent, Apple, etc. Since then, more specifications were developed as technology mature, particularly IEEE 802.11a and IEEE 802.11g.

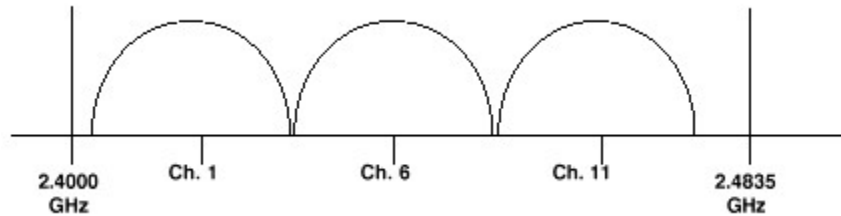
##### **1. IEEE 802.11 Original**

In 1997, the Institute of Electrical and Electronics Engineers (IEEE) created the first WLAN standard. They called it **802.11** after the name of the group formed to oversee its development. Unfortunately, 802.11 only supported a maximum bandwidth of 2 Mbps - too slow for most applications. For this reason, ordinary 802.11 wireless products are no longer being manufactured.

##### **2. IEEE 802.11b**

The original 802.11 standard defines the basic architecture, features, and services of 802.11b. The 802.11b specification affects only the physical layer, adding higher data rates and more robust connectivity. The IEEE 802.11b standard operates in the 2.4 GHz ISM band and utilizes Direct Sequence Spread Spectrum (DSSS). The DSSS technique divides the 2.4 GHz band into 14 twenty-two MHz channels. Adjacent channels overlap one another partially, with 3 of the 14 being completely non-overlapping. Data is sent across one of these 22 MHz channels without hopping to other channels. To compensate for noise on a given channel, a technique called “chipping” is used. Each bit of user data is converted into a series of redundant bit patterns called “chips.” The inherent redundancy of each chip combined with spreading the signal across the 22 MHz channel

provides for a form of error checking and correction; even if part of the signal is damaged, it can still be recovered in many cases, minimizing the need for retransmissions. (Refer to Figure 9).



**Figure 9 - DSSS Non-Overlapping Channels**

To support very noisy environments as well as extended range, 802.11b WLANs use *dynamic rate shifting*, allowing data rates to be automatically adjusted to compensate for the changing nature of the radio channel. Ideally, users connect at the full 11 Mbps rate. However when devices move beyond the optimal range for 11 Mbps operation, or if substantial interference is present, 802.11b devices will transmit at lower speeds, falling back to 5.5, 2, and 1 Mbps. Likewise, if the device moves back within the range of a higher-speed transmission, the connection will automatically speed up again. Rate shifting is a physical-layer mechanism transparent to the user and the upper layers of the protocol stack.

### **3. IEEE 802.11g**

802.11g is an extension of 802.11b and operates in the same 2.4 GHz band as 802.11b. It brings data rates up to 54 Mbps using OFDM<sup>17</sup> (Orthogonal Frequency Division Multiplexing) technology. Because 802.11g is backward-compatible with 802.11b, an 802.11b device can interface directly with an 802.11g access point.

A physical layer standard for WLANs in the 2.4 GHz and 5 GHz radio band. It specifies three available radio channels. The maximum link rate is 54 Mbps per channel, compared with 11 Mbps for 802.11b. The 802.11g standard uses orthogonal frequency-

---

<sup>17</sup> OFDM (Orthogonal Frequency Division Multiplexing) is a method of using many carrier waves instead of only one, and using each carrier wave for only part of the message. OFDM is also called multi carrier modulation (MCM) or Discrete Multi-Tone (DMT). We first describe Multiplexing, then Frequency Division and then Orthogonal. It is important to stress that OFDM is not really a modulation scheme since it does not conflict with other modulation schemes. It is more a coding scheme or a transport scheme.

division multiplexing (OFDM) modulation but, for backward compatibility with 802.11b, it also supports complementary code keying (CCK) modulation and, as an option for faster link rates, allows packet binary convolutional coding (PBCC) modulation.

Speed similar to 802.11a and backward compatibility may appear attractive but these are modulation issues: Conflicting interests between key vendors have divided support within IEEE task group for the OFDM and PBCC modulation schemes. The task group compromised by including both types of modulation in the draft standard. With the addition of support for 802.11b's CCK modulation, the end result is three modulation types. This is perhaps too little, too late and too complex compared with 802.11a. However, there are advantages for vendors looking to supply dual-mode 2.4 GHz and 5 GHz products, in that using OFDM for both modes will reduce silicon cost.

#### 4. IEEE 802.11a

The next wave of wireless products is based on the IEEE 802.11a standard. IEEE 802.11a uses the same MAC layer as 802.11b (including CSMA/CA). The main differences are that the 802.11a standard operates at a higher frequency band and uses a different encoding scheme. The standard operates at the 5 GHz UNII (Unlicensed National Information Infrastructure) band and the total bandwidth is broken into three "domains" for a total of 300 MHz as shown in Table 2.

Frequency	Max Power Output Allowed
5.15 MHz – 5.25 MHz	50mW
5.25 MHz – 5.35 MHz	250mW
5.725 MHz – 5.825 MHz	1 W (outdoor only)

**Table 2 - Frequencies and Power Output in the UNII 5.2 GHz**

Given the same radiated power and encoding scheme used in IEEE 802.11b, transmission in higher frequencies results in shorter reception distances, about 3 – 5 miles<sup>18</sup>. With the higher frequencies, the transmitted signal is more susceptible to multi-path fading. To counter this, 802.11a uses frequency division multiplexing instead of the spread spectrum encoding that 802.11b requires.

---

<sup>18</sup> Broadband Access Platform – Stagg Newman, McKinsey and Company, April 2002 [2]



The encoding is done with "coded OFDM", which was developed specifically for indoor wireless use. COFDM breaks a single 20 MHz channel of a high-speed data carrier into 52 lower-speed sub-carriers. Each sub-channel is approx 300 KHz wide. These sub-channels are then transmitted in parallel. COFDM uses 48 of these sub-channels for data and the remaining four for error correction.

The 802.11a standard specifies that all vendor products must support 6 Mbps, 12 Mbps, and 24 Mbps. Higher data rates are allowed, but not explicitly discussed in the standard. However, the de-facto vendor standard is turning out to be 54 Mbps.

The 54Mbps data rate is achieved by using 64QAM<sup>19</sup> (64-Level Quadrature Amplitude Modulation). This allows for up to 1.125Mbps per 300 KHz sub -channel. With 48 channels the result is a 54Mbps data rate.

At lower speeds, binary phase shift keying (BPSK) is used to encode 125 Kbps per sub-channel, resulting in 6Mbps. Using Quadrature Phase Shift Keying (QPSK), the data rate doubles to 12Mbps. Using 16-level Quadrature Amplitude Modulation (encoding 4 bits per hertz), yields 24Mbps.

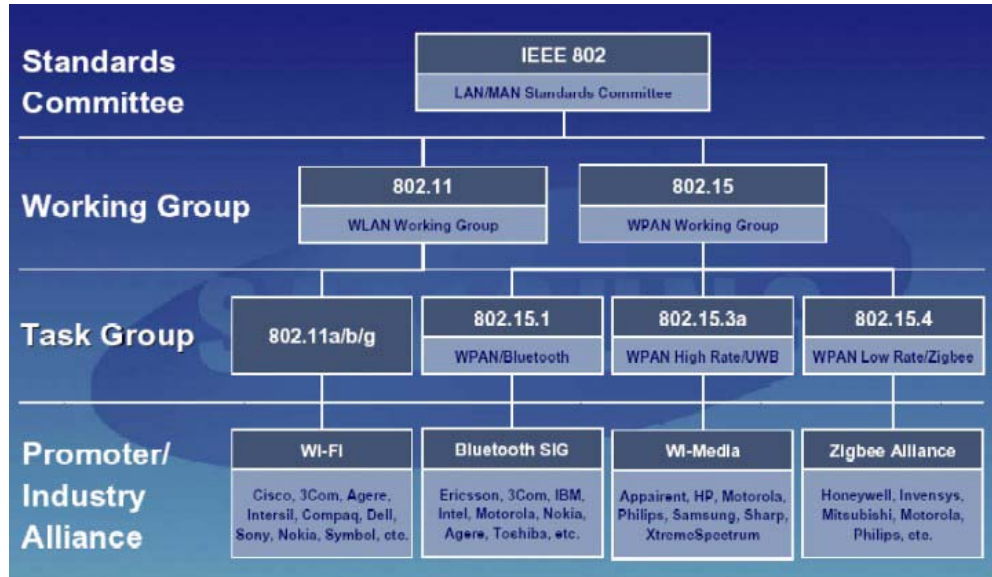
Many proponents of this technology feel that, not only does it provide for greater scalability, it also operates in a much cleaner RF band with less interference than the 2.4 GHz band. However, there are still some issues to consider before worldwide adoption of this new standard. While the UNII band is relatively unpopulated in the United States, the same is not true in other parts of the world.

In Europe, the ETSI (European Telecommunications Standards Institute) is requiring DFS (Dynamic Frequency Selection) and TPC (Transmit Power Control) functionality before allowing unlicensed applications to use the 5 GHz band. These two protocols will allow a client to dynamically change channels and/or use lower power modulation if it sees interference, thus giving existing signals on the band first priority.

---

<sup>19</sup> This digital frequency modulation technique is primarily used for sending data downstream over a coaxial cable network. 64QAM is very efficient, supporting up to 28-mbps peak transfer rates over a single 6-MHz channel. But 64QAM's susceptibility to interfering signals makes it ill suited to noisy upstream transmissions (from the cable subscriber to the Internet).

In Japan, only the lower 100 MHz of the FCC's UNII band is available. This means that users in Japan will only have 5 channels to choose from instead of the 10 that will be available in the United States and Europe<sup>20</sup>.



**Figure 10 - Various IEEE 802.11 Standards and Industry Players**

Over an above the physical standards, there are a number of sub-committees of the IEEE working on functionality such as Quality of Service (QoS), Security, Mobility, and European/Global approvals. It should be noted that most of these advancements would be backward compatible with the current install base of wireless products.

## E. HOW DOES IT WORK

Wireless LAN configurations vary from simple, independent, peer-to-peer connections between a set of PCs, to more complex, intra-building infrastructure networks. There are also point-to-point and point-to-multipoint wireless solutions. A point-to-point solution is used to bridge between two local area networks, and to provide an alternative to cable between two geographically distant locations (up to 30 miles). Point-to-multipoint solutions connect several, separate locations to one single location or building. In a typical wireless LAN infrastructure configuration, there are two basic components:

<sup>20</sup> <http://www.stanford.edu/group/networking/NetConsult/wireless/80211a.html>

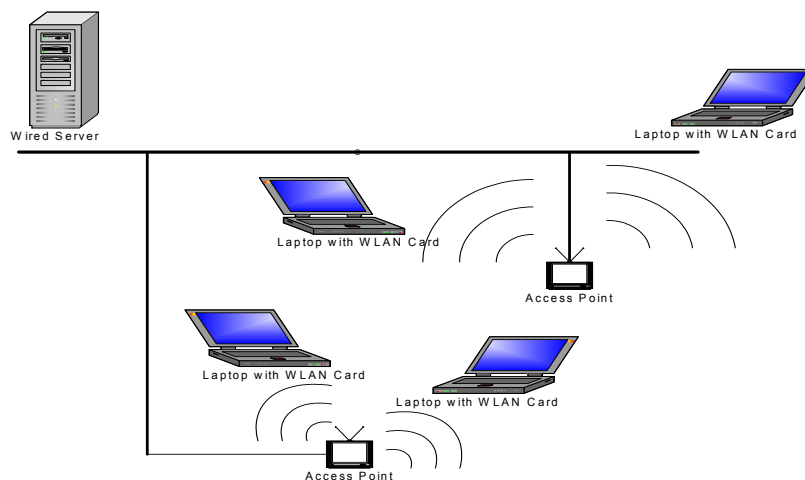
## 1. Access Points

An access point or base station connects to a LAN by means of Ethernet cable or RJ-11 (standard twisted pair port). Usually installed in the ceiling, access points receive, buffer, and transmit data between the wireless LAN and the wired network infrastructure. A single access point supports on average twenty users and has a coverage varying from 20 meters in areas with obstacles (walls, stairways, elevators) and up to 100 meters in areas with clear line of sight<sup>25</sup>. A building may require several access points to provide complete coverage and allow users to roam seamlessly between access points. The access point can essentially be mounted anywhere that is practical as long as the desired radio coverage is obtained. The coverage concept is similar to that of a cell coverage (that is used in the mobile phone technology).

## 2. Wireless Client Adapter

A wireless adapter connects users via an access point to the rest of the LAN. A wireless adapter can be a PC card in a laptop, an ISA or PCI adapter in a desktop computer, or can be fully integrated within a handheld device. The adapters provide an interface between the client network operating system (NOS) and the airwaves (via an antenna). The nature of the wireless connection is transparent to the NOS.

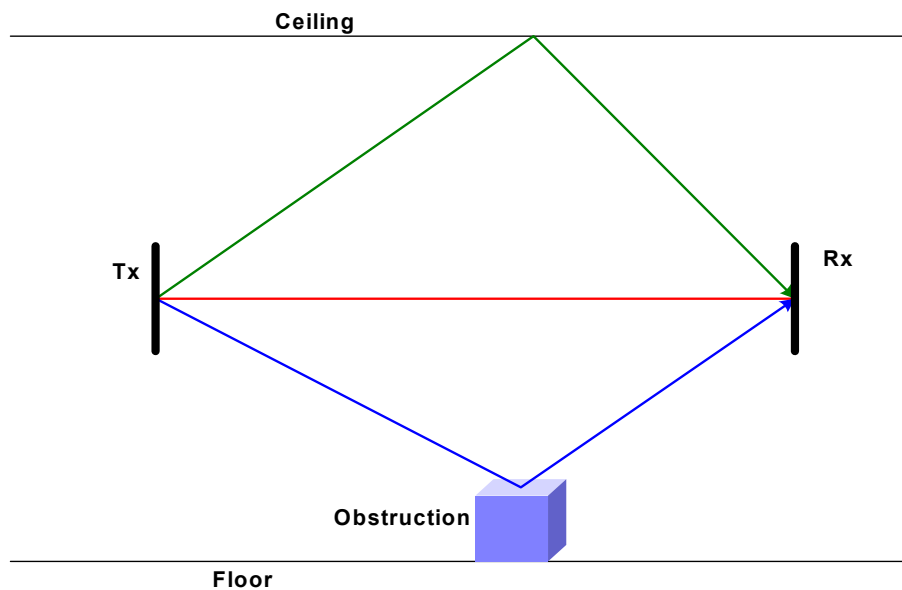
With understandings of the basic components, the basic wireless LAN architecture is as shown in Figure 11.



**Figure 11 - Typical Wireless LAN Configuration**

Wireless LAN uses electromagnetic airwaves (radio and IR) to communicate information from one point to another without relying on any physical connection. Radio waves are often referred to as radio carriers because they simply perform the function of delivering energy to a remote receiver. The data being transmitted is superimposed on the radio carrier so that it can be accurately extracted at the receiving end. This is generally referred to as modulation of the carrier by the information being transmitted. Once data is superimposed (modulated) onto the radio carrier, the radio signal occupies more than a single frequency, since the frequency or bit rate of modulating information adds to the carrier.

Multiple radio carriers can exist in a same space at the same time without interfering with each other if the radio waves are transmitted on different radio frequencies. To extract data, a radio receiver tunes in (or selects) one radio frequency while rejecting all other radio signals on different frequencies.



**Figure 12 - Radio Signals Traveling Over Different Paths [From 4]**

Each radio carrier signal can travel from the transmitter to the receiver in many paths, especially when there are buildings, walls, trees, etc. Figure 12 illustrates the many paths that can be taken by the same radio signal, resulting in different arriving time at the receiver. The time difference can be crucial, as it will cause a phase shift in each of the arrived signal. This phenomenon is known as the multi-path effect. If a signal arrived in

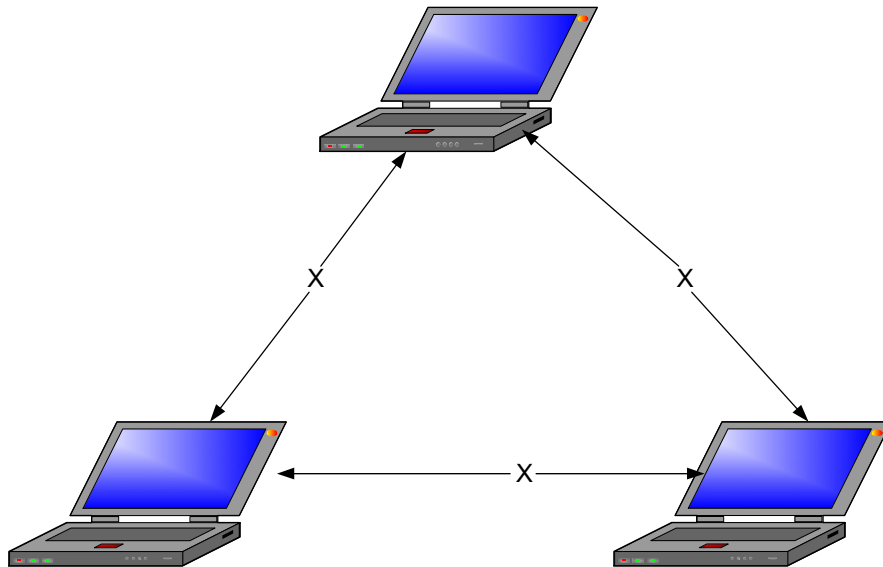
phase at the receiver together with another signal (having taken another path) that arrived out of phase at the receiver, the signal will be cancelled, resulting in total signal loss. OFDM is used to combat this multi-fading effect, hence enhancing the signals' transmission and reducing the bit error rate.

## F. WIRELESS LAN CONFIGURATIONS

Having gone through the basics of a wireless LAN system and understanding the way radio waves travel, this section discusses the various configurations of the wireless LAN.

### 1. Independent Wireless LANs

The simplest wireless LAN configuration is an independent (or peer-to-peer) wireless LAN that connects a set of PCs with wireless adapters. Any time two or more wireless adapters are within range of each other, they can set up an independent network. These on demand networks typically require no administration or pre-configuration.

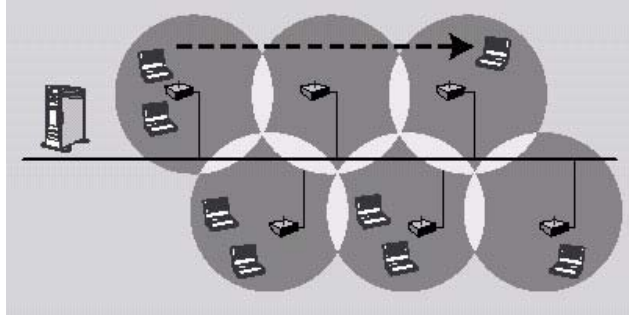


**Figure 13 - Independent Wireless LAN Configuration [From 5]**

By introducing an access point to the independent network, the access point literally acts as a repeater, effectively doubling the distance between wireless PCs.

## 2. Infrastructure Wireless LANs

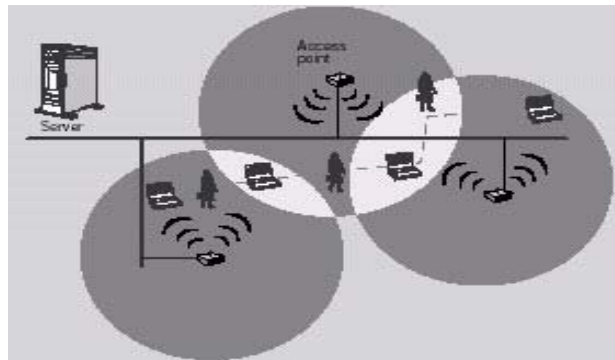
In the infrastructure wireless LANs, multiple access points link the wireless LAN to a wired network and allow users to efficiently share network resources. The access points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple access points can provide wireless coverage for an entire building or campus.



**Figure 14 - Infrastructure Wireless LAN Configuration [From 5]**

## 3. Micro Cells and Roaming

Wireless communication is limited by how far signals carry for the given power output. Wireless LAN uses cells, called micro cells, which is similar to the cellular telephone system to extend the range of wireless connectivity. At any point in time, a mobile PC equipped with a wireless LAN adapter is associated with a single access point and its micro cells, or area of coverage. Individual micro cells overlap to allow continuous communication within the wired network, as illustrated in Figure 15 below. The micro cells handle low power signals and ‘hand off’ users as they roam through a given geographic area.



**Figure 15 - Handing Off Between Access Points [From 5]**

## **G. WIRELESS LAN TECHNOLOGY OPTIONS**

Manufacturers of wireless LAN have a range of technologies to choose from when designing a wireless LAN solution. Each technology comes with its own set of advantages and limitations.

Most wireless LAN system use spread spectrum technology, which is a wideband radio frequency technique originally developed by the military for use in reliable, secure, mission-critical communication systems. Spread spectrum is designed to trade off bandwidth efficiency for reliability, integrity and security. In other words, more bandwidth is consumed than in the case of a narrowband transmission, but the tradeoff produces a signal that, in effect, louder and thus easier to detect, provided that the receiver know s the parameters of the spread spectrum signal being broadcasted. If a receiver is not tuned to the right frequency, a spread spectrum signal looks like background noise. When observed via an oscilloscope, the signal is of no difference with the white noise. By using a wider frequency spectrum, the probability that the data be corrupted or jammed is significantly reduced. Any narrowband jamming will thus affect only a small part of the information falling into the narrowband signal's frequency. The peak power of a spread spectrum signal is also low, hence, making spread spectrum a good choice for wireless technology transmission.

### **1. Frequency Hopping Spread Spectrum (FHSS) [From 6]**

Frequency hopping spread spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short duration impulse noise.

The IEEE 802.11 standard specifies data rates of 1 Mbps and 2 Mbps. In order for a frequency hopping system to be 802.11 compliant, it must operate in the 2.4 GHz ISM band (which is defined by the FCC as being from 2.4 GHz to 2.4835 GHz). Based on the ISM band of 2.4 GHz, the spread of frequency for FHSS is 83.5 MHz and thus, allowing a theoretical maximum of 79 channels.

## **2. Direct-Sequence Spread Spectrum (DSSS) [From 6]**

Direct-sequence spread spectrum is very widely known and the most used of the spread spectrum types, owing most of its popularity to its ease of implementation and high data rates. The majority of wireless LAN equipment on the market today uses DSSS technology. DSSS is a method of sending data in which the transmitting and receiving systems are both on a 22 MHz -wide set of frequencies. The wide channel enables devices to transmit more information at a higher data rate than the FHSS systems.

In the 2.4 GHz ISM band, the IEEE specifies the use of DSSS at a data rate of 1 or 2 Mbps under the 802.11 standard. Under the 802.11b standard, data rates of 5.5 and 11 Mbps are specified. Equipment of the latter standard is able to communicate with the former as the standard provides for backward compatibility. Users employing 802.11 devices do not need to upgrade their entire wireless LAN in order to use 802.11b devices.

## **3. Orthogonal Frequency Division Multiplexing (OFDM) [From 8]**

Orthogonal Frequency Division Multiplexing (OFDM) is special form of multi-carrier modulation, patented in 1970. It is particularly suited for transmission over a dispersive channel. In a multi-path channel, most conventional modulation techniques are sensitive to inter-symbol interference unless the channel symbol rate is small compared to the delay spread of the channel. OFDM is significantly less sensitive to inter-symbol interference, because a special set of signals is used to build the composite transmitted signal. The basic idea is that each bit occupies a frequency-time window, which ensures little or no distortion of the waveform. In practice, it means that bits are transmitted in parallel over a number of frequency-nonselective channels.

## **H. SECURITY IN WIRELESS LAN**

Wireless LANs are not inherently secure; however, if no precautions or configurations for defenses are taken with wired LAN, they are not secure either. The security solution used in wireless LAN is known as Wired Equivalency Protocol (WEP<sup>21</sup>) as specified by IEEE 802.11.

---

<sup>21</sup> WEP uses the RC4 encryption algorithm, which is known as a stream cipher. A stream cipher operates by expanding a short key into an infinite pseudo-random key stream. The sender XORs the key stream with the plaintext to produce cipher text. The



Wired Equivalent Privacy (WEP) is an encryption algorithm used by the Shared Key authentication process for authenticating users and for encrypting data payloads over only the wireless segment of the LAN.

WEP is a simple algorithm that utilizes a pseudorandom number generator (PRNG) and the RC4 stream cipher. The RC4 stream cipher is fast to decrypt and encrypt which saves on CPU cycles, and is also simple enough for most software developers to code it into software.

When WEP is referred to as being simple, it means that it is weak. The RC4 algorithm was inappropriately implemented in WEP, yielding a less-than-adequate security solution for 802.11 networks. Both 64-bit and 128-bit WEP (the two available types) have the same weak implementation of a 24-bit Initialization Vector (IV) and use the same flawed process of encryption. The flawed process is that most implementation of WEP initializes hardware using an IV of 0 – thereafter incrementing the IV by 1 for each packet sent. For a busy network, statistical analysis shows that all possible IVs ( $2^{24}$ ) would be exhausted in half a day, meaning that IV would be re-initialized starting at zero at least once a day. This scenario creates an open door for determined hackers. When WEP is used, the IV is transmitted in the clear with each encrypted packet.

All is not lost with the known weakness as new strengthen security solutions are sought to replace WEP for 802.11 standards. New security standard like 802.1x with EAP is already in consideration to be taken as the security solution for IEEE 802.11.

The 802.1x standard provides specifications for port-based network access control and has been incorporated into many wireless LAN systems has become almost a standard practice among many vendors. With combined with extensible authentication protocol (EAP), 802.1x can provide a very secure and flexible environment based on various authentication schemes. EAP, which was first defined for the point-to-point protocol (PPP), is a protocol for negotiating an authentication method. EAP is defined in RFC 2284 and defines the characteristics of the authentication method including the

---

receiver has a copy of the same key, and uses it to generate identical key stream. XORing the key stream with the cipher text yields the original plaintext.

required user credentials (password, certificate, etc), the protocol to be used, support of key generation and support of mutual authentication.

## **I. CONSIDERATIONS FOR WIRELESS NETWORKING**

Compared with wired LANs, wireless LANs provide installation and configuration flexibility and the freedom inherent in the network mobility. The following issues should be considered when implementing a wireless network.

### **1. Range and Coverage**

Most wireless LAN system uses RF because radio waves can penetrate many indoor walls and surfaces. The range or radius of coverage for a typical wireless LAN system varies from under 100 feet to more than 500 feet. Coverage can be extended, and true freedom of mobility via roaming, provided through micro cells can be achieved.

### **2. Throughput**

Typical data rates range from 1 to 11 Mbps. With the introduction of IEEE 802.11g and 802.11a, data rates are extended to 54 Mbps. Users of traditional Ethernet LANs generally experience little difference in performance when using a wireless LAN and can expect similar latency behavior.

### **3. Integrity and Reliability**

Radio interference can cause degradation in throughput, however such interference is rare in the workplace. Robust designs of proven wireless LAN technology and the limited distance over which signals travel in connections that are far more robust than cellular phone connections and provide data integrity performance equal to or better than wired networking.

### **4. Interoperability with Wired Infrastructure**

Most wireless LAN systems provide industry-standard interconnection with wired systems, including Ethernet (IEEE 802.3) and the Token Ring (IEEE 802.5). Standard-based interoperability makes the wireless portions of a network completely transparent to the rest of the network. Wireless LAN nodes are supported by network operating systems

in the same way as any other LAN node drivers. Once installed, the NOS treats wireless nodes like any other component of the network.

## **5. Interoperability with Wireless Infrastructure**

There are several types of interoperability that are possible between wireless LANs. Products from different vendors employing the same technology and the same implementation typically allow for the interchange of adapters and access points. The goal of industry standards, such as the IEEE 802.11 specifications is to allow compliant products to interoperate without explicit collaboration between vendors.

## **6. Interference and Coexistence**

The unlicensed nature of radio-based wireless LANs means that other products that transmit energy in the same frequency spectrum can potentially provide some measure of interference to a WLAN system. Microwave ovens are a potential concern, but most WLAN manufacturers design their products to account for microwave interference. Another concern is the co-location of multiple WLAN systems. While co-located WLANs from different vendors may interfere with each other, others co-exist without interference.

## **7. Simplicity and Ease of Use**

Users need very little new information to take advantage of wireless LANs. This is because the wireless nature of a WLAN is transparent to a user's Network Operating System (NOS). WLAN products incorporate a variety of diagnostic tools to address issues associated with the wireless elements of the system; however, products are designed so that most users rarely need them. WLAN simplifies many of the installation and configuration issues that plague network managers. Since only the access points of WLANs require cabling, network managers are freed from pulling cables for WLAN end users. Once configured, WLANs can be moved from place to place with little or no modifications.

## **8. Security**

Because wireless technology has roots in military applications, security has long been a design criterion for wireless devices. Security provisions are typically built into

wireless LANs as in the transmission techniques of using FHSS and DSSS. While the new security solution is yet to be formalized by IEEE, it is certain the chosen solution would be much stronger than WEP but in general, individual nodes must be security-enabled before they are allowed to participate in network traffic.

### **9. Implementation Cost**

A wireless LAN implementation includes both infrastructure costs, for the wireless access points, and user costs, for the wireless LAN adapters. The number of access points typically depends on the required coverage region and the number and type of users to be serviced. The coverage area is proportional to the square of the product range. Wireless LAN adapters are required for standard computer platforms, and range in price from \$100 to \$500. The cost of installing the maintaining a wireless LAN generally is lower than the cost of installing and maintaining a traditional wired LAN.

### **10. Scalability**

Wireless networks can be designed to be extremely simple or quite complex. Wireless networks can support large number of nodes and large physical areas by adding access points to boost or extend coverage.

### **11. Battery Life for Mobile Platform**

End user wireless products are capable of running off the battery power from their host notebook or handheld computer. Wireless LAN vendors typically employ special design techniques to maximize the host computer's energy usage and battery life.

### **12. Safety**

The output power of wireless LAN systems is very low, much less than that of a handheld cellular phone. Since radio waves fade rapidly over distance, very little exposure to RF energy is provided to those in the area of a wireless LAN system. Wireless LAN must meet stringent government and industry regulations for safety. No adverse health effects have ever been attributed to wireless LANs.

## **IV. FREE-SPACE OPTICS TECHNOLOGY**

This section will introduce the FSO technology that will include description of different components that made up the FSO systems. In addition, various FSO implementation issues, FSO security aspects, advantages and limitations of using FSO will be covered in this section.

The second wireless technology available is Free-Space Optics (FSO). FSO technology that overlaps the optical and wireless categories has long been under development yet it has not achieved acceptance as a standard access option for providers. FSO vendors have done a good job emphasizing the technology's advantages of being cost-effective and easy to deploy, but they have had difficulty convincing service providers of the technology's viability and marketability. In early market trials, weather and other obstacles resulted in not-so-great signal availability, and providers quickly categorized FSO as more of a "back-up" solution or one that only works well in a campus environment.

Deployment of FSO networks has picked up recently, although much faster outside the U.S. Vendors see many more requests for information coming from carriers rather than enterprise customers (the reverse trend of a year ago). This chapter shall discuss the FSO technology in details.

### **A. OVERVIEW**

The invention and application of fiber optics has significantly changed the course of telecommunications around the world. Fiber optic cables connect all major countries and continents around the world, enabling the ultra high-speed transfer of data voice, video signals and of course the Internet. Fiber optic cables are also used in all telecommunication switches, i.e. the central office. What is lacking, as discussed in the previous chapters, is the high-speed communication line between these central offices

and the homes. Today, about 5% of the commercial buildings in the US are connected to fiber optics for high bandwidth services, and the percentages are even smaller in Asia and other parts of the world.

Free-Space Optics (FSO), also known as free-space photonics, is the technology whereby the voice, video and data can be transmitted through the atmosphere using modulated visible or infrared beams. Laser beams are generally used and preferred in the industry, although non-lasing sources such as Light Emitting Diodes (LEDs) or InfraRed Emitting Diodes (IREDS) will serve the purpose.

Through the use of Free-Space Optics, broadband communication can be achieved, just like fiber optics transmission. The difference is that Free-Space Optics uses air as the transmission medium instead of fiber or glass. At the source, the visible or infrared energy is modulated with the data to be transmitted. While at the destination, the beam is received by a photo-detector, the data is extracted from the visible or IR beam (demodulated), and the resulting signal is amplified and sent to the hardware.

Free-Space Optics requires line of sight (visual) between the source and the destination. In cases where by there is no line of sight, strategically positioned mirrors can be used to reflect the energy. The beams can pass through glass windows with little or no attenuation (as long as the windows are clean). Depending on the type of source used and the visibility condition of the atmosphere, Free-Space Optics systems can function over distances of several kilometers.

Nowadays, Free-Space Optics is becoming more and more popular, as Free-Space Optics equipment is being deployed for a variety of applications, including last-mile connections to buildings, mobile networks assist, network backup and emergency relief. Marketing experts estimated that global equipment revenues in the Free-Space Optics market are projected to reach \$2 billion in year 2005, up from less than \$100 million in year 2000.

## **B. BRIEF HISTORY OF FREE-SPACE OPTICS**

Free-Space Optics (FSO) uses lasers to transmit data, voice and video communications through the air, allowing optical connectivity without laying fiber or securing spectrum licenses.

The idea of using lasers to transmit data through the air first attracted widespread interest in the 1960s, when scientists started developing applications for the military. With the Cold War in full bloom, physicists on both sides of the Iron Curtain were looking for ways to offer secure, high-speed communications. The properties of light - its ability to carry information great distances at high speeds with little degradation of the signal - also intrigued scientists developing communications for space exploration. These laser-based FSO communications had potential benefits well beyond other wireless technologies - including security levels and data rates beyond those that could be obtained using existing radio frequency (RF) solutions. However, many of these programs did not fully materialize due to funding cuts and changing priorities.

However, after Corning researchers Robert Maurer, Donald Keck and Peter Shultz developed the first optical fiber capable of transmitting information over long distances, physicists began focusing more on the properties of optical cable. The study of optical transmissions through the air continued, but the industry focused more on developing land-based fiber optics.

By the early 1990s, researchers again started focusing on FSO technology. Developments in optics and lasers drove down the price of components, making FSO a cost-effective approach to addressing the skyrocketing demand for broadband services.

Recent developments in the technology have advanced it from a short-term solution for short-haul bridges to a viable alternative for helping service providers deliver the promise of optical networks. The increasing demand for high bandwidth "now" in the metro networks - as service providers clamor for a wide range of applications, including metro network extension, enterprise LAN-to-LAN connectivity, wireless backhaul and

LMDS supplement - has caused an imbalance, a "connectivity bottleneck". Service providers are faced with a need to turn up services quickly and cost effectively, at a time when capital expenditures are restrained.

As an optical technology, FSO is a natural extension of the metro optical core. FSOs bring optical capacity to the edge of the network, allowing end users to connect with technology that is cost-effective, reliable and quickly installed.

### C. HOW FSO WORKS

Free-Space Optics is a technology similar to fiber optic cable infrastructure except that no cable is involved. The light pulses are transmitted through the atmosphere in a small conical shaped beam by the means of low powered lasers or LED's. It is hence a point-to-point, line of sight method for delivering high data rate through optical signals, using the free space as a medium. Instead of focusing the output of a laser into a strand of optical fiber, the output is broadcast in a thin beam across the sky, at the receiving unit.

#### 1. Operating Frequency Band

FSO equipment usually operates in two ranges of wavelength - one is between 780 nanometers (nm) to 900 nm and the other is between 1550 nm to 1600 nm. The visible light spectrum is between 380 nm to 740 nm.

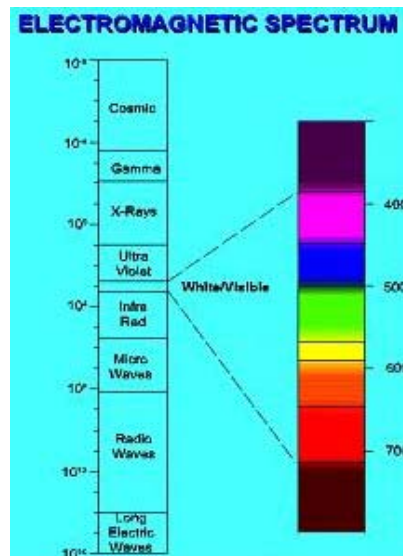


Figure 16 – Visible Light Spectrum [From 8]

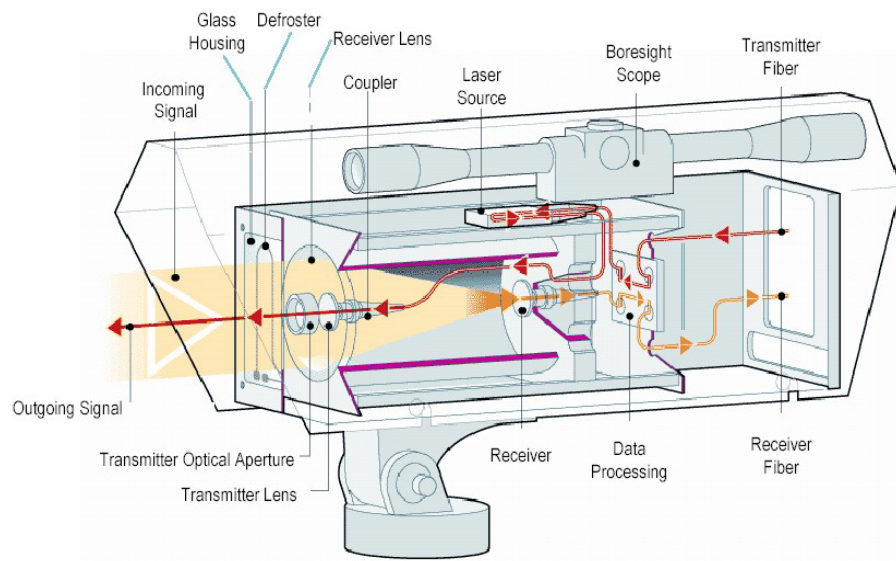


Most FSO vendors do not use the 1300 nm window, which is used in fiber optics because it has poor transmission characteristics through atmospheric conditions. Of the two operating frequency range, the 1500 nm laser would be better in terms of power, distance and eye safety. IR radiation at 1500 nm tends not to reach the retina of the eye, being mostly absorbed by the cornea. Regulations accordingly allow these longer wavelength beams to operate at higher power than the 800 nm beams, by about two orders of magnitude. With this increase in power, it can boost the link lengths by a factor of at least five while maintaining sufficient signal strength for proper link operation.

Alternatively, it would be able to boost data rate considerably over the same length of link. So for high data rates, long distances, poor propagation conditions, or combination of these conditions, the 1550 nm operating frequency range can be rather attractive, but of course, it is at the expense of the cost of equipment, which is much more expensive than those operating at 800 nm. The smaller wavelength (850 nm) is about one-tenth the price of the larger (1550 nm) wavelength to manufacture.

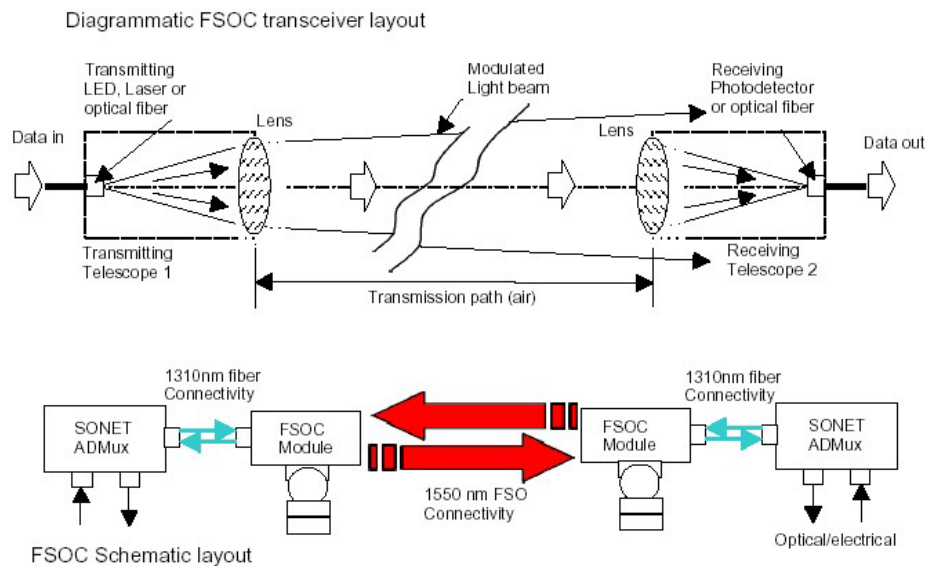
## 2. Description of the Transceiver

Normally, an FSO link refers to a pair of free space transceivers that are called link heads, aiming beam at one another and creating a full-duplex communication link. Figure 17 shows a typical link head.



**Figure 17 - Typical Link Head for FSO [From 9]**

In its simplest form, FSOC is the transmission and reception of modulated light through the air rather than through a fiber. Well known examples of FSOC systems are TV remote controllers and infrared (IRDA) wireless links for office printers and PDA's. For a telecommunications application, an FSOC link would typically consists of two adjustably mounted telescopes facing each other at opposing ends of a transmission path as shown in Figure 18. A LED, laser diode or network fiber (producing a data modulated optical output), is placed at the focal point one of these telescopes (telescope 1). The telescope lens captures the modulated light produced from the optical transmitter. The lens projects the light as a collimated or semi-collimated light beam toward the distant telescope (telescope 2). The lens of telescope 2 captures a percentage of the transmitted light and brings this light to focus at telescope 2's focal point. At telescope 2's focal point, a photo detector or optical fiber is positioned to receive this focused light. The arriving photons are converted back into electrons in the case of the focal plane photo detector, or conveyed (by the optical fiber), to other remote optoelectronics. As long as the telescopes stay well aligned to each other, the transmission path is reasonably short (< 5 km), and the transmission path is clear of obstructions and attenuators, the optical link is capable of transmitting multiple tens of gigabits of data, video, multimedia and voice traffic per second.



**Figure 18 - Diagrammatic FSO Communication Layout [From 10]**

#### **D. FSO IMPLEMENTATION ISSUES**

As mentioned, a strict line-of-sight needs to be maintained within the link at all times for optimal operation in FSO. As such, a thorough pre-installation site evaluation must be done to ensure that the paths between the Free-Space Optics units are clear and will remain so for a number of years. One of the main issues with the technology is that fog and severe weather can have a detrimental impact on the performance of the Free-Space Optics systems. The main factor is fog, with rain and snow also affecting to the maximum distances that can be achieved.

When planning a Free-Space Optics system, it is recommended that the city's fog table is revealed and the anticipated distance of the connection. The vendor's product specifications should be used to ensure that the product would perform in a satisfactory manner for the connection. One other factor involved in limiting the distance of the connections is the atmosphere itself. As the beam goes through small pockets of differing variations in air temperature and wind speed the light can be refracted off course. Since these variations are physically very small, most vendors will use multiple lasers in parallel on the Free-Space Optics system to compensate, especially on units designed for longer distances.

Figure 19 shows a table taken from Reference [11] on the Optical Access web site and is representative of the impact of fog and bad weather on the operational distance of a Free-Space Optics system. The table shows also the distance achieved and signal loss ratio based on the fog condition and visibility.

Weather condition	Precipitation		Visibility	dB loss/ km	TerraLink 8-155 Range			
		mm/hr						
Dense fog			0 m					
			50 m	-315.0	140 m			
Thick fog			200 m	-75.3	460 m			
Moderate fog			500 m	-28.9	980 m			
Light fog	Snow	Cloudburst	100	770 m	-18.3	1.38 km		
				1 km	-13.8	1.68 km		
Thin fog	Snow	Heavy rain	25	1.9 km	-6.9	2.39 km		
				2 km	-6.6	2.79 km		
Haze	Snow	Medium rain	12.5	2.8 km	-4.6	3.50 km		
				4 km	-3.1	4.38 km		
Light Haze	Snow	Light rain	2.5	5.9 km	-2.0	5.44 km		
				10 km	-1.1	6.89 km		
Clear		Drizzle	0.25	18.1 km	-0.6	8.00 km		
				20 km	-0.54	8.22 km		
Very Clear						23 km	-0.47	8.33 km
						50 km	-0.19	9.15 km

**Figure 19 - Impact of Fog and Bad Weather on the Operational Distance of a Free-Space Optics System [From 11]**

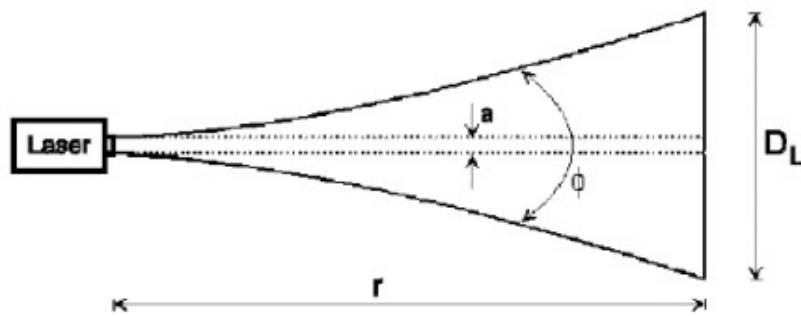
Since RF (radio frequency) wireless systems like the ones based on the 802.11b standard are not affected so much by fog, some manufacturers are using these as a redundant system and have incorporated them into their Free-Space Optics systems. The growth of trees and the construction of buildings need to be considered along with any aesthetic issues and required permits. The units can be mounted on building tops, sides and even behind windows. Speeds range from single T-1<sup>22</sup> and 10 Mbps to 2.5 Gbps on currently available products. 40 Gbps has been successfully tested in laboratories; speeds could potentially be able to reach into the Terabit range.

<sup>22</sup> T-1 line is a dedicated phone connection supporting data rate of 1.544Mbps per second. A T-1 line actually consists of 24 individual channels, each of which supports 64Kbits per second. Each 64Kbit/second channel can be configured to carry voice or data traffic. Most telephone companies allow you to buy just some of these individual channels, known as *fractional T-1* access. T-1 lines are a popular leased line option for businesses connecting to the Internet and for Internet Service Providers (ISPs) connecting to the Internet backbone. The Internet backbone itself consists of faster T-3 connections.

## E. COUNTERING DIFFICULTIES

A common difficulty that arises when deploying Free-Space Optics links on tall buildings or towers is sway due to wind or seismic activity. Both storms and earthquakes can cause buildings to move enough to affect beam aiming. The problem can be dealt with in two complementary ways: through beam divergence and active tracking.

With beam divergence, the transmitted beam is purposely allowed to diverge, or spread, so that by the time it arrives at the receiving link head, it forms a fairly large optical cone.



$$D_L = \sqrt{a^2 + r^2 \phi^2} \text{ where}$$

$$D_L = \sqrt{a^2 + r^2 \phi^2} \text{ - Beam Diameter}$$

$a$  - Beam Diameter

$r$  - Range

$\phi$  - Beam Divergence

**Figure 20 - Beam Divergence [From 11]**

As shown in Figure 20, the beam divergence can be calculated based on the given formula. The result will be able to give FSO network designers a fairly good estimate. Depending on product design, the typical Free-Space Optics light beam subtends an angle of 3 to 6 milli-radians (10 to 20 minutes of arc) and will have a diameter of 3 to 6 meters after traveling for 1 km. If the receiver is initially positioned at the center of the beam, divergence alone can deal with many perturbations. This inexpensive approach to maintaining system alignment has been used quite successfully by the FSO vendors.

If however, the link heads are mounted on the tops of extremely tall buildings or towers, an active tracking system may be required. More sophisticated and costly than beam divergence, active tracking is based on movable mirrors that control the direction in which the beams are launched. A feedback mechanism continuously adjusts the mirrors so that the beams stay on target. These closed loop systems are also valuable for high-speed links than span long distances. In those applications, beam divergence is not a good approach. By its very nature, it reduces the beam power density just when receivers, being less sensitive at high data rates, need all the power they can get.

#### **F. FREE-SPACE OPTICS SECURITY**

FSO transmissions are inherently hard to intercept. Unlike microwave radio transmissions whose signal propagates across a large area, FSO systems use a very narrow beam spread (1-11 milli-radian) that cannot be easily intercepted. With most FSO installations on top of buildings and the narrow beam spread, a person wishing to tap the beam would have to be very high in the air to reach the bottom edge of the beam. Unlike microwave systems that can be easily detected from the ground with relatively inexpensive frequency laptop scanners, infrared light is invisible and provides inherent difficulty in laser beam location detection. Even with an infrared viewer, a laser beam cannot be seen unless you are physically in direct view of the laser beam - which is high in the air for most FSO installations. With the LOS requirements for FSO communications links, laser beam interception is practically impossible without detection. If someone wishes to tap the line and put a mast to intercept the light signal between the LOS, they will interrupt the signal at which point data transmissions cease and are detected via network monitoring. The diffraction characteristics of RF transmissions may make it possible to intercept the microwave signal and direct a portion of it to the receiving antenna to avoid link disruption.

Encryption equipment could also be used on each end to encrypt and decrypt data. It would be very difficult to find encryption devices that could support the speeds that Free-Space Optics are capable of, but it is an alternative. In doing research for this paper an interesting technology was discovered that is currently under development. It involves

applying a varying analog input to a laser and the laser responding by transmitting a digital chaotic output. The theory is that if the receiving end had a similar analog input the chaotic signal could be decrypted. Any device intercepting the signal would view it as being chaotic and could not discern a pattern or be able to crack an encryption algorithm. This technology could potentially be used on Free-Space Optics equipment making encrypted high-speed connections a reality.

## **G. ADVANTAGES OF USING FREE-SPACE OPTICS**

Free-space optical wireless has relatively more than just cost-effectiveness to offer the world of networking. Many of the benefits are experienced through better, faster, more ubiquitous service. With the ability to create links quickly and economically, optical wireless complements existing services including cable, DSL, radio and microwave.

The lower initial outlays also allow service providers to build out their networks at unprecedented speeds and extend them to isolated areas. In sparsely populated locales, few providers can justify bringing fiber close enough to offer high-speed services. But optical wireless complements these services by taking the place of fiber, making it economical to extend service areas and making it possible to cross previously difficult terrain.

And optical wireless also allows service provider to pay off the initial expense in a matter of months with no licensing or leasing fees. Easy, fast deployment and lower link costs for service providers spell better service to homes and businesses. Optical wireless is also known as "Free-space" optics. This is the part of the electromagnetic spectrum not regulated by government agencies. A Free-space optical link transmits information through the atmosphere on beams of light created by lasers. The beams of light are similar to those created by the TV remote and are perfectly safe to the skin and eyes.

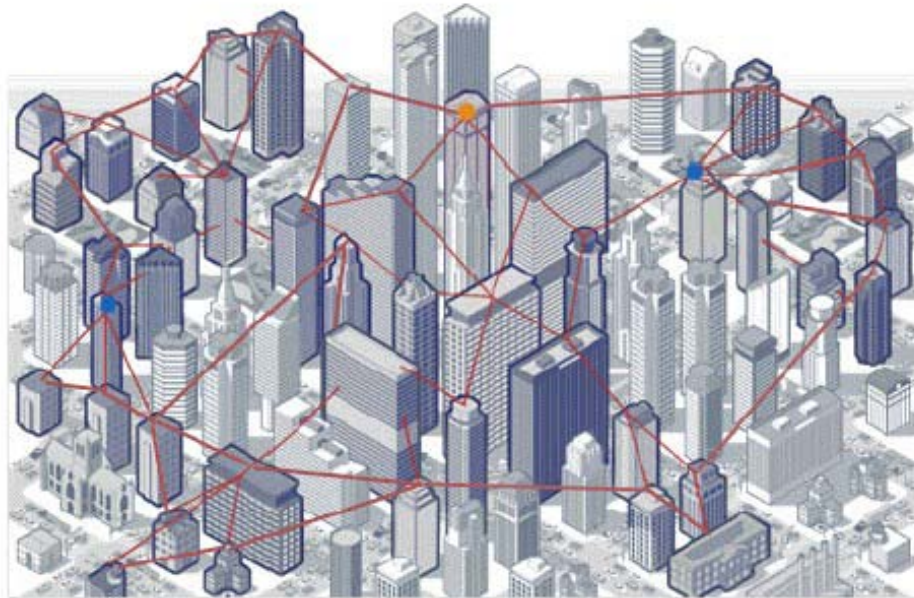
### **1. High Speed Broadband Access**

Free-Space Optics (FSO) utilizes advanced wireless optical technologies to bridge the last-mile in carrier networks and makes high-speed broadband access a reality. Based

on optical technology, it provides levels of bandwidth comparable to fiber optic cable. With current availability of up to 1.25 Gbps<sup>23</sup>, throughputs of hundreds of Gbps are possible in the future.

## 2. Low Cost Bypass of Copper Infrastructure

FSO solutions enable service providers to dramatically lower their cost of providing high-speed broadband access to end-users compared to other commercially available last mile<sup>24</sup> solutions. This is because it does not involve the expensive process of obtaining rights-of-way, licenses, or permits from governments, digging the ground to lay cable, or charges for spectrum rights. All that while maintaining costs that are lower than traditional infrastructure. FSO offers a return on investment of weeks or a couple of months, versus the years it takes for other solutions. An example of implementing FSO in bypassing the copper wire infrastructure is as shown in Figure 21.



**Figure 21 - Bypassing Copper Wire Infrastructure [From 12]**

---

<sup>23</sup> Gbps stands for *billions of bits per second* and is a measure of bandwidth on a digital data transmission medium such as optical fiber. With slower media and protocols, bandwidth may be in the Mbps (millions of bits or megabits per second) or the Kbps (thousands of bits or kilobits per second) range.

<sup>24</sup> Last-mile technology is any telecommunications technology, such as wireless radio, that carries signals from the broad telecommunication along the relatively short distance (hence, the "last mile") to and from the home or business. Or to put it another way: the infrastructure at the neighborhood level. In many communities, last-mile technology represents a major remaining challenge to high-bandwidth applications such as on-demand television, fast Internet access, and Web pages full of multimedia effects.



### **3. Rapid Deployment and Service Provisioning**

FSO optical wireless products enable service providers to avoid time-consuming processes, such as obtaining rights-of-way, and other governmental licenses, or the labor-intensive process of digging and installing cables in the ground. As a result, FSO can be installed and made operational in a few hours. Using available Network Management Systems, service providers can efficiently and cost-effectively perform provisioning from a central location through a point-and-click graphical user interface, thus eliminating time consuming onsite service calls or "truck-rolls".

### **4. Improved Availability and Reliability**

FSO can be deployed to operate over an optical mesh architecture that allows transmission between any two points on the network and enables full traffic re-routing around a failed link. The short mesh configuration enables the wireless link to remain connected in all types of weather.

### **5. Improved Scalability and Flexibility**

An FSO solution can be designed to scale efficiently as demand for bandwidth and new services grow, therefore initial deployment is also cost effective.

### **6. Creation of New Revenue Opportunities for Service Providers and Carriers**

Service providers and carriers are able to rapidly introduce new upgrades, thanks to available software and system-based products. Features include new service level agreements, Quality of Service enhancements, dedicated wavelengths to the end users, and bandwidth on demand, without significant hardware changes or additions.

Depending on the bandwidth requirements, FSO may be the lowest cost technology. One way to view the cost advantage of FSO is to compare it to leased line costs.

## **H. LIMITATIONS OF FREE-SPACE OPTICS**

For Free-Space Optics, challenges to achieving this level of performance take the shape of environmental phenomena that vary widely from one micrometeorological area to another. Included here is scintillation, scattering, beam spread, and beam wanders.

Scintillation is best defined as the temporal and spatial variations in light intensity caused by atmospheric turbulence. Such turbulence is caused by wind and temperature gradients that create pockets of air with rapidly varying densities and therefore fast-changing indices of optical refraction. These air pockets act like prisms and lenses with time-varying properties. Their action is readily observed in the twinkling of stars in the night sky and the shimmering of the horizon on a hot day.

FSO communications systems deal with scintillation by sending the same information from several separate laser transmitters. These are mounted in the same housing, or link head, but separated from one another by distances of about 200 mm. It is unlikely that in traveling to the receiver, all the parallel beams will encounter the same pocket of turbulence since the scintillation pockets are usually quite small. Most probably, at least one of the beams will arrive at the target node with adequate strength to be properly received. This approach is called spatial diversity, because it exploits multiple regions of space. In addition, it is highly effective in overcoming any scintillation that may occur near windows. In conjunction with a design that uses multiple and spatially separated large-aperture receive lenses, this multi-beam approach is even more effective.

Dealing with fog, more formally known as Mie scattering<sup>25</sup>, is largely a matter of boosting the transmitted power, although spatial diversity also helps to some extent. In areas with frequent heavy fogs, it is often necessary to choose 1550 nm lasers because of the higher power permitted at that wavelength. Also, there seems to be some evidence that Mie scattering is slightly lower at 1550 nm than at 850 nm. However, this assumption has recently been challenged, with some studies implying that scattering is independent of the wavelength under heavy fog conditions. Nevertheless, to ensure carrier-class availability for a single FSO link in most non-desert environments, the link length should be limited to 200-500 meters. Other atmospheric disturbances, like snow and especially rain, are less of a problem for Free-Space Optics than fog.

---

<sup>25</sup> Mie theory provides rigorous solutions for light scattering by an isotropic sphere embedded in a homogeneous medium.

## **V. PRESENT OPERATING CONCEPT AND PRESENT ENCOUNTERED PROBLEMS**

### **A. OVERVIEW**

The previous four chapters gave detail descriptions of the F-16 aircraft, portable maintenance aid (EDNA) and the ALR-69 systems. In addition, two state-of-art wireless technologies, i.e., IEEE 802.1x and Free-Space Optics, were also explained. This chapter starts by giving a brief history of the Republic of Singapore Air Force (RSAF) since it gained independence on 9<sup>th</sup> of August 1965. In addition, this chapter will also introduce the location of the various airbases in Singapore and the basic layout of a typical flight line operational environment. It will then discuss the operational concept for loading the critical data file onto the ALR-69 system operation onboard the F-16 aircraft, in the maintenance crews' aspects. A typical scenario is used to illustrate the operational time required to prepare the ALR-69 systems with the latest critical data file prior to the flight. This will be crystallized in a timing chart to demonstrate the long lead time required and also discuss the potential problems that RSAF is currently facing for using the present method of loading critical data file onto the EDNA prior to loading to the ALR-69 systems onboard the F-16 aircraft.

### **B. BRIEF HISTORY OF REPUBLIC OF SINGAPORE AIR FORCE (RSAF)**

Situated at an important crossroads in the heart of Southeast Asia, Singapore is a vital economic link between the rapidly industrializing economies of East Asia and Europe and the Middle East. Just over 600 square kilometers in area, Singapore achieved its independence from firstly, British colonial rule and then Malaysia (Malaya) on the 9<sup>th</sup> of August 1965. Initially, air defense responsibilities fell on the shoulders of the Royal Air Force (RAF) with assets such as the Lightning, Javelin and Hunters in RAF markings a common sight around Singapore's airbases. However, with economic difficulties besetting the UK in the late 1960s, the then Labor Government in London decided in 1971 that all British forces were to be pulled out, thrusting the responsibility of defending the small island state on its citizens shoulders.



**Figure 22 - Two of RSAF's Hunter Mk. 47s Taking Off [From 12]**

With the impending British pullout imminent, the Singapore Air Defence Command (SADC) was set up in 1968. Pilots were initially trained with aircraft borrowed from the Singapore Flying Club. By May 1969, eight Cessna 172s, the SADC's first aircraft, were purchased to serve as basic trainers. These were soon followed by SADC's first rotary winged assets, eight Aerospatiale Alouette III utility helicopters flown by a pool of French trained pilots. The arrival of 16 BAC 167 Strikemaster trainer/light-attack aircraft heralded the dawn of the SADC's jet age.



**Figure 23 - Crewmen Posed with a BAC 167 Strikemaster [From 12]**

The next big event in the SADC's annals was the delivery of the first of 47 Hawker Hunters (34 FGA Mk74s for ground attack, 4 FR Mk74s for reconnaissance and 9 TMk75s 2-seat trainers) from the UK in the September of 1970. With the Five-Power Defence Arrangement (FPDA), consisting of Singapore, Malaysia, Australia, New

Zealand and the UK, being set up in early 1971, the SADC was ready to take over the reins of Singapore's air defence by the time of the final British pullout in September 1971.

Inheriting the former RAF bases at Tengah, Sembawang, Seletar and Changi, the SADC received a further boost in the form of 40 ex-US Navy A-4B/C Skyhawk fighter-bombers in the April of 1974. These aircraft were brought up to A-4S standard and with follow-up orders; the Skyhawk is today numerically the most important aircraft in Singapore's inventory with 120 airframes (though only 60-70 are serviceable) serving with 2 squadrons. By 1975, the SADC was renamed the Republic of Singapore Air Force (RSAF) and became a separate branch of the armed forces.



**Figure 24 - A Pair of Skyhawks In Formation. Aircraft 687 is a TA-4S Advanced Trainer With a Separate Canopy for the Instructor, a Feature that Makes the RSAF's TA-4 Unique in the World [From 12]**

From the 1980s onwards, the RSAF underwent great changes. Most facilities at the former RAF base at Changi made way for the new civilian airport and transferred to the previous civilian airport at Paya Lebar. New aircraft types such as the F-5E/F Tiger II and S-211 advanced trainer were added in the late 1970s/early 80s. Concurrently, a shift in emphasis from strength to technology was reflected by recent purchases such as the F-16 Fighting Falcon and E-2C Hawkeye Airborne Early Warning (AEW) aircraft. At the same time, Singapore Aerospace (SAe) was set up to undertake various projects

involving the aviation industry in Singapore. These have included upgrading the Skyhawk to the A-4SU Super Skyhawk with a brand new avionics fit and the F-404 engine as used by the F/A-18 Hornet. SAe has also assembled Aerospatiale AS332 Super Pumas helicopters and SIAI Marchetti S-211 trainers for the RSAF, which were delivered in kit form from their respective manufacturers.



**Figure 25 - RF-5E Tiger [From 12]**

With more F-16s on order and projects underway to upgrade the existing F-5s, the RSAF is set to face challenges unique to a small force. Shortage of land means that the RSAF has had to relocate part of its training assets overseas. At the same time it has boosted its interaction with foreign air forces leading to a marked increase in exercises with these foreign air forces, both locally and overseas.

In January of 1985, the government of Singapore ordered eight F-16/79 fighters and took an option for 12 more. The F-16/79 was a cost-reduced version of the Fighting Falcon powered by the General Electric J79 turbojet rather than the F100 turbofan. In mid-1985, it became apparent that the F100-powered version would be made available, and Singapore changed its order to eight F-16A/B Block 15 OCU aircraft (four single-seaters and four two-seaters). This purchase was under the *Peace Carvin* Foreign Military Sales program, and was intended to replace the aging Hawker Hunters still serving with the Republic of Singapore Air Force.



Singapore took delivery of its first Pratt & Whitney F100-PW-220 powered F-16 (a two-seater) on February 20, 1988 [13]. Although all aircraft are Block 15 models, they actually have strengthened Block 30 airframes. The machines were initially delivered to Luke Air Force Base, where the RSAF trains its F-16 pilots. Singapore also leased nine F-16As previously used by the Thunderbirds flight demonstration team, for use at Luke Air Force Base. Subsequently, Peace Carvin II and Peace Carvin III programs were carried out and at present, RSAF is training in Luke Air Force Base and Cannon Air Force Base in the United States of America.

### C. AIRBASES IN SINGAPORE



**Figure 26 - Airbases in Singapore [From 15]**

There are four airbases in Singapore, namely Tengah Airbase, Sembawang Airbase, Seletar Airbase and Paya Lebar Airbase. Changi is Singapore's International airport and is used primarily for commercial aircraft.



**Figure 27 - Logo of Paya Lebar and Tengah Airbase Respectively**

Of the four airbases, Tengah Airbase houses the F-16 and A-4SU aircraft. This is the primary fighter aircraft Airbase located in the northwestern part of the Singapore Island. The other fighter aircraft Airbase, Paya Lebar Airbase, houses the C-130 Hercules and F-5 aircraft. The Sembawang Airbase is known to be a helicopter airbase and houses various types of helicopter, namely Fennac, Super Puma, Chinook and UH1H Bell. The trainer aircraft is based in Seletar Airbase located in the eastern part of the Singapore Island.

#### **D. BASIC LAYOUT OF FLIGHT LINE OPERATING ENVIRONMENT**

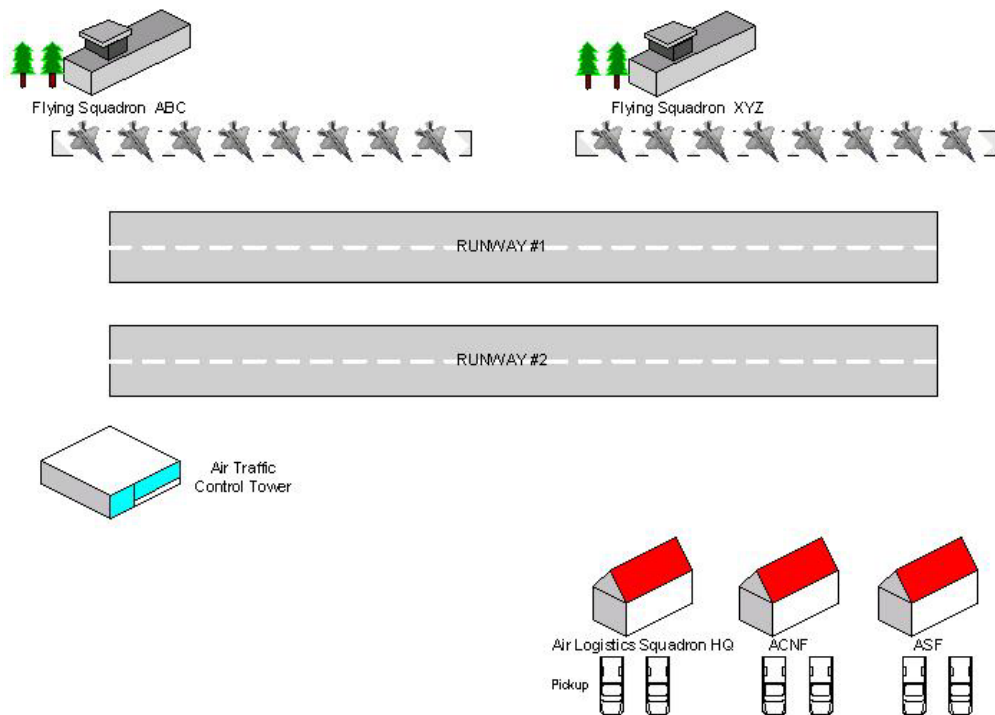
A typical airbase consists of several flying squadrons and one Aircraft Logistics Squadron (ALS). The flying squadron is lead by a squadron commander, usually called Squadron Commanding Officer, and he is a pilot by vocation. He is in-charge of the pilots under his squadron, including, limited ground support crews seconded to the flying squadron to support the preparation of the aircraft prior to flight, receiving the aircraft after flight and also weapon load crews. The weapon load crews are responsible for the loading, arming and unloading of ammunition on the aircraft. This group of ground support crews is not responsible for the maintenance of aircraft defects, normally called snag. The pilot will log the defects into the aircraft logbook and it is the responsibility of the technicians and engineers from the Air Logistics Squadron to rectify the snag and to recover the aircraft for follow-on flight.

Air Logistics Squadron (ALS), supports the 'O', 'I' and limited 'D' level maintenance of the aircraft within the airbase. ALS is commanded by a Commanding Officer (CO ALS), usually an engineer by vocation and is supported by two deputy squadron commanders, namely Deputy Commanding Officer (Mechanical) – DyCO (M) and Deputy Commanding Officer (Electrical) – DyCO (E). Under the chain of command in ALS, there are several flights, each supporting the various components on the aircraft. Just to name a few, the flights are Electrical Instrument Flight (EIF), Propulsion Flight (PrF), Air Communications and Navigation Flight (ACNF), Air System Flight (ASF), etc. The respective flights are in-charge of a particular group of components within the



aircraft and are headed by a Officer Commanding (OC). The Air System Flight (ASF) in the Air Logistics Squadron maintains the subject topic of this thesis, the ALR-69 systems and the EDNA.

The flying squadrons are located within close proximity to the airfield, where the aircraft takes off and land. On the other hand, the Air Logistics Squadron is located further away from the flying squadrons. The following shows a typical ground layout of an airbase.



**Figure 28 - Typical Layout<sup>26</sup> of an Airbase**

As shown in Figure 28, the CO ALS clusters the building location of close proximity among various flights together for ease of command and control. In addition, it is believed that there will be greater synergy when the flights are located close to one another. The ground distance from ALS to the aircraft parking area of the flying squadron ranges from 5 kilometers (approximately 3.2 miles) to 10 kilometers (approximately 6.4 miles). This distance, although short, posed a substantial amount of time for loading of

<sup>26</sup> The typical layout of an Airbase as explained in this thesis is a hypothetical illustrations and by no means similar or close resemblance to RSAF's Airbase layout.

critical data file on the ALR-69 system onboard the F-16 aircraft. This is mainly due to the low speed limit imposed on all military vehicles that ferry the technicians from ASF to the flying squadron. This is discussed in later section of this chapter.

**E. PRESENT OPERATIONAL CONCEPT (MAINTENANCE CREW'S ASPECTS) FOR LOADING CRITICAL DATA FILE ONTO THE ALR-69 SYSTEM ONBOARD THE F-16 AIRCRAFT**

The flying squadron, as explained in previous section in this chapter, locates close to the airfield for ease of take-off and landing. The aircraft are usually parked close to one another; see Figure 29, for the ease of the ground crew to perform before-flight checks (BF<sup>27</sup>) or after-flight checks (AF<sup>28</sup>) on the aircraft.



**Figure 29 - RSAF's Pilots and Aircraft Technicians Standing in Front of the F-16 Aircraft. Aircraft are Usually Parked Side-By-Side Close to the SQCP<sup>29</sup>**

---

<sup>27</sup> A standard list of checks on aircraft done by ground maintenance crews to assure that the aircraft is good for flight. These checks are usually done two hours before the actual flight.

<sup>28</sup> A standard checklist to be done on aircraft by ground maintenance crews after the aircraft return from a mission/flight. This is to assure that the aircraft is free from defects after the previous flight. Should the ground maintenance crews find defects, the ALS technicians will be notified and the aircraft will be labeled unserviceable for next flight.

<sup>29</sup> Squadron Command Post is the command center of the flying squadron. The commanding officer will be commanding his pilots in the SQCP.

The critical data file on the ALR-69 systems onboard the F-16 aircraft are loaded via the EDNA (refer to Figure 30) by the ASF maintenance crews. As RSAF adopted the task-oriented work practices, well trained and fully qualified maintenance crews from ASF can only perform the loading of critical data file on the ALR-69 systems onboard the F-16 aircraft.

ALR-69 system, by its nature, is classified as electronic warfare systems. The higher command of EW systems is the Higher HQ Command in the MINDEF<sup>30</sup>. The Higher HQ Command controls the version of the critical data file to be loaded on the ALR-69 systems onboard the F-16 aircraft. As briefly described in chapter 2, ALR-69 systems is a RWR system that is able to detect, identify, process and display airborne interceptor (AI), surface-to-air missile (SAM) and anti-aircraft artillery (AAA) weapon systems. Situation awareness provides the crew with threat type, emitter mode and threat angle-of-arrival (AOA) information. As such, the critical data file on the ALR-69 systems is dynamic and can change on every mission or flight that the pilot is assigned or tasked.



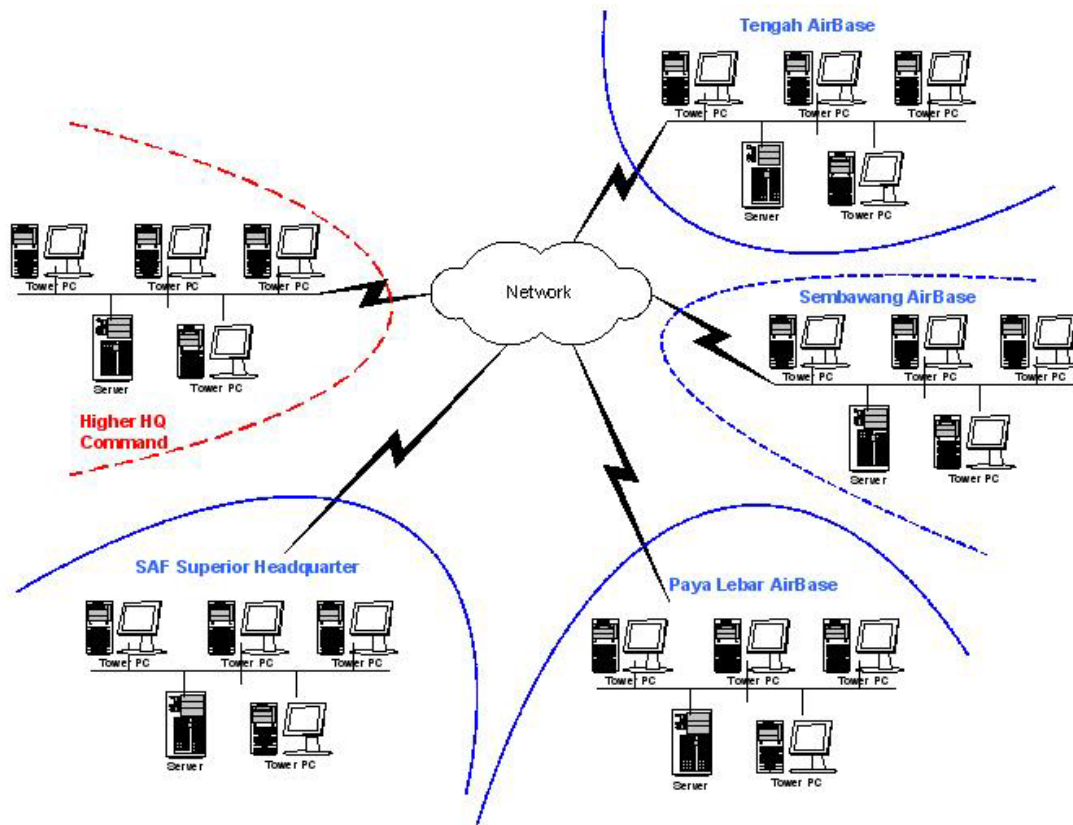
**Figure 30 – Technicians (Non RSAF) Loading Data File to the Aircraft Using EDNA**

---

<sup>30</sup> MINDEF stands for Ministry of Defence.

The Higher HQ Command is not located within the airbase and is located elsewhere on the Singapore Island. Refer to Figure 31 for simplified LAN layout within SAF. The backbone is provided by the fiber optics cables as it is resilient to security breach. The LAN setup is confirmed to SAF and thus it is termed Intranet. The Operating systems within the computers are Windows NT based.

The required critical data file for the ALR-69 systems is transmitted to ASF<sup>31</sup> using secured LAN and normally takes several seconds (this short time is insignificant to the overall uploading time and is assumed to be spontaneous). However, the main challenge is to download the newly received critical data file from ASF to the EDNA and eventually traveled to the aircraft to upload to the ALR-69 systems onboard the F-16 aircraft.



**Figure 31 - Simplified Network Layout of Higher HQ Command and Various Airbases (a.k.a. Intranet)**

<sup>31</sup> Air System Flight (ASF) – The department or flight that is responsible for the maintenance of the ALR-69 systems. ASF is also responsible to upload the required data file onto the ALR-69 systems onboard the aircraft.

## **1. Operational Scenario of Loading Critical Data to EDNA Prior to ALR-69 System Onboard the F-16 Aircraft**

The critical data file for use by the ALR-69 system is to be loaded onto the F-16 aircraft using the EDNA. The following steps are required to accomplish the loading of the critical data onto the ALR-69 system. Figure 32 shows the sequential event flow and timing requirement for uploading the newly received critical data file, using EDNA, onto the ALR-69 system onboard the F-16 aircraft in the flying squadron. The sequential event flow (with timing requirement) is as follows:

- a. Higher HQ Command to program the required critical data file for a particular sortie<sup>32</sup>
- b. Higher HQ Command will forward the critical data file to ASF in the respective Airbases (assume spontaneous with no time delay)
- c. ASF will download the newly received critical data file onto floppy diskette (one at a time) and passed to a RWR Uploading Team<sup>33</sup>, each team equipped with one EDNA (< 5 minutes)
- d. RWR Loading Team is then dispatched, via pickup truck, to the respective flying squadron (< 20 minutes<sup>34</sup>)
- e. The RWR Loading Team will then prepare<sup>35</sup> the aircraft for uploading the critical data file (< 15 minutes)

---

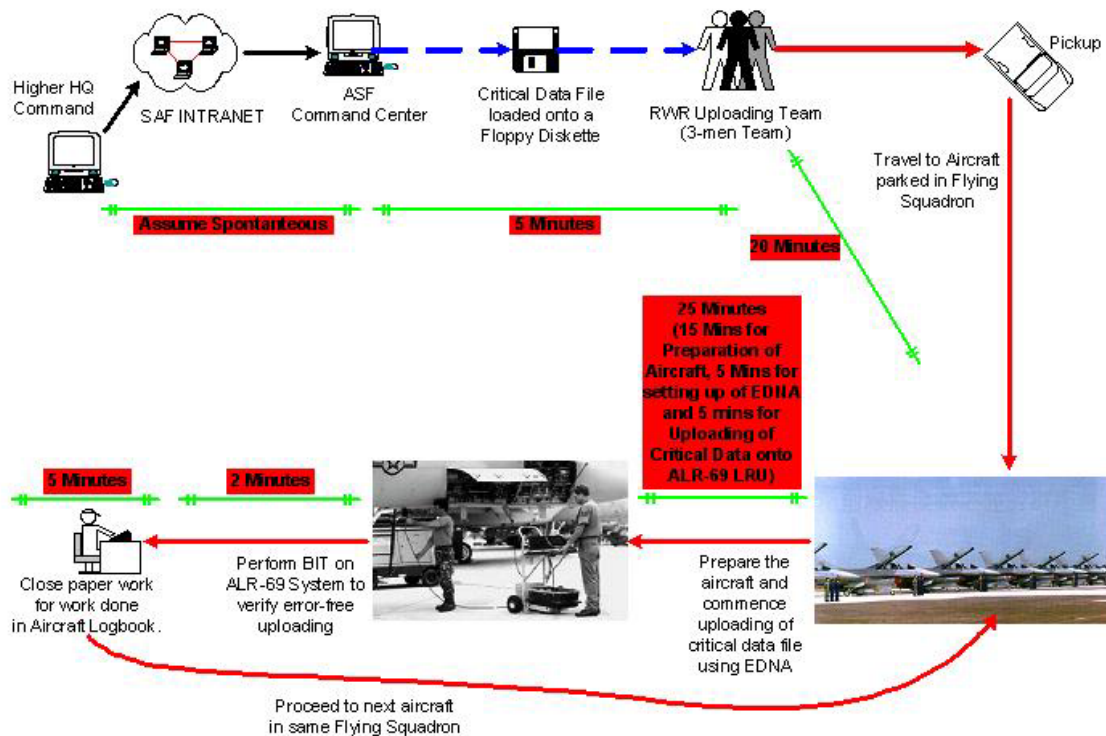
<sup>32</sup> A sortie is defined as one aircraft making one takeoff and one landing; an operational flight by one aircraft. Hence, six sorties may be one flight each by six different aircraft, or six flights by a single aircraft. Threat air capabilities are often stated in terms of the number of sorties per day by a particular type of aircraft. They are based on an evaluation of the available number of aircraft and aircrews (ideally more than one crew per aircraft), and the threat's maintenance, logistics, and training status.

<sup>33</sup> RWR Uploading Team is a group of three ASF technicians responsible to upload the critical data file onto the ALR-69 system onboard the F-16 aircraft. A group consists of an IC, must be qualified F-16 and RWR system senior technician and two junior technicians.

<sup>34</sup> 20 minutes is the average time required to travel from ASF to the aircraft in the flying squadron. This is an average time as some flying squadron is located further away from ASF. This long lead-time is also attributed by the speed limit imposed on the military trucks within the airbase. Generally speed limit for all vehicles within the airbase is no more than 20 kilometers per hour.

<sup>35</sup> Prepare the aircraft is to ensure that the aircraft is safe for working on ground by the technicians. It encompasses the making safe of aircraft armament, powering the aircraft using external power source, opening the relevant aircraft panels for the connection of cables from EDNA to ALR-69 LRU.

- f. Power up the EDNA and invoke to relevant uploading software. Select the newly received critical data file on the floppy diskette for preparation to transfer the critical data file to the ALR-69 LRU (< 5 minutes)
- g. Commencements of uploading of critical data file from the EDNA to the ALR-69 LRU onboard the F-16 aircraft (< 5 minutes)
- h. Perform a BIT<sup>36</sup> test to ensure that the critical file is correctly transferred and error-free (< 2 minutes)
- i. Close up all aircraft panels and complete the required paperwork. The paperwork includes logging the job performed, Rank and Name of technicians responsible for this current job, etc on the respective aircraft logbook (< 5 minutes)

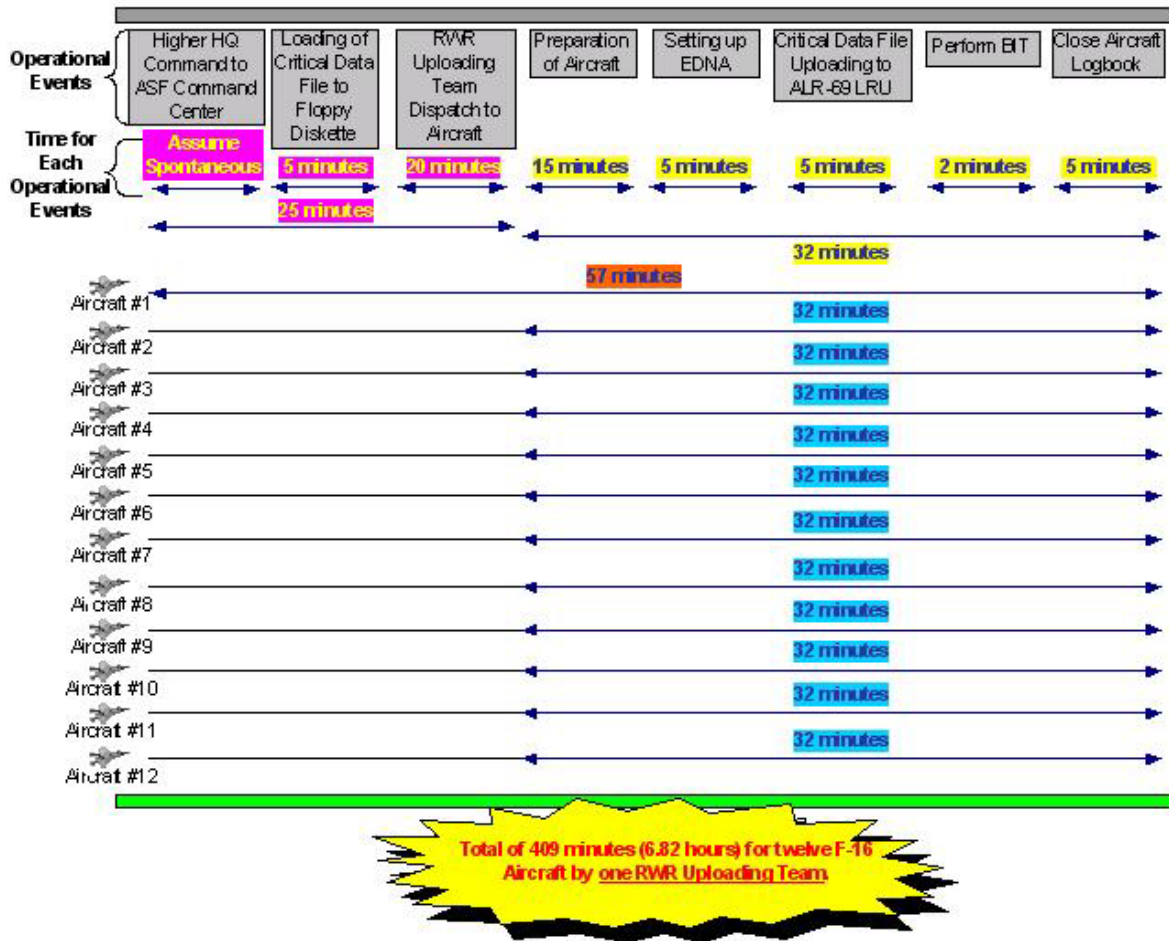


**Figure 32 - Operational Workflow for RWR Uploading Team**

<sup>36</sup> BIT stands for Built-in Test. It is a test within the ALR-69 LRU to perform a self-test and will report if the newly uploaded critical data file has errors.

## 2. Timeline for Present Operational Workflow for RWR Uploading Team

Figure 33 crystallized the timing requirements for present operational workflow for RWR Uploading Team. The RWR Uploading Team, on average, takes around 60 minutes for the first aircraft. Subsequent aircraft would only require 30 minutes<sup>37</sup>. The same RWR Uploading Team will proceed to upload the critical data file onto another aircraft. This team is responsible for all the aircraft<sup>38</sup> for a particular flying squadron since all aircraft of a particular flying squadron are parked within close proximity.



**Figure 33 - Timing Chart for Operational Events for RWR Uploading Team**

<sup>37</sup> The subsequent time of 30 minutes exclude the forwarding of new critical data file from Higher HQ Command, downloading of critical data file to floppy diskette and traveling time to flying squadron. This is a reduction of 30 minutes.

<sup>38</sup> In this thesis, it is assumed that a flying squadron has 12 F-16 aircraft under its inventory. This figure is fictitious and by no means represents the number of aircraft within a flying squadron in RSAF.



From Figure 33, the total time required to complete the uploading of new critical data file for ALR-69 on all twelve aircraft in one flying squadron takes no less than 409 minutes, which is equivalent to 6.82 hours. This time is far too long and is not acceptable by pilots, as they usually demand the time to be shortening to no longer than 2 hours. Anyway, this is only a hypothetical study and in actual ground operation, there are usually more than one RWR Uploading Team being dispatched to support this operational scenario. However, the number of EDNA that the RSAF owns is restricting the number RWR Uploading Team.

EDNA is a ruggedized piece of aircraft ground support equipment and is the only approved ground support equipment to support such operation by the aircraft manufacturer. The cost of one EDNA is close to several hundred thousands dollars. With such high price tag, RSAF is not willing to invest and purchase more EDNA than is required. RSAF only purchased 10 EDNA together with the initial aircraft purchase contract. As EDNA is the only piece of equipment for use on the F-16 aircraft, many other flights are also using EDNA for other purposes. For example, EDNA is used by PrF (Propulsion Flight) to download engine health status and flying hours. EDNA is also used by FCF (Fire Control Flight) to upload and download other critical information as required by the F-16 aircraft. As such, ASF is only allocated three EDNA and thus only three RWR Uploading Teams can be formed to support the uploading of the critical data file on the ALR-69 system onboard the F-16 aircraft.

#### **F. POTENTIAL PROBLEMS IN PRESENT OPERATIONAL WORKFLOW FOR RWR UPLOADING TEAM**

There are several problems that ASF is facing currently. They are as follows:

##### **1. Long Time Required to Complete Uploading of RWR Critical Data File for One Squadron of Aircraft**

One RWR Uploading Team requires a total of 6.82 hours to complete the uploading of new critical data file onto ALR-69 system onboard the F-16 aircraft. This timeframe is considered long by the pilots as it is only recommended to complete such task within two hours.



**2. Limited Number of EDNA Directly Restricting the Number of RWR Loading Team**

Considering increasing more RWR Uploading Team to carry out the uploading of critical data file operation simultaneously. However, the limiting factor is the number of EDNA in RSAF's inventory. ASF is only allocated three EDNA and, as such, only a maximum of three RWR Uploading Teams can be formed. To further dilute the RWR Uploading Teams, there are several flying squadrons within an airbase. Although there can be three RWR Uploading Team, each team is to support one or more flying squadrons. To further aggregate the problem, the locations of these flying squadrons are not close to each other. They may be 5 to 10 kilometers apart.

**3. Insufficient Number of EDNA in RSAF Inventory**

There is a total of ten EDNA in RSAF's inventory. Only three EDNA is allocated to ASF for uploading of critical data file onto the RWR-system. The remaining seven EDNAs are allocated to other flights for other maintenance purposes.

**4. Time Wasted on Floppy Diskette Transfer and Traveling to the Aircraft**

The Higher HQ Command will forward the new critical data file for ALR-69 system to ASF through the Intranet. Subsequently, ASF then download the newly received critical data file onto floppy diskette. After which, the RWR Uploading Team is then dispatched to the flying squadron. The distance from ASF Command Center to flying squadron is no less than 10 kilometers. Coupled with the slow speed limit imposed on military vehicle, the traveling time from ASF Command Center to flying squadrons takes around 20 minutes (on average). This amount of time can be reduced or eliminated to reduce the over time required for uploading the critical data file onto the ALR-69 system.

**5. Increased Risk of Military Vehicle Accident**

The 20 minutes time required to travel from ASF Command Center to flying squadron also increases the risk of vehicle accident. The reason being that the RWR Uploading Team is in a rush to complete the uploading task as soon as possible. Quoting Murphy's Law - 'things that can go wrong will go wrong'. As such the risk of vehicle accident happening in this scenario is increased. In fact, there are several occasions

where vehicle accidents had happened when the RWR Uploading Team rushes to complete the uploading task.

## **6. Human Fatigue is Crucial**

RWR Uploading Team is composed of flesh and blood human beings. As such, fatigue will occur as the RWR Uploading Team proceeds to upload critical data for more than 1 hour. Similarly, there are several occasions where human fatigue caused some work-related accidents.

## **7. Security Considerations**

As mentioned in S/No (4) above, the Higher HQ Command will forward the new critical data file for ALR-69 system to ASF through the Intranet. Subsequently, ASF then download the newly received critical data file onto floppy diskette. Due to security precautionary measures imposed by MSD<sup>39</sup>, the Higher HQ Command can only forward to a single OA account in ASF Command Center. Even though there are three RWR Uploading Teams, ready for dispatch to the flying squadron, there is a lead-time to download the newly received critical data file onto floppy. The downloading to each floppy diskette takes around 5 minutes and this downloading to floppy diskette can only be performed one at a time. As such, only one RWR Uploading Team is dispatched at any one time, after the team has received the floppy diskette loaded with the new critical data file. Time is wasted in this aspect.

## **8. Insufficient Military Vehicles**

Each RWR Uploading Team is dispatched via military vehicle from ASF Command Center to flying squadron. ASF owns 2 military vehicles and thus ferrying the RWR Uploading Team to the respective flying squadron is delayed by the problem of insufficient military vehicles. Ideally, each RWR Uploading Team should be mobile and should be assigned with one military vehicle. As there are only two military vehicles but three RWR Uploading Teams, two of teams are required to share military vehicle. To further worsen the insufficient vehicle problem, on many occasions, technicians who are

---

<sup>39</sup> MSD stands for Military Security Department. MSD is responsible for all security aspects in the MINDEF.

servicing the snags on aircraft already use the military vehicles<sup>40</sup>. As such, time is also wasted to recall the military vehicles to ferry the RWR Uploading Team to the flying squadron.

From the above, it is evident that insufficient EDNA equipment and military vehicles cause these problems. As such, the subsequent two chapters of this thesis shall study the possibility of implementing 802.1x protocols to reduce the overall time required to upload the critical data file onto the ALR-69 system onboard the F-16 aircraft.

---

<sup>40</sup> Military vehicle is used to ferry technicians to flying squadron for various purposes, such as Uploading of critical data file, servicing aircraft snags, etc. As such, utilization rate for military vehicle is usually high through out the day.

THIS PAGE INTENTIONALLY LEFT BLANK

## **VI. FEASIBILITY STUDY ON UPGRADING OF PRESENT SYSTEM TO INCLUDE WIRELESS TRANSMISSION CAPABILITY**

This chapter conducts a feasibility study on upgrading of the present system to incorporate wireless transmission capability. The initial section will study the advantages and disadvantages of the two available wireless technologies, IEEE 802.11 and FSO as discussed in Chapter III and IV respectively. Eventually one of these two technologies will be selected for use in the upgrading of the present system of assisting to get critical data file from command center to EDNA prior to loading to the ALR-69 LRU onboard the F-16 aircraft. This chapter shall also address the user's requirements and how these requirements are fulfilled. The choice of new equipment will also be recommended and proposed.

### **A. SPECIFIC REQUIREMENTS**

Currently, RSAF's acquisition policy is to use commercial off the shelf (COTS) technology to meet the system requirements (system requirements include user's requirements and hardware requirements). There are several advantages to not using Military Specification (MIL-SPEC) components. First, the system cost will be significantly less by avoiding the MIL-SPEC process. Second, the time to develop, build, and maintain the system is greatly reduced by using immediately available parts. Lastly, the system is easier and cheaper to update as new technology provides better solutions.

#### **1. User's Requirements**

Since the formal MIL-SPEC process is not being used to define the requirements, special attention must be paid when identifying the user's unique military requirements. The military requirements are used to identify the special capabilities needed by the system to perform its military mission. They are as follows:

**a. *Weather Resistant***

The system must be able to operate in extreme conditions including dust, sand and rain.

**b. *Security***

The system must be able to provide confidentiality and authenticity while transmitting secret documents. The security considerations were established based on the existing Intranet security guidelines and requirements for wireless LANs. The security for Internet connectivity is to be managed by the Intranet network security administrator.

**c. *Wireless Capability Upgrade to the EDNA Must be Stable***

The uploading of critical data file onto the EDNA is mission critical and must be resistant to system crashes and lockups to the greatest extent possible.

**d. *Minimize Disruptions to Existing Wired LAN Infrastructure (Intranet)***

The constraints of the project required the wireless design plan to make do with the existing wired laboratory infrastructure, space and electrical fittings as much as possible, and minimize disruptions to the current wired LAN configurations.

**e. *Connection to Existing Wired LAN Infrastructure (Intranet)***

Interconnection with stations on a wired backbone LAN (Intranet) is required. For infrastructure mode wireless LANs, this is usually accomplished through the use of control modules that connect to both the wired and wireless LANs research.

**f. *Above 99% Availability of the New Wireless System***

Availability is a critical requirement for this system. According to RSAF's acquisition policy, the availability of the system should not fall below 99%.

**g. *Wireless System Endurance***

The system must operate for a period of at least 8 hours without requiring powering down, which will permit most missions to be completed without interruption.

***h. Ease of Installation***

The new system proposed should be relatively ease to install.

***i. HERO Safe***

The radiated power output at the downrange site must be less than 1 Watt at 10 feet or 5 Watts at 25 feet so that system will not cause electrically initiated explosives to detonate.

***j. Effective Range No Less Than 200 Meters in Diameter***

The effective range of the wireless link must be a minimum of 200 meters, to allow the transferring of critical data from the SQCP to the aircraft that is parked furthest away.

***k. Affordability***

What the user can afford to purchase. Affordability for this system should be measured by the value of its capabilities. The question is how much is it worth for what it can do? A reasonable figure would be \$45,000 to \$50,000 for initial procurement of a complete system and no more than \$10,000 for follow-on annual maintenance.

**2. Hardware Specifications**

The hardware specifications are used to identify the special capabilities needed by the system. They are as follows:

***a. Number of Access Points***

The access point links the wireless users to the wired network of the Intranet. Given the coverage of an access point using 802.11b standard, two access points (with radius of 200 meters) should be adequate to cover the distant from SQCP to the furthest aircraft. The two access points could also act as redundancy for one another whenever one is down.

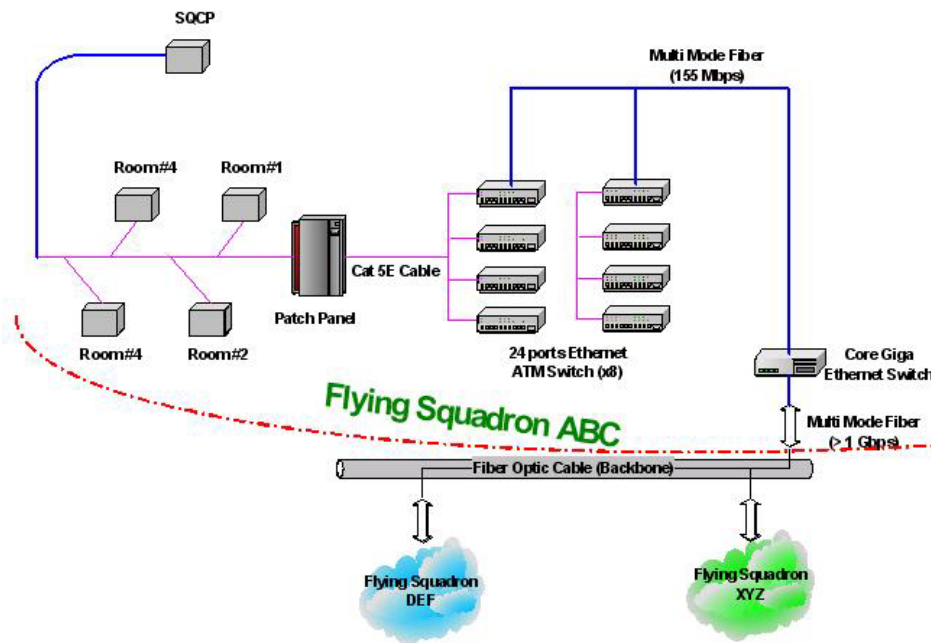
***b. Network Equipment***

The existing wired LAN network in the SQCP is already equipped with one 16-port Ethernet hub and one 16-port Ethernet switch. There are adequate ports left for the proposed two access points. Some Ethernet cables would be needed to connect the

access points to the wired LAN and the EDNA would also require a client adapter. It is preferable and recommended that the manufacturer of the client adapter be the same vendor as the access points for greater confidence of hardware compatibility.

**c. Intranet Backbone**

The Intranet is made up of a large number of small LAN's spread over all the airbases in the Singapore Island. Thus, the Intranet uses fiber optic-cables as a transmission medium (backbone) that allows a higher bandwidth and lower delay to interconnect its main buildings to each other (intranet) within a single airbase and to facilitate their communications with the network from other airbases. In addition, individual airbase is connected via Gigabit Ethernet network technology. The fiber optic-cable is directly linked to core Gigabit Ethernet switches that are usually located at the computer center in each airbase. The data transmission speed of this switch is rated at 1 Gbps, which utilizes the single mode fiber optics.



**Figure 34 - Network Diagram For Wired LAN Within an Airbase**

Figure 34 shows Intranet’s backbone and wired LAN configurations. The Intranet backbone requirements for the wireless LAN in each SQCP is straightforward, as no additional hubs or switches would be purchased for the wireless interfacing. Each



SQCP will be allocated one access point. This access point will be connected to the existing Ethernet hub and switch, which belong to the wired LAN in the SQCP. The only requirement is to register the port numbers of the hub and switch intended for wireless connections with the airbase network administrator so that the SQCP wireless LAN could be legally established in the airbase.

## **B. RATIONALE FOR SELECTION OF EITHER IEEE 802.11 OR FSO WIRELESS TECHNOLOGY**

As explained in Chapters III and IV, there are two technologies that are suitable for used in this upgrade study. This section shall explore the advantages and disadvantages and select the best method for use for the upgrade.

### **1. Comparison of Suitability of IEEE 802.11 Wireless Technology Against FSO for the Upgrade in This Thesis Work**

The option of using IEEE 802.11 wireless is using the concept that is similar to the cellular phone system. Access points will be co-located with the base stations to provide a complete coverage from SQCP to the furthest aircraft parked in the flight line. As explained in chapter III, the IEEE 802.11 has range of not more than 350 meters, which is sufficient to fulfill the maximum coverage requirement. For extended distance up to more than 350 meters, the Yagi antenna is used in conjunction with the access point.

Free-Space Optics (FSO) operates in an unlicensed frequency, and is a comparatively cheap, easy to deploy, and high capacity broadband solution, enterprises around the globe have been using it as a means of connecting dispersed office LANs, and for redundant fiber backup. But the deployment of FSO in carrier networks must be carefully assessed, as the technology has some inherent limitations: FSO is a line-of-sight (LOS) technology. The reliability of an FSO link is affected by fog, scintillation, and buildings sway. Links must be constructed at distances ranging from 820.25 feet (250 meters) to 6,562 feet (2 kilometers) in order to decrease susceptibility to interference.

Table 3 shows the scoring table for choosing one of the two available wireless technologies. The scoring criterion is a common method used in RSAF acquisition policy. The scoring is from minimum of 1 to maximum of 5.

	<b>IEEE 802.11</b>	<b>FSO</b>
<b>Weather Resistant</b>	<b>3</b>	<b>4</b>
<b>Contaminated Environments</b>	<b>5</b>	<b>5</b>
<b>Secure</b>	<b>4</b>	<b>5</b>
<b>Compatible with Existing System</b>	<b>5</b>	<b>4</b>
<b>Stable</b>	<b>5</b>	<b>5</b>
<b>Availability of the New System</b>	<b>5</b>	<b>5</b>
<b>Endurance</b>	<b>5</b>	<b>5</b>
<b>Ease of Installation</b>	<b>5</b>	<b>2</b>
<b>HERO Safe</b>	<b>5</b>	<b>1</b>
<b>Effective Range (min 400 feet)</b>	<b>5</b>	<b>5</b>
<b>Affordability</b>	<b>5</b>	<b>3</b>
<b>Total Scoring</b>	<b>52</b>	<b>44</b>

**Table 3 - Selection Criteria Scoring Table**

From Table 4, it is evident that IEEE 802.11 outscored the FSO technology. As such, the IEEE 802.11 technology is selected based on its ability to fulfill the user's requirement.

## **2. Which IEEE 802.1x Standard to Use**

Since IEEE 802.11 is selected for the upgrade, the next question is which of the three available standards is to be adopted. The three standards are IEEE 802.11b, IEEE 802.11a and IEEE 802.11g. Each of the three available IEEE 802.11 standards has their advantages and disadvantages.

The maturity of wireless LAN technology based on the 802.11b standard, introduced in late 1999, has spawned a variety of reasonably priced wireless products. What's more, new 802.11a products are gaining momentum, as is the promise of a third standard, 802.11g.

Wireless devices adhering to the 802.11b standard actually work and, for most part, are interoperable, meaning that one manufacturer's AP will work with another's wireless PC card. Prices have fallen as well. Two years ago an AP cost about \$1,000; today we can buy one for as low as \$100 (Ref. [www.ebay.com](http://www.ebay.com)). The agency that tests for interoperability is an industry consortium known as the Wi-Fi Alliance (formerly known as Wireless Ethernet Compatibility Alliance - WECA). Those 802.11b products that pass the WECA's tests are given the Wi-Fi (wireless fidelity) seal of approval. The IEEE 802.11b specification makes use of 2.4GHz band and has throughput of 11 Mbps.

Today, the most common work performed across the wireless LANs entails office applications, such as e-mail, spreadsheet building and word processing. Both 802.11b and 802.11a are adequate to handle such traffic. However, as streaming video and dynamic content become more common, the throughput of 802.11b products will not be enough. This is where 802.11a comes in, a new specification that represents the next generation of enterprise-class wireless LANs. Because it operates in the 5 GHz spectrums, it offers more bandwidth and thus more channels than 802.11b. However, the critical data file is merely less than 500 kilobytes in file size, the advantage of bandwidth could thus, be traded for range instead.

As shown in Figure 35, 802.11b provides range coverage of up to 600 feet while 802.11a only provides up to 100 feet even without using another access point to extend the range further.

While 802.11a and 802.11b use the same MAC layer technology, i.e. CSMA/CA, there are significant differences at the physical layer. 802.11b, using the ISM band, transmits in the 2.4 GHz range, while 802.11a, using the Unlicensed National Information Infrastructure (UNII) band, transmits in the 5 GHz range. Because their signals travel in different frequency bands, one significant benefit is that they will not interfere with each other. A related consequence, therefore, is that the two technologies are not compatible.

	<b>IEEE 802.11b</b>	<b>IEEE802.11a</b>
Time Table	Standard in 1997. Products in 2000	Standard in 2001, Products in 2002.
Frequency Band and Bandwidth	Transmit at 2.4 GHz – IEEE 802.11g standard increases speed of 802.11b to 22 Mbps in the same 2.4 GHz band	5 GHz
Speed	11 Mbps (Effective speed-half of rated speed)	54 Mbps (Effective speed-50% rated speed)
Modulation Technique	Spread Spectrum	OFDM (Orthogonal Frequency Division Multiplexing)
Distance Coverage	Up to 600 feet	100 feet – speed goes down with increased distance
Number of access points required	Every 200 feet in each direction	Every 50 feet
Maturity	More matured products	Less matured but progressing fast
Market Penetration	Quite widespread	Just starting in 2002
Interference with other devices	Band is more polluted – significant interference here	Less polluted because of fewer devices in this band
Interoperability	Not as problematic as 802.11a	Problems now but expect resolution soon
Cost	Cheaper: \$300 for access point and \$75 for adapter	More expensive (\$500 in 01/2002 – will come down)
Vendors	Major vendors in both camps	
No. of channels	3 non-overlapping channels	9 non-overlapping channels

**Figure 35 - Comparison of Wireless LAN Standards – IEEE 802.11a Versus IEEE 802.11b (PC Magazine, May 21 2002)**

Thus, 802.11a has some compatibility issues to work out as 802.11b products clearly dominate the market. Also, although all 802.11a products use the same chip set, their implementation by each manufacturer differs enough to make them incompatible. Until interoperability standard is established, 802.11a products from one company may not talk with those of another.

As wireless technology is still every changing, there is tremendous potential for technology to change and grow. As such, the emphases for the wireless LAN design for this thesis stressed on simplicity and scalability. For example, nearly all Wi-Fi networks worldwide use 802.11b standard. But it is not considered to be as secure or as fast as 802.11a, which is an approved standard that broadcasts a more powerful signal, running

on 12 channels in 5 GHz spectrum, and transfers data up to five times faster than 802.11b. While it is faster, it has not been backward compatible to 802.11b, which is a problem. Another Wi-Fi standard known as 802.11g, which is more secure than 802.11b and has the speed of 802.11a. However, the appropriate standards bodies have not approved it. More changes in the wireless standards arena are expected in near future.

In summary, the choice of the wireless hardware and design for the upgrade should take into consideration these changes so as to avoid wastages. The criteria for vendor selection should contain these factors: a large market share, good recommendations from newsgroups, trade journals, and Subject Matter Experts (SME), used by the military and universities, and must support 802.11a and b. As discussed above, the IEEE 802.11b is able to fulfill the range requirement as the minimum effective range should be no less than 200 meters as stated in the user's requirement. In addition, IEEE 802.11b is a proven technology and it is also relatively cheaper compared to IEEE 802.11a.

So it is concluded that *IEEE 802.11b* is deemed more suitable and favorable and thus it is selected for the upgrade for the purpose of this thesis work.

### **C. SELECTION OF EQUIPMENT FOR IEEE 802.11B WIRELESS TECHNOLOGY**

Two equipments needed for the upgrades are the wireless access point for the infrastructure and the wireless client adapter for the EDNA.

#### **1. Access Points for the Infrastructure**

Several renowned manufacturers of access points were identified and the strength and shortcomings of every model are being considered. Some of the renowned manufactures include Cisco Systems<sup>41</sup>, DLink<sup>42</sup>, Netgear<sup>43</sup> and Linksys<sup>44</sup>.

---

<sup>41</sup> CISCO Systems web page – [www.cisco.com](http://www.cisco.com)

<sup>42</sup> Dlink web page – [www.dlink.com](http://www.dlink.com)

<sup>43</sup> Netgear web page – [www.netgear.com](http://www.netgear.com)

<sup>44</sup> Linksys web page – [www.linksys.com](http://www.linksys.com)

Cisco's Aironet® 1200 wireless access point<sup>45</sup>, as shown in Figure 36, is chosen for the upgrade proposal as it offers good range coverage that suits user's requirement. The other main consideration is that the overall power transmitted by Cisco Aironet® 1200 wireless AP is within the limit imposed by the HERO requirement as stated in the user's requirement.

The Cisco Aironet® 1200 wireless access point is a thin, rectangular metal box that can be mounted on walls or ceilings, or hidden behind ceiling panels. It includes either an embedded 802.11b radio that can transmit and receive data at 11 Mbps, or a radio module that can be plugged into the unit for connecting to devices supporting the IEEE's new 802.11a standard, which can transmit and receive data at 54 Mbps, supports more channels and suffers less interference than the IEEE 802.11b standard. Laptops and PDAs, however, will need compatible 802.11a wireless access cards before they can take advantage of the higher speeds and other benefits of the latest Cisco 802.11a access points.



**Figure 36 - Cisco Aironet® 1200 Series Access Point**

This provides an option to build a wireless LAN (WLAN) that can be migrated from 11-Mbps to 54-Mbps at either 2.4 GHz or 5.2 GHz.

Cisco Aironet® 1200 Series access points deliver the security, manageability, upgradeability and reliability to create high-performance, enterprise-class wireless LANs.

---

<sup>45</sup> Refer to Appendix A of this thesis for more information of CISCO Aironet 1200 series access point.

With simultaneous support for both 2.4 GHz and 5 GHz radios, the Cisco Aironet® 1200 Series preserves existing IEEE 802.11b investments and provides a migration path to future IEEE 802.11a and IEEE 802.11g technologies. Its modular design supports single- and dual-band configuration, plus the field upgradeability to change these configurations as requirements change and technologies evolve. Investment protection is further provided by large storage capacity and support for Cisco management tools, delivering the capacity and means to upgrade firmware and deliver new features as they become available.

The cast-aluminum-cased device provides the ruggedness required in factories and warehouse installations, while still meeting the aesthetic requirements of a corporate lobby. The Cisco Aironet® 1200 Series supports both inline power over Ethernet and local power, features an integrated mounting system for wall and ceiling mounting, leverages Cisco's broad line of antennas, and delivers an extended operating temperature range. All this and more makes the Cisco Aironet® 1200 Series the most flexible access points available, ideal for deployment in a wide range of industries, facilities, and orientations.

## **2. Network Interface Card (NIC) for the EDNA**

The EDNA has provision for PCMCIA 2.0 expansion slot to accommodate the Network Interface Card (NIC) required for wireless communication. There are many manufacturer of NIC in the market that suits the needs of the user's requirement. The NIC selected is Cisco Aironet® 350 Series Client Adapters and the specification can be found in Appendix B in this thesis.

The effective maximum range for this NIC is 800 ft (244 meters) @ 11 Mbps or 2000 ft (610 meters) @ 1 Mbps [16]. This range exceeds the user's requirement of only 200 meters. The following are some features of the Cisco Aironet® 350 Series Client Adapters [16]:

- Plugs directly into laptop type-II PCMCIA slot
- Broadest operating system support
- Wi-Fi (IEEE 802.11b) certified interoperability

- Low power consumption
- High performance 11 Mbit/s data rate.
- Superior range of up to 1,750 ft/550 m and throughput
- Secure network communications
- World mode for international roaming
- Support for all popular operating systems



**Figure 37 - Cisco Aironet® 350 Series Client Adapter**

**D. EMI/EMC OR ANY POSSIBLE INTERFERENCE WITH AIRCRAFT OR ARMAMENT SYSTEMS**

The IEEE 802.11b wireless standard operates in the 2.4 GHz ISM band and utilizes Direct Sequence Spread Spectrum (DSSS). According to the inventory of systems onboard the F-16 aircraft, there are no systems currently utilizes this frequency band. In addition, the loading of the critical data file from the EDNA to the ALR-69 LRU onboard the F-16 aircraft is usually done on ground using only in-house or external power supply unit (without actual aircraft power). The strict requirement to declare an aircraft to be “on ground” would means all amunitions loaded on the aircraft must be put in safe-mode via physical safety pins and proper grounding. Moreoever, all other avionics or radar related equipment onboard the F-16 aircraft are not powered on at the ALR-69 critical data



uploading stage. As such, it is deemed safe for operation of the IEEE 802.11b wireless transfer from the SQCP to the EDNA in the flight line environment.

The maximum transmit power output by the wireless access points is only 100milli-watts and is well below the limit of less than 1 Watt at 10 feet or 5 Watts at 25 feet in the user's HERO requirement.

However, it is recommended to perform a full EMI/EMC test conforming to the Mil-Std 461/462<sup>46</sup> to ensure no EMI/EMC concern but this is beyond the scope of this thesis work.

#### **E. RECOMMENDATION FOR THE SETUP OF IEEE 802.11B WIRELESS CAPABILITY IN THE SQCP**

So far, we have identified the Cisco Aironet 1200 Series wireless access point for the SQCP and Cisco Aironet® 350 Series Client Adapters for the EDNA. This section will discuss the recommendation for the setting up of these equipments. In addition, a network diagram will crystallised the integration of the access point to the existing Intranet.

##### **1. Recommendation of Mounting Point for Cisco Aironet® 1200 Series Wireless Access Point**

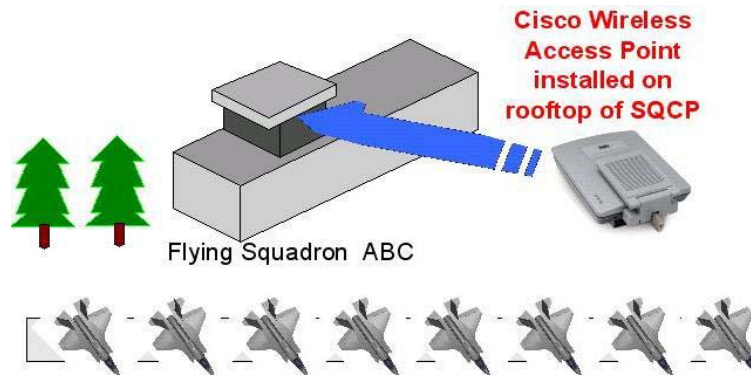
The access point (AP) provides connectivity to the existing Intranet backbone. All roaming stations, EDNA with NIC in our scenario, communicate through the AP. The AP, thus provide connectivity to the Intranet backbone (wired LAN). The make and model selected for this thesis work is the Cisco Aironet® 1200 Series wireless access point. In our scenario, the wireless connectivity required is for outdoor environment. It is recommended that the Cisco Aironet® 1200 Series wireless access point be mounted at the edge of the SQCP. The AP is then connected to the Intranet backbone via standard CAT 5E cables.

Singapore is located in the earth's equator and rainfall is heavy throughout the year. On average, there are rainfalls every other day with occasion thunderstorm.

---

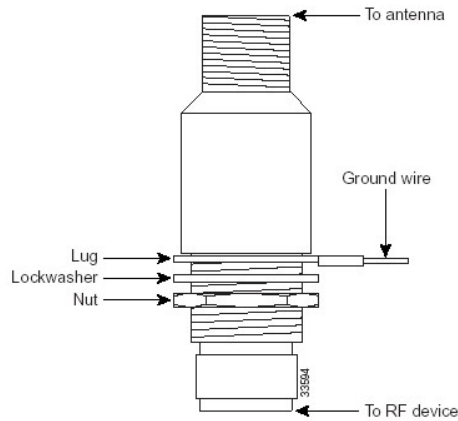
<sup>46</sup> MIL-STD-461 / 462 states the requirements for the Control of Electromagnetic Interference Emissions and Susceptibility test.

According to peacetime training doctrine, RSAF normally do not operate during thunderstorm or adverse weather. Nevertheless, the wireless upgrade equipment selected and the location for mounting the AP is suitable to operate in such adverse weather. It is recommended to enclose the AP and be mounted on the rooftop of the SQCP facing the aircraft parking area. In this way, the AP is protected from heavy rain.



**Figure 38 - Recommended Location for Installing the Access Point in SQCP**

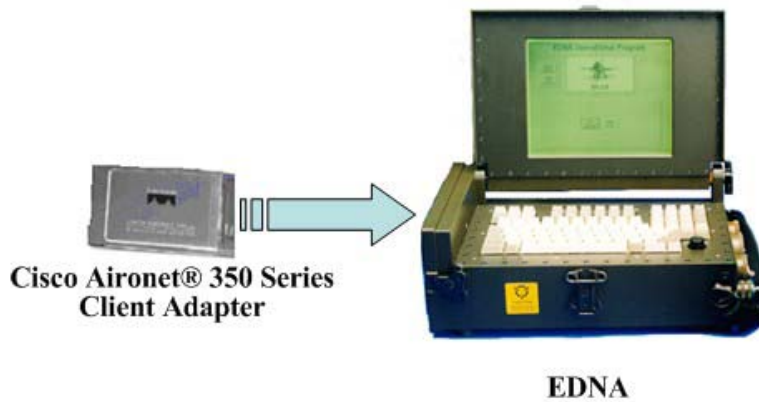
In addition, to combat the thunderstorm condition, it is recommended to install lightning arrestors in the building, especially close to the location of the AP. These lightning arrestors are effective against lightning surge that will destroy the WLAN equipment in the SQCP. The make and model for the lightning arrestor is Cisco Aironet® lightning arrestors. Since over voltage transients can be created through lightning static discharges, switch processes, direct contact with power lines, or through earth currents. Cisco Aironet® lightning arrestors limit the amplitude and duration of disturbing interference voltages and improve the over voltage resistance of in-line equipment, systems, and components. A lightning arrestor installed according to these mounting instructions balances the voltage potential, thus preventing inductive interference to parallel signal lines within the protected system. This arrestor is to be installed between the antenna cable that is attached to an outdoor antenna and the Cisco Aironet® wireless radio device. There is a requirement to ground the arrestor by using a ground lug attached to the arrestor and a heavy wire and connect the lug to a good earth ground. Figure 39 shows a Cisco Aironet® lightning arrestor and the part number for the lightning arrestor is AIR-ACC3354. The kit contains a lightning arrestor, an EMP grounding ring, and this instruction sheet.



**Figure 39 - Cisco Aironet® Lightning Arrestor<sup>47</sup>**

**2. Installation of Cisco Aironet® 350 Series Client Adapter to the EDNA**

The EDNA has provision for PCMCIA 2.0 expansion slot to accommodate the Cisco Aironet® 350 Series Client Adapter. The installation of the client adapter into the PCMCIA 2.0 expansion slot is simple as shown in Figure 40. The installation of the client adapter is complete after the successful installation of the required drivers for the Windows Operating System use by the EDNA.



**Figure 40 – Cisco Aironet® 350 Series Client Adapter Installed in the PCMCIA Expansion Slot of the EDNA**

<sup>47</sup> Cisco Aironet® Lightning Arrestor installation information obtained from [http://www.cisco.com/univercd/cc/td/doc/product/wireless/aironet/miscell/ltnng\\_arr.htm](http://www.cisco.com/univercd/cc/td/doc/product/wireless/aironet/miscell/ltnng_arr.htm), accessed on November 6 2003.

### 3. Network Diagram of the Newly Installed Wireless Access Point Integrated to the Intranet

The complete wireless and wired LAN set-up in the SQCP is given in Figure 41. The Cisco Aironet® 1200 Series AP is planned for the wireless LAN design and should be adequate to provide continuous LOS transmission to the F-16 aircraft parked furthest away from the squadron. The Cisco Aironet® 1200 Series protects current and future network infrastructure investments. The Aironet® 1200 AP is able to do this through its compliance with both the IEEE 802.11a and 802.11b standards, and allows for both single- and dual-band configuration.

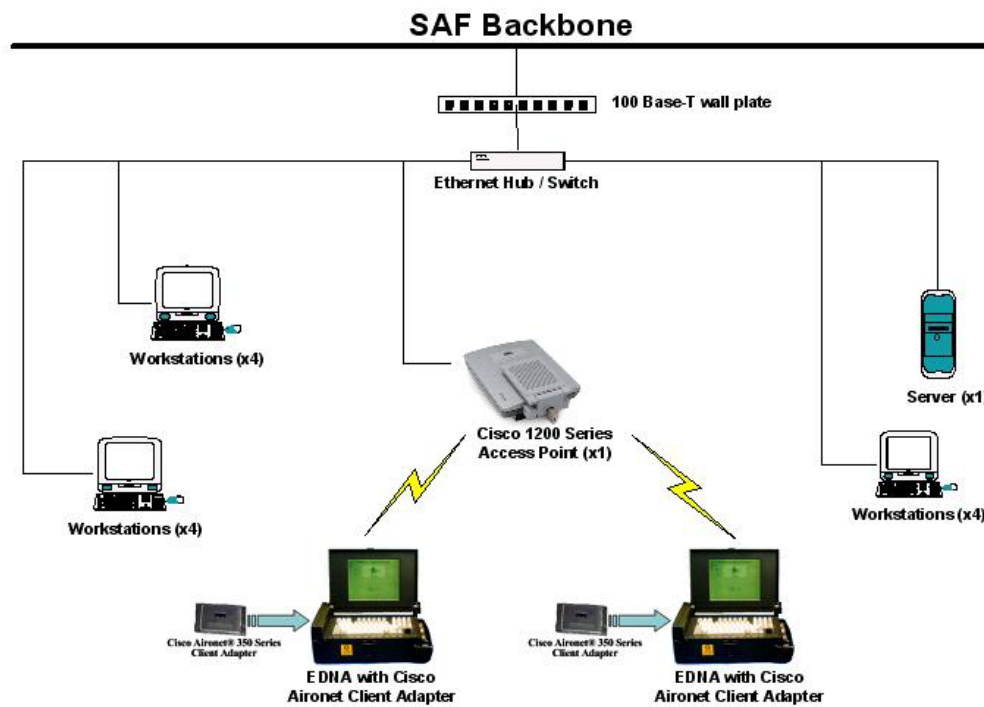


Figure 41 - Network Diagram of Newly Installed Wireless Access Point Integrated to the Intranet

## VII. BENEFITS AFTER IMPLEMENTATION OF IEEE 802.11B

This chapter shall discuss the new workflow for the RWR Uploading Team after incorporating the IEEE 802.11b wireless transmission technology in the SCQP. Comparison between new and old workflow is being discussed and will highlight the areas that contribute to the elimination of some tasks in the workflow after the incorporation of the IEEE 802.11b wireless transmission technology. In addition, a new timing chart will crystallise and demonstrate significant saving in time from 408 minutes to 164 minutes to load the new critical data file onboard the ALR-69 LRU for the same number of F-16 aircraft by just one RWR Uploading Team. Lastly, the total cost for the IEEE 802.11b upgrade will be calculated and tabled.

### A. NEW OPERATIONAL CONCEPT AFTER INCORPORATING IEEE 802.11B WIRELESS TRANSMISSION CAPABILITY

Before proceeding to discuss the new operational concept, it is important to review the present operating concept as shown in Figure 42.

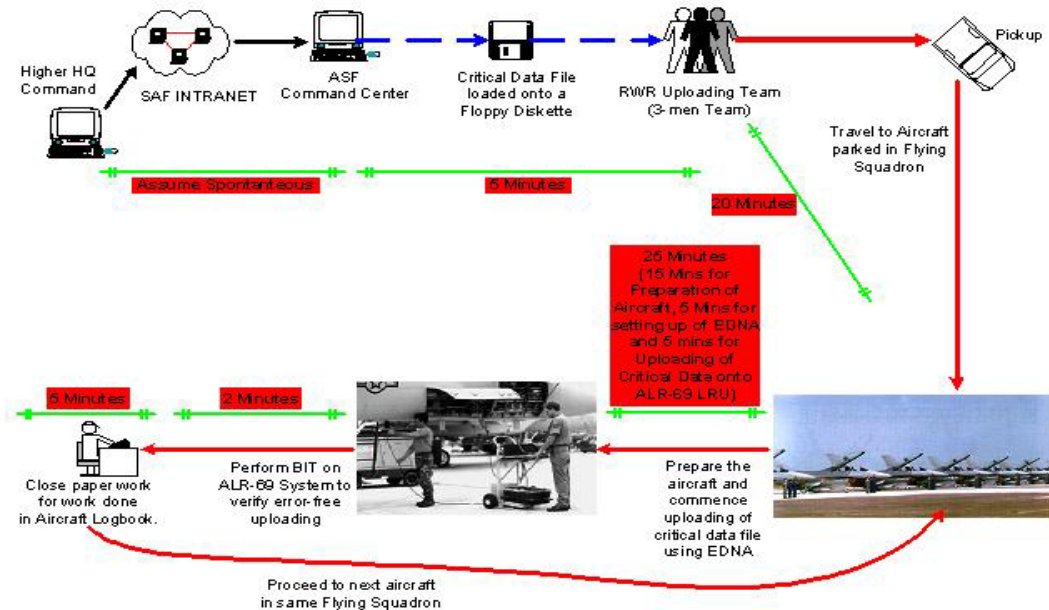
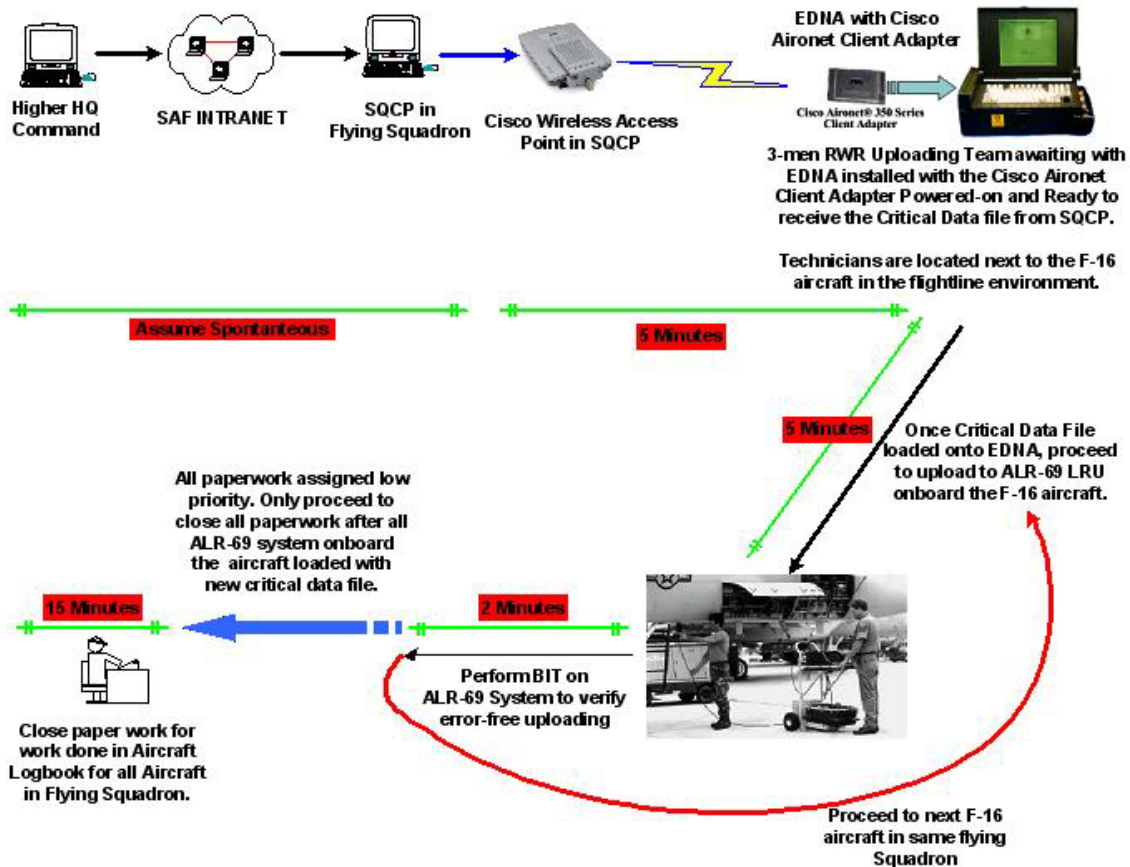


Figure 42 - Present Operational Workflow<sup>48</sup> for RWR Uploading Team

<sup>48</sup> Similar figure used in Chapter V, Figure 32 in this thesis.

After the installation of the IEEE 802.11b wireless transmission capability, the new workflow for the uploading of critical data file is shown in Figure 43.



**Figure 43 - New Operational Workflow for RWR Uploading Team After Incorporating the IEEE 802.11b Wireless Technology Upgrade**

Making comparison between the new and old workflow, it is evident in Figure 42 and Figure 43 that some tasks are eliminated. They are as follows:

**1. Sending of New Critical Data File to SQCP Directly**

The Higher HQ Command will forward the new critical data file to the SQCP instead to the ASF Command Center. This allows decentralizing of the distribution of the critical data file onto the EDNA. Previously, the critical data file is only forwarded to ASF Command Center and the RWR Uploading Team is situated in the ASF to receive the new critical data file. Upon receiving the new critical data file, the RWR Uploading Team then travels to the SQCP to commence the uploading of the critical data file onto the ALR-69 onboard the F-16 aircraft.

**2. Transfer of Critical Data File to EDNA Using Wireless Transmission Media Instead of Floppy Diskette**

The present method of transferring the new critical data file to EDNA is via floppy diskette. After the incorporation of the wireless transmission capability, the new critical data will be sent directly to SQCP. The SQCP will then transmit the new critical data file via wireless medium to the EDNA that is equipped with wireless network adapter. As such, the slow floppy diskette method is thus made obsolete in the new operational concept.

**3. RWR Uploading Team is Pre-Dispatched to Aircraft**

In the present operating concept, the RWR Uploading Team is located in ASF to receive the new critical data file. On the contrary, the new operating concept allows the RWR Uploading Team to pre-dispatch to the flying squadron next to the F-16 aircraft. By doing so, the traveling time factor can be eliminated from the total timing of uploading the critical data file by the RWR Uploading Team. In addition, the risk of vehicle accident can be reduced, as the rush and stress to deploy to the aircraft after the receipt of the new critical data file is made redundant.

**4. F-16 Aircraft Can Be Pre-Prepared to Save Time**

The RWR Uploading Team is pre-dispatched to the F-16 aircraft prior to the receipt of the new critical data file. This will allow ample time to prepare the aircraft for the uploading of the critical data file onto the ALR-69 LRU onboard the aircraft. This is possible as the Higher HQ Command will usually pre-notify the flying squadron which aircraft is required in the next sortie and for whatever mission. This information is usually released hours prior to the release of the new critical data file. As such, it is helpful to capitalize on this information flow by preparing the aircraft for uploading the critical data file even before Higher HQ Command releases the critical data file. By doing so, the time factor to prepare the aircraft for uploading can be eliminated from the total timing of uploading the critical data file by the RWR Uploading Team.

## 5. Signed-off the Aircraft Logbook for All Aircraft

In the present operational flow, after successful uploading of the critical data file on the aircraft, the RWR Uploading Team is required to close the aircraft logbook before proceeding to start the next aircraft. It is proposed that the closure of the aircraft logbook be deferred until the completion of the last aircraft. Upon completing the last aircraft in the flying squadron, the RWR Uploading team will then proceed to close all aircraft logbooks. By doing so, there is a significant reduction in the timing from 5 minutes for each of the 12 aircraft (i.e. 5 minutes x 12 = 60 minutes) to mere 15 minutes.

## B. SIGNIFICANT TIME SAVING

Before discussing the reduction in timing attributed to the new operational workflow after incorporating the IEEE 802.11b wireless transmission upgrade, it is necessary to review the timing chart for the present operational workflow as shown in Figure 44. The total time required is 409 minutes for one RWR Uploading Team to complete twelve F-16 aircraft.

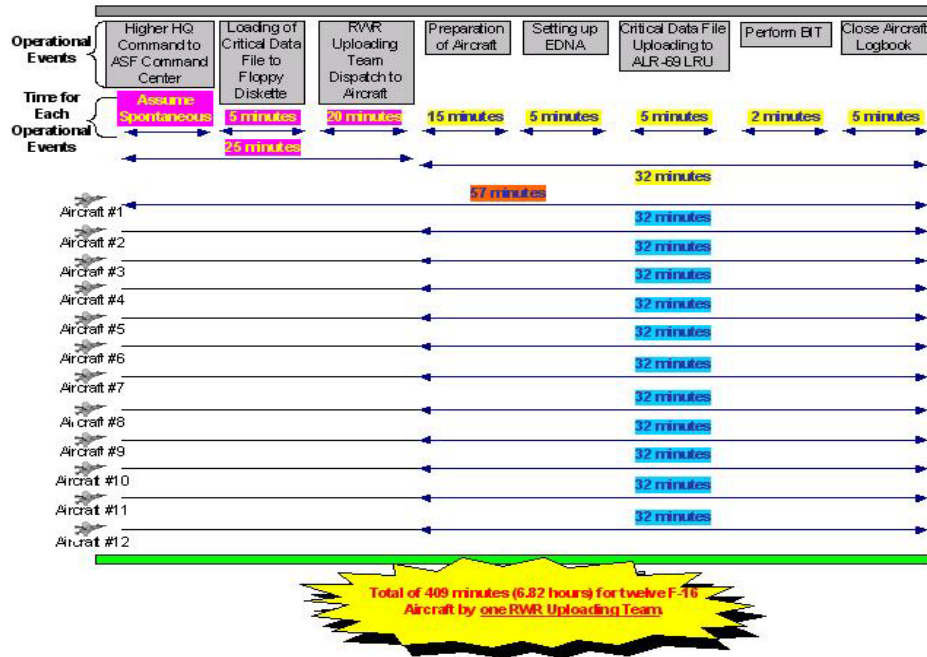
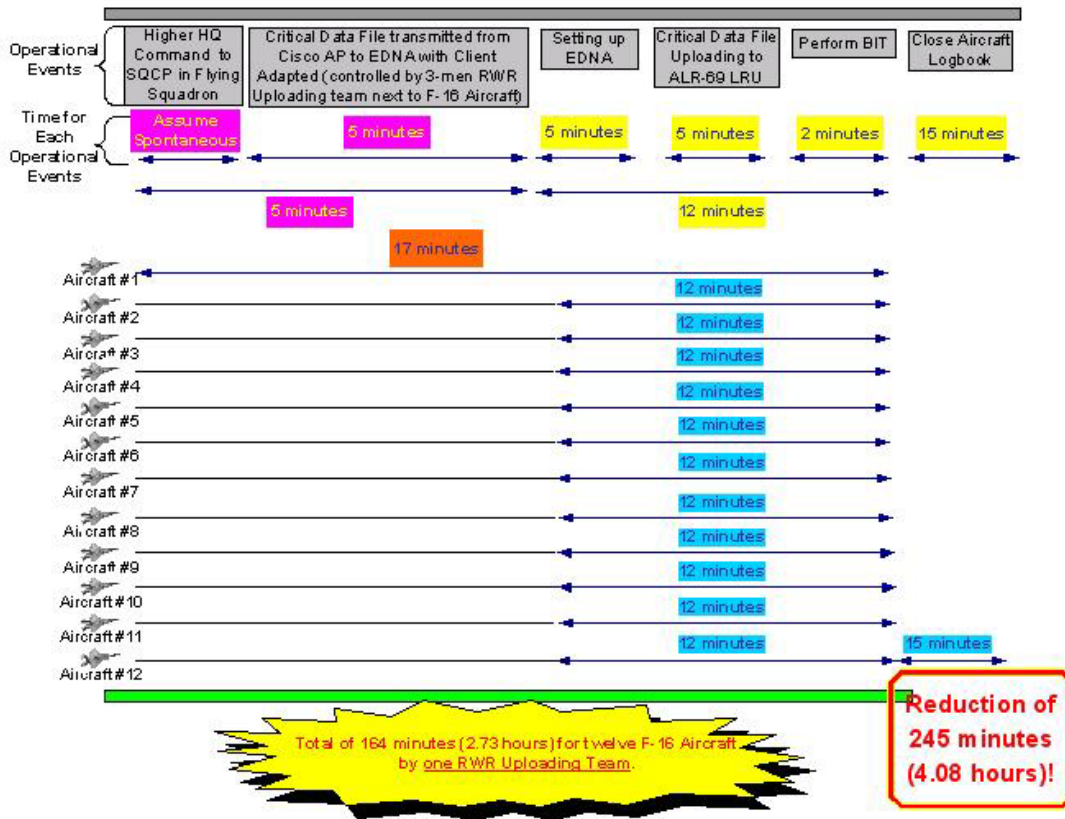


Figure 44 - Timing Chart for Present Operational Events<sup>49</sup>

<sup>49</sup> Similar figure used in Chapter V, Figure 33 in this thesis.



The new timing chart for the operational events for RWR Uploading Team after incorporating the IEEE 802.11b wireless technology upgrade is as shown in Figure 45.



**Figure 45 - New Timing Chart for Operational Events for RWR Uploading Team After Incorporating IEEE 802.11b Wireless Transmission Technology Upgrade**

Comparing Figure 44 and 45, it is evident that the time for one RWR Uploading Team to complete twelve F-16 aircraft is reduced from 409 minutes to 164 minutes. This accounts for a saving of 245 minutes for the total RWR Uploading timing. The breakdown of the saving in RWR Uploading timing is as follows:

**1. Save on Traveling Time**

Time required for loading of new critical data file to floppy and traveling time of RWR Uploading Team from ASF to aircraft originally takes 25 minutes. In the new operational workflow, the time is reduced to just 5 minutes. The RWR Uploading Team is pre-dispatched to the aircraft in the flying squadron. In addition, the new critical data file is sent directly to SQCP and transmitted to the EDNA via wireless media. This allows a saving of 20 minutes of the total RWR uploading time.

## **2. Aircraft is Pre-Prepared**

Aircraft is pre-prepared by the RWR Uploading Team before the receipt of the new critical data file. As explained previously, this is possible as the Higher HQ Command will usually pre-notify the flying squadron which aircraft are required in the next sortie and for whatever mission. This information is usually released hours prior to the release of the new critical data file. As such, it is helpful to capitalize on this information flow by preparing the aircraft for uploading the critical data file even before Higher HQ Command releases the critical data file. By doing so, there is a saving of 15 minutes for each aircraft.

It is also recommended that a separate team, known as Aircraft Preparation Team, be formed and this team is solely responsible for the preparation of the F-16 aircraft. This will allow the RWR Uploading Team to concentrate the uploading of the critical data file to the aircraft. The Aircraft Preparation Team needs to include only two technicians who must be fully qualified on F-16 aircraft. This group of technicians is similar in role to the present aircraft crew chief that is responsible for ensuring full serviceability state of the aircraft and to perform pre-flight checks on the aircraft prior to the arrival of the pilot just before flight. In synergy, it is recommended that aircraft crew chief to take on the role of the Aircraft Preparation Team.

## **3. Consolidation of Closing Paperwork**

In the original operational workflow, the RWR Uploading Team spent about 5 minutes to close the aircraft logbook before proceeding to another aircraft. On the other hand, the new operational workflow recommends that the closure of the aircraft logbook be deferred till the completion of uploading of critical data file on the last aircraft. By doing so, the time required for closing the aircraft logbook is reduced from 60 minutes to just 15 minutes. This yielded a total saving of 45 minutes from the RWR Uploading timing.

In summary, after incorporating the wireless transmission upgrade, the new operational workflow yields a reduction of 245 minutes from original timing of 409 minutes to the new timing of only 164 minutes. The manpower requirement may have increased from one RWR Uploading Team to two teams, namely RWR Uploading Team

and Aircraft Preparation Team, the increase is, however easy to justify because there is a significant time reduction in the new operation workflow after the implementation of the wireless capability upgrade.

**C. BUDGET REQUIRED FOR NEW HARDWARE REQUIRED FOR THE WIRELESS TRANSMISSION CAPABILITY UPGRADE**

The cost to purchase the required hardware amounted to **\$10,730** as shown in Table 4.

Item	Specification	Qty	Cost	Subtotal	Justification
Access Point	Cisco Aironet 1200	6	\$1,200	\$7,200	Two Aps for each squadron and two APs as spares.
Wireless NIC Card	Cisco Aironet® 350 Series Client Adapter	12	\$160	\$1,920	One wireless network adaptor for each of the existing 10 EDNA with two as spares.
Lightning Arrestor	Cisco Aironet Lightning Arrestor (AIR-ACC3354)	7	\$220	\$1,540	One lightning arrestor for each flying squadron with two spares.
Cable	25FT100BT CAT5E CABLE	10	\$7	\$70	Standard Ethernet cable for each flying squadron and some spares.
<b>Hardware Equipment Total</b>				<b>\$10,730</b>	

**Table 4 - Hardware Cost for IEEE 802.11b Wireless Transmission Capability Upgrade**

The required software drivers are packaged in the purchase of the new equipment and thus do not incur any additional purchase cost.

The hardware is covered under manufacturer warranty for the initial first year. Subsequently, it is recommended that Intranet Management Centre (SMC) undertake the repair. It is estimated that the annual recurrent maintenance cost is not more than \$2,000.

**D. SECURITY [16]**

Security is by far the biggest challenge for a wireless LAN design and implementation, and undoubtedly warrants a separate thesis on it. With traditional wired LANs in the pre-Internet age, access to network is controlled by housing it within the office and hence logging on remotely was difficult. But with a wireless LAN, network

communications are broadcast via radio waves past the office walls, through the building and can reach out into the car garage and beyond. Unless proper security is considered and implemented, anyone with the right tool and a little know-how can see the network traffic or gain access to the private network.

All wireless computer systems face security threats that can compromise their systems and services. Unlike the wired network, the intruder does not need physical access in order to pose the following security threats:

- **Eavesdropping**

This involves attacks against the confidentiality of the data that is being transmitted across the network. In the wireless network, eavesdropping is the most significant threat because the attacker can intercept the transmission over the air from a distance away from the premise of the company.

Thick bushes and tall trees usually surround the airbase. In addition, the Flying Squadrons are located deep within the airbase. As such, the probability of eavesdropping by adversary forces is not possible, as the signal of IEEE 802.11b wireless transmission protocol will suffer propagation losses, which does not allow propagation to the perimeter outside the airbase.

- **Tampering**

The attacker can modify the content of the intercepted packets from the wireless network and this results in a loss of data integrity.

- **Unauthorized Access and Spoofing**

The attacker could gain access to privileged data and resources in the network by assuming the identity of a valid user. This kind of attack is known as spoofing. To overcome this attack, proper authentication and access control mechanisms need to be put up in the wireless network.

- **Denial of Services (DOS)**

In this attack, the intruder floods the network with either valid or invalid messages affecting the availability of the network resources. The attacker could also flood a receiving wireless station thereby forcing it to use up its valuable battery power.

- **Other Security Threats**

The other threats come from the weakness in the network administration and vulnerabilities of the wireless LAN standards, e.g. the vulnerabilities of the Wired Equivalent Privacy (WEP), which is supported in the IEEE 802.11 wireless LAN standard.

For the wireless transmission upgrade for this thesis, it is recommended that the following security measures be implemented, at a minimum:

- 1. Change the Default Network Name (SSID)**

SSID stands for **S**ervice **S**et **I**dentifier, a 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the BSS. The SSID differentiates one WLAN from another; so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID. Because an SSID can be sniffed in plain text from a packet it does not supply any security to the network. An SSID is also referred to as a *Network Name* because essentially it is a name that identifies a wireless network. Hackers commonly know each manufacturer's default settings. As such, it is important to change the default SSID, which is needed to sign on to a WLAN and the default password on the AP.

- 2. Disable the SSID Broadcast in the AP Bacon**

By default, APs periodically transmit their SSID values. Wireless utilities in Microsoft XP and freeware such as Network Stumbler<sup>50</sup> capture this value and present a

---

<sup>50</sup> NetStumbler is an IEEE 802.11b tool that listens for available networks and records data about that access point.

list of available networks to the user. Disabling this broadcast makes it more difficult for intruders to recognize the network.

### 3. Enabled Wired Equivalent Privacy (WEP)

Data is transmitted in readable form without encryption, and anyone within the radio range using a wireless protocol analyzer or a promiscuous-mode network adapter may capture the data without joining the network. WEP employs RC4 encryption, the same algorithm used for secure online shopping. WEP encryption can generally be found in 64-bit or 128-bit. Use the stronger 128-bit variety if available.

### 4. Change Encryption Keys Periodically

The basic security rule applies, i.e., the less data transmitted with the same encryption key, the less vulnerable it will be.

### 5. Enable MAC Filtering on APs

Each wireless PC card has a unique identifier known as the MAC address. Many access points have the capability to build a list of MAC addresses that are permitted on the network. Those not listed are denied.

It is important to reiterate that the above steps are minimal; even if all the steps are taken, the data is still at risk. More stringent security considerations need to be put in place if the SAF security requirements change. Table 5 summarizes how all the above security mechanisms work together to reduce the vulnerability of a wireless LAN against the specific threats of eavesdropping, tampering, unauthorized access, spoofing, and DOS.

Protective Mechanism	Spread Spectrum	WEP Encryption	Wireless Network Access ID	Network Authentication	Ethernet Address Restriction
<b>Threat</b>					
<b>Eavesdropping</b>	✓	✓			
<b>Tampering</b>	✓	✓			
<b>Unauthorized Access &amp; Spoofing</b>		✓	✓	✓	✓
<b>Denial of Service</b>	✓				

**Table 5 - Summary of Key Security Mechanism That Can Be Implemented in WLAN**

## **VIII. CONCLUSION AND FUTURE WORK**

### **A. CONCLUSION**

Flexibility, ease, and mobility have certainly made the IEEE 802.11b wireless transmission protocol attractive as an alternative replacement for the old manual floppy diskette method of loading the critical data file from the command center to the EDNA prior to loading the data onto the ALR-69 system onboard the F-16 aircraft.

Two wireless transmission methods, IEEE 802.1x and Free-Space Optics (FSO), were presented. The IEEE 802.1x wireless transmission method is assessed technically and discovered to be relevant for use in the upgrade work of this thesis. Within the family of 802.1x wireless protocols, studies revealed that IEEE 802.11b protocol is deemed most suitable for the upgrade work in this thesis.

With the user's requirement in mind, the Cisco Aironet® 1200 Series wireless access point and the Cisco Aironet® 350 Series Client Adapter were selected as wireless hardware for the upgrade. The total hardware cost for the upgrade amounted to US\$10,730 with an annual recurrent maintenance cost of US\$2,000.

After incorporating the IEEE 802.11b wireless transmission upgrade, the new operational workflow yields a reduction of 245 minutes from original timing of 409 minutes. The new operational workflow requires only 164 minutes for the same amount of F-16 aircraft with just one RWR Uploading Team.

In conclusion, this study has satisfied all the user's requirements and the use of IEEE 802.11b wireless transmission protocol is deemed feasible to replace the manual method (via floppy diskette) of loading the critical data file from the command center to the EDNA prior to loading the data onto the ALR-69 system onboard every F-16 aircraft.

### **B. FUTURE WORK**

#### **1. EDNA Made Redundant**

The EDNA is the most crucial piece of ground equipment in the uploading of the critical data file from the Higher HQ Command to the ALR-69 systems onboard the F-16

aircraft. The EDNA acts like a ‘middle-man’ between the computer in the SQCP and the ALR-69 system onboard the aircraft. With today’s advanced wireless transmission technology, it may be possible to make the EDNA redundant. It may be feasible to transmit the critical data file via wireless medium directly, without the use of EDNA, from the computer in the SQCP to the ALR-69 systems onboard the F-16 aircraft. The ALR-69 systems are required to incorporate the wireless receiving capability to make the EDNA redundant. By doing so, the timing for the operational workflow of the RWR Uploading team can be reduced further.

## **2. Replace EDNA With Other COTS Equipment**

The EDNA is an expensive piece of aircraft ground equipment. One of the potential problems, as described in Chapter V of this thesis, is that there is an insufficient number of EDNAs in the RSAF inventory. In today’s technology-savvy market, other portable and lightweight equipment are readily available. For example the PALM PDA<sup>51</sup> and Toshiba Pocket PC, fitted with fast and powerful CPU with large onboard memory, are deemed sufficient to replace the EDNA as a critical data uploading equipment used by the RWR Uploading Team. The IEEE 802.11b wireless transmission capability is usually integrated into these equipments and is compatible with the wireless transmission upgrade as presented in this thesis. However, the main challenge is the fabrication of connector cables from the PDA or Pocket PC to the ALR-69 systems onboard the F-16 Aircraft. Technically this is assessed to be possible but economically may meet strong resistance from the equipment manufacturer, as this may be deemed to reduce the profit from the sales of the EDNA equipment.

## **3. Critical Issue of Operational Support**

On any network, especially for wireless LANs, it is crucial to plan effective operational support to ensure that the network runs smoothly, because good operational support will enhance availability, performance, and security, and reduce costs. There is need for further research into supporting mechanisms for the wireless LAN in the

---

<sup>51</sup> PDA stands for Personal Digital Assistant.



laboratory. To start, it is recommended that an operational support system for wireless LAN should consider the following:

**a. *Implementing Wireless LAN Support Tools***

Support tools are needed so that network problems can be identified before they become serious. For example, the increase in packet retries on a particular AP could indicate RF interference in that area of the facility or collisions resulting from hidden nodes. The identification of a rogue AP can pinpoint a possible security threat. Support can identify and resolve these problems. Some wireless LAN support tools include products from AirWave, Symbol and Wavelink, which focus on the monitoring and configuration of APs and client devices. For example, the AirWave Management Platform is a comprehensive wireless network management solution that helps reduce support costs, improve network performance, and enforce security policies uniformly across the wireless LAN.

**b. *Monitoring the Network***

The network is monitored for connectivity, status, availability, performance attributes and security settings. Monitoring needs to be done regularly by examining each AP and user. Again, tools like AirWave have features to indicate possible channel interference and environmental factors that impact performance. However, too much monitoring can have negative consequences as it introduces overhead on the network, which lowers throughput. As such, the network needs to be monitored sparingly. Most of the support tools have user-defined triggers that will automatically alert staff from the Intranet Management Centre (SMC) via a console, e-mail, or pager if problems crop up. For example, the software can trigger an alert if it detects an AP's configuration parameters are different from security policies, which may mean it is a rogue AP.

**c. *Configuration Management***

The main benefit of some supporting tools is that they allow remote control of multi-vendor access points, and provide access to security settings, RF channel

settings, SSID, Power-over-Ethernet (PoE<sup>52</sup>) control, and network management. The SMC staff uses a centralized console to perform configuration management of all APs instead of interfacing with each AP separately. Some support tools can even configure new APs automatically when they are found and ensure that they comply with security policies. This feature is good because the AP may be operating with factory default settings, which generally does not include any form of security. This ensures all APs are set the same, and thus improves security.

However, a sound operational support plan for wireless LANs is not inexpensive and one needs to weigh the pros and cons of the requirements versus the costs and manpower needs before deciding on the right balance.

---

<sup>52</sup> A Power-over-Ethernet (PoE) or "Active Ethernet" solution only requires technicians to run one Ethernet cable to the access point for supplying both power and data. With PoE, power-sourcing equipment detects the presence of an appropriate "powered device" (e.g., an access point or Ethernet hub) and injects applicable current into the data cable. An access point can operate solely from the power it receives through the data cable. This allows greater flexibility in the locating of AP's and network devices and may significantly decrease installation costs.

## **APPENDIX A: CISCO AIRONET® 1200 SERIES ACCESS POINT**

The Cisco Aironet® 1200 Series AP, see Figure 46, sets the enterprise standard for next generation high performance, secure, manageable, and reliable wireless local-area networks (WLANs), while also providing investment protection because of its upgrade capability and compatibility with current standards. The modular design of the Cisco Aironet® 1200 AP supports IEEE 802.11a and 802.11b technologies in both single and dual-mode operation. You can configure the Cisco Aironet® 1200 to meet customerspecific requirements at the time of purchase and then reconfigure and upgrade the product in the field as these requirements evolve. In addition, the Cisco Aironet® 1200 Series creates a wireless infrastructure that provides customers with maximum mobility and flexibility, enabling constant connection to all network resources from virtually anywhere wireless access is deployed.



**Figure 46 - Cisco Aironet® 1200 Series Access Point**

## A. KEY FEATURES AND BENEFITS<sup>53</sup>

Feature	Benefit
Modular platform for single or dual band operation	The access point can be configured for either IEEE 802.11b only, 802.11a only, or for simultaneous support of IEEE 802.11b and IEEE 802.11a to provide the maximum number of channels and maximum available data rates in a single device.
Field upgradable radios	Flexibility and investment protection is provided through field-upgradable card bus and mini-PCI radios. CardBus-based IEEE 802.11a modules can easily be fitted into installed Cisco Aironet 1200 Series access points.
5 GHz integrated antennas	Unique articulating antenna paddle incorporates high-gain omnidirectional and hemispherical patch antennas to deliver two distinct coverage patterns.
2.4 and 5 GHz Diversity Antennas	Diversity antennas for both the 2.4 and 5 GHz radios ensures optimum performance in high-multipath environments such as offices, warehouses, and other indoor installations.
Cisco IOS Software	Provides end-to-end solution support for Intelligent Network Services. Produces predictable and consistent network behavior with uniform applications and services.
Virtual LAN (VLAN) support	Allows segmentation of up to 16 user groups creating increased system flexibility by allowing differentiation of LAN policies and services, such as security and QoS, for different users.
Quality of Service (QoS) support	Prioritization of traffic for different application requirements to improve the voice and video user-experience.
Proxy Mobile IP	Provides seamless roaming between subnets and enhances mobility of voice over IEEE 802.11 wireless.
Cisco Structured Wireless-Aware Network (SWAN)	A comprehensive Cisco framework for deploying, operating, and managing hundreds to thousands of Cisco Aironet access points using the Cisco infrastructure. This framework extends to the wireless LAN the same level of security, scalability, and reliability that customers have come to expect in their wired LAN by introducing "wireless-aware" capabilities into the Cisco infrastructure.
Wireless Domain Services (WDS)	A component of the Cisco Structured Wireless-Aware Network, WDS is a collection of Cisco IOS Software features that enhance WLAN client mobility and simplify WLAN deployment and management. WDS includes fast secure roaming and IEEE 802.1X local authentication.
Fast Secure Roaming	Allows authenticated client devices to roam securely from one access point to another without any perceptible delay during reassociation. Provides support for latency-sensitive applications such as VoIP, ERP and Citrix.
IEEE 802.1X Local Authentication Service	Allows the access point to act as a local RADIUS server to authenticate wireless clients when the AAA server is not available. Provides remote site survivability and backup authentication services during WAN link or server failure.
Two reverse-polarity threaded naval connectors (RP-TNC) for external 2.4 GHz antenna connection	Diversity support for the 2.4 GHz radio to improve reliability in high-multipath environments. The RP-TNC connectors are compatible with the Cisco Aironet optional antennas, enabling WLAN architects to customize radio coverage for specific deployment scenarios.
8 MB Flash memory	Provides memory space for future firmware upgrades and supports new IEEE 802.11 standards and advanced features.
Support for Cisco Discovery Protocol and Software Image Manager (SWIM) within CiscoWorks Resource Essentials (RME)	Allows centralized and automatic firmware upgrades on remote access points across the enterprise.
Standard IEEE 802.11b radio with 100-mW maximum transmit power and 85-dBm receive sensitivity at 11 Mbps data rate	2.4 GHz radio offers superior radio performance that results in industry-leading range. The greater the range of the access point, the fewer access points needed, resulting in lower total system cost.
IEEE 802.11a radio module provides 40-mW maximum transmit power for UNII 1 and UNII2 bands and -68 dBm (typical) receive sensitivity at 54 Mbps data rate	Superior 5 GHz radio design provides industry-leading performance and receive sensitivity and maximum capacity through eight nonoverlapping channels in the UNII1 and UNII 2 bands.
Support for both line power over Ethernet and local power	To decrease the cost and complexity of installation, the Cisco Aironet 1200 Series can be powered over an Ethernet cable, eliminating the need to run expensive AC power to remote access-point installation locations. Depending on radio configuration, the Cisco 1200 Series can be powered via Cisco line-power-enabled switches, multipoint midspan power panels, or single-port power injectors. In instances where AC power is available at the installation location, the power supply for the Cisco Aironet 1200 Series can be plugged into an electrical outlet.
Aesthetically pleasing cast aluminum case, Underwriters Laboratories Inc. (UL) 2043 certification, and extended operating temperature (-20 to 55°C or -4 to 131°F)	The product design meets the aesthetic requirements of the enterprise and the rugged features support deployment in factories, warehouses, and the outdoors (in a NEMA enclosure). The broad operating temperature range and UL 2043 certification for plenum rating requirements set by local fire codes supports installation in environmental air spaces such as areas above suspended ceilings.
Multipurpose mounting bracket	Flexibility of the multipurpose mounting bracket gives numerous deployment options for site-specific requirements.
Two separate locking mechanisms for the access point and radio	Theft deterrence has become a requirement as wireless LANs proliferate into public areas. Additional investment protection is provided with built-in locking mechanisms.

<sup>53</sup> Information obtained from [www.cisco.com](http://www.cisco.com), accessed on November 3, 2003.

## B. HARDWARE SPECIFICATIONS

Specifications	With IEEE 802.11a Radio Installed	With IEEE 802.11b Radio Installed	With both IEEE 802.11a and 802.11b Radios Installed
Radio module form factor	CardBus (32-bit)	Mini-PCI (32-bit)	IEEE 802.11a: CardBus (32-bit) IEEE 802.11b: Mini-PCI (32-bit)
Data rates supported	6, 9, 12, 18, 24, 36, 48, and 54 Mbps	1, 2, 5.5, and 11 Mbps	IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps IEEE 802.11b: 1, 2, 5.5, and 11 Mbps
Network standard	IEEE 802.11a	IEEE 802.11b	IEEE 802.11a IEEE 802.11b
Uplink	Autosensing 802.3 10/100Base-T Ethernet	Autosensing 802.3 10/100Base-T Ethernet	Autosensing 802.3 10/100Base-T Ethernet
Frequency band	5.15 to 5.35 GHz (FCC UNII 1 and UNII 2) 5.15 to 5.25 GHz (TELECOM) 5.15 to 5.25 GHz (Singapore) 5.25 to 5.35 GHz (Taiwan)	2.412 to 2.462 GHz (FCC) 2.412 to 2.472 GHz (ETSI) 2.412 to 2.484 GHz (TELECOM) 2.412 to 2.462 GHz (MII) 2.422 to 2.452 GHz (Israel)	5.15 to 5.35 GHz (FCC UNII 1 and UNII 2) 5.15 to 5.25 GHz (TELECOM) 5.15 to 5.25 GHz (Singapore) 5.25 to 5.35 GHz (Taiwan) 2.412 to 2.462 GHz (FCC) 2.412 to 2.472 GHz (ETSI) 2.412 to 2.484 GHz (TELECOM) 2.412 to 2.462 GHz (MII) 2.422 to 2.452 GHz (Israel)
Network architecture type	Infrastructure, star topology	Infrastructure, star topology	Infrastructure, star topology
Wireless medium	Orthogonal frequency-division multiplexing (OFDM)	Direct Sequence Spread Spectrum (DSSS)	IEEE 802.11a: Orthogonal Frequency Division Multiplexing (OFDM) IEEE 802.11b: Direct Sequence Spread Spectrum (DSSS)
Media Access Protocol	Carrier sense multiple access with collision avoidance (CSMA/CA)	Carrier sense multiple access with collision avoidance (CSMA/CA)	Carrier sense multiple access with collision avoidance (CSMA/CA)
Modulation	(OFDM subcarrier) BPSK @ 6 and 9 Mbps QPSK @ 12 and 18 Mbps 16-QAM @ 24 and 36 Mbps 64-QAM @ 48 and 54 Mbps	DBPSK @ 1 Mbps DQPSK @ 2 Mbps CCK @ 5.5 and 11 Mbps	OFDM: • BPSK @ 6 and 9 Mbps • QPSK @ 12 and 18 Mbps • 16-QAM @ 24 and 36 Mbps • 64-QAM @ 48 and 54 Mbps DSSS: • DBPSK @ 1 Mbps • DQPSK @ 2 Mbps • CCK @ 5.5 and 11 Mbps

Specifications	With IEEE 802.11a Radio Installed	With IEEE 802.11b Radio Installed	With both IEEE 802.11a and 802.11b Radios Installed
Operating channels	FCC: 8 TELEC (Japan): 4 Singapore: 4 Taiwan: 4	ETSI: 13 Israel: 7 North America: 11 TELEC (Japan):14 MII: 11	5 GHz Band • FCC: 8 • TELEC (Japan): 4 • Singapore: 4 • Taiwan: 4 2.4 GHz Band • ETSI: 13 • Israel: 7 • North America: 11 • TELEC (Japan):14 • MII: 11
Nonoverlapping channels	8 (FCC only) 4 (Japan, Singapore, Taiwan)	3	11
Receive sensitivity	6 Mbps: -85 dBm 9 Mbps: -84 dBm 12 Mbps: -82 dBm 18 Mbps: -80 dBm 24 Mbps: -77 dBm 36 Mbps: -73 dBm 48 Mbps: -69 dBm 54 Mbps: -68 dBm	1 Mbps: -94 dBm 2 Mbps: -91 dBm 5.5 Mbps: -89 dBm 11 Mbps: -85 dBm	1 Mbps: -94 dBm 2 Mbps: -91 dBm 5.5 Mbps: -89 dBm 6 Mbps: -85 dBm 9 Mbps: -84 dBm 11 Mbps: -85 dBm 12 Mbps: -82 dBm 18 Mbps: -80 dBm 24 Mbps: -77 dBm 36 Mbps: -73 dBm 48 Mbps: -69 dBm 54 Mbps: -68 dBm
Available transmit power settings	40 mW (16 dBm) 20 mW (13 dBm) 10 mW (10 dBm) 5 mW (7 dBm) Maximum power setting will vary according to local regulations.	100 mW (20 dBm) 50 mW (17 dBm) 30 mW (15 dBm) 20 mW (13 dBm) 5 mW (7 dBm) 1 mW (0 dBm) Maximum power setting will vary according to local regulations.	IEEE 802.11a • 40 mW (16 dBm) • 20 mW (13 dBm) • 10 mW (10 dBm) • 5 mW (7 dBm) IEEE 802.11b • 100 mW (20 dBm) • 50 mW (17 dBm) • 30 mW (15 dBm) • 20 mW (13 dBm) • 5 mW (7 dBm) • 1 mW (0 dBm) Maximum power setting will vary according to local regulations.

Specifications	With IEEE 802.11a Radio Installed	With IEEE 802.11b Radio Installed	With both IEEE 802.11a and 802.11b Radios Installed
Range (typical at maximum transmit power setting, 2.2 dBi gain diversity dipole antenna for 2.4 GHz; 6 dBi gain patch and 5 dBi omni antenna for 5 GHz)	<p>Omnidirectional antenna:</p> <ul style="list-style-type: none"> <li>• Indoor: <ul style="list-style-type: none"> <li>— 60 ft (18 m) @ 54 Mbps</li> <li>— 130 ft (40 m) @ 18 Mbps</li> <li>— 170 ft (52 m) @ 6 Mbps</li> </ul> </li> <li>• Outdoor: <ul style="list-style-type: none"> <li>— 100 ft (30 m) @ 54 Mbps</li> <li>— 600 ft (183 m) @ 18 Mbps</li> <li>— 1000 (304 m) ft @ 6 Mbps</li> </ul> </li> </ul> <p>Patch antenna:</p> <ul style="list-style-type: none"> <li>• Indoor: <ul style="list-style-type: none"> <li>— 70 ft (21 m) @ 54 Mbps</li> <li>— 150 ft (45 m) @ 18 Mbps</li> <li>— 200 ft (61 m) @ 6 Mbps</li> </ul> </li> <li>• Outdoor: <ul style="list-style-type: none"> <li>— 120 ft (36 m) @ 54 Mbps</li> <li>— 700 ft (213 m) @ 18 Mbps</li> <li>— 1200 ft (355 m) @ 6 Mbps</li> </ul> </li> </ul>	<p>Indoor:</p> <ul style="list-style-type: none"> <li>• 130 ft (40 m) @ 11 Mbps</li> <li>• 350 ft (107 m) @ 1 Mbps</li> </ul> <p>Outdoor:</p> <ul style="list-style-type: none"> <li>• 800 ft (244 m) @ 11 Mbps</li> <li>• 2000 ft (610 m) @ 1 Mbps</li> </ul>	<p>IEEE 802.11a omnidirectional antenna:</p> <ul style="list-style-type: none"> <li>• Indoor: <ul style="list-style-type: none"> <li>— 60 ft (18 m) @ 54 Mbps</li> <li>— 130 ft (40 m) @ 18 Mbps</li> <li>— 170 ft (52 m) @ 6 Mbps</li> </ul> </li> <li>• Outdoor: <ul style="list-style-type: none"> <li>— 100 ft (30 m) @ 54 Mbps</li> <li>— 600 ft (183 m) @ 18 Mbps</li> <li>— 1000 ft (304 m) @ 6 Mbps</li> </ul> </li> </ul> <p>IEEE 802.11a patch antenna:</p> <ul style="list-style-type: none"> <li>• Indoor: <ul style="list-style-type: none"> <li>— 70 ft (21 m) @ 54 Mbps</li> <li>— 150 ft (45 m) @ 18 Mbps</li> <li>— 200 ft (61 m) @ 6 Mbps</li> </ul> </li> <li>• Outdoor: <ul style="list-style-type: none"> <li>— 120 ft (36 m) @ 54 Mbps</li> <li>— 700 ft (213 m) @ 18 Mbps</li> <li>— 1200 ft (355 m) @ 6 Mbps</li> </ul> </li> </ul> <p>IEEE 802.11b omnidirectional antenna:</p> <ul style="list-style-type: none"> <li>• Indoor: <ul style="list-style-type: none"> <li>— 130 ft (40 m) @ 11 Mbps</li> <li>— 350 ft (107 m) @ 1 Mbps</li> </ul> </li> <li>• Outdoor: <ul style="list-style-type: none"> <li>— 800 ft (244 m) @ 11 Mbps</li> <li>— 2000 ft (610 m) @ 1 Mbps</li> </ul> </li> </ul>
Antenna	Integrated 6 dBi diversity patch (55 degree horizontal, 55 degree vertical beamwidths, 5 dBi diversity omnidirectional with 360 degree horizontal and 40 degree vertical beamwidths)	2 RP-TNC connectors (antennas optional, none supplied with unit)	<p>5 GHz</p> <ul style="list-style-type: none"> <li>• Integrated 6-dBi diversity patch (55° horizontal, 55° vertical beamwidths, 5 dBi diversity omnidirectional with 360° horizontal and 40° vertical beamwidths)</li> </ul> <p>2.4 GHz</p> <ul style="list-style-type: none"> <li>• 2 RP-TNC connectors (antennas optional, none supplied with unit)</li> </ul>

Specifications	With IEEE 802.11a Radio Installed	With IEEE 802.11b Radio Installed	With both IEEE 802.11a and 802.11b Radios Installed
Security architecture client authentication	<p>Cisco Wireless Security Suite including:</p> <p>Authentication:</p> <ul style="list-style-type: none"> <li>IEEE 802.1X support including LEAP, PEAP, EAP-TLS, EAP-TTLS, and EAP-SIM to yield mutual authentication and dynamic, per-user, per-session WEP keys</li> <li>MAC address and by standard IEEE 802.11 authentication mechanisms</li> <li>Supports Wi-Fi Protected Access (WPA)</li> </ul> <p>Encryption:</p> <ul style="list-style-type: none"> <li>Support for static and dynamic IEEE 802.11 WEP keys of 40 bits and 128 bits</li> <li>Pre-standard TKIP WEP enhancements: key hashing (per-packet keying), message integrity check (MIC) and broadcast key rotation</li> <li>Supports Wi-Fi Protected Access (WPA)</li> </ul>	<p>Cisco Wireless Security Suite including:</p> <p>Authentication:</p> <ul style="list-style-type: none"> <li>IEEE 802.1X support including LEAP, PEAP, EAP-TLS, EAP-TTLS, and EAP-SIM to yield mutual authentication and dynamic, per-user, per-session WEP keys</li> <li>MAC address and by standard IEEE 802.11 authentication mechanisms</li> <li>Supports Wi-Fi Protected Access (WPA)</li> </ul> <p>Encryption:</p> <ul style="list-style-type: none"> <li>Support for static and dynamic IEEE 802.11 WEP keys of 40 bits and 128 bits</li> <li>Pre-standard TKIP WEP enhancements: key hashing (per-packet keying), message integrity check (MIC) and broadcast key rotation</li> <li>Supports Wi-Fi Protected Access (WPA)</li> </ul>	<p>Cisco Wireless Security Suite including:</p> <p>Authentication:</p> <ul style="list-style-type: none"> <li>IEEE 802.1X support including LEAP, PEAP, EAP-TLS, EAP-TTLS, and EAP-SIM to yield mutual authentication and dynamic, per-user, per-session WEP keys</li> <li>MAC address and by standard IEEE 802.11 authentication mechanisms</li> <li>Supports Wi-Fi Protected Access (WPA)</li> </ul> <p>Encryption:</p> <ul style="list-style-type: none"> <li>Support for static and dynamic IEEE 802.11 WEP keys of 40 bits and 128 bits</li> <li>Pre-standard TKIP WEP enhancements: key hashing (per-packet keying), message integrity check (MIC) and broadcast key rotation</li> <li>Supports Wi-Fi Protected Access (WPA)</li> </ul>
Status LEDs	3 indicators on the top panel report association status, operation, error/warning, firmware upgrade and configuration, network/modem, and radio status.	3 indicators on the top panel report association status, operation, error/warning, firmware upgrade and configuration, network/modem, and radio status.	3 indicators on the top panel report association status, operation, error/warning, firmware upgrade and configuration, network/modem, and radio status.
Software image network and inventory support	CiscoWorks RME <sup>1</sup> , CiscoWorks SWIM <sup>2</sup>	CiscoWorks RME, CiscoWorks SWIM	CiscoWorks RME, CiscoWorks SWIM
Remote configuration support	DHCP <sup>3</sup> , Telnet, HTTP, FTP <sup>4</sup> , TFTP <sup>5</sup> , and SNMP	DHCP, Telnet, HTTP, FTP, TFTP, and SNMP	DHCP, Telnet, HTTP, FTP, TFTP, and SNMP
Local configuration	Direct console port (RJ-45 interface)	Direct console port (RJ-45 interface)	Direct console port (RJ-45 interface)
Processor	IBM PowerPC405 200 MHz	IBM PowerPC405 200 MHz	IBM PowerPC405 200 MHz
System Memory	16 MB RAM 8 MB Flash	16 MB RAM 8 MB Flash	16 MB RAM 8 MB Flash
Warranty	1 year	1 year	1 year

1. CiscoWorks Resource Manager Essentials
2. Software Image Manager
3. Dynamic Host Configuration Protocol
4. File Transfer Protocol
5. Trivial File Transfer Protocol

## C. POWER REQUIREMENTS

Specifications	With IEEE 802.11a Radio Installed	With IEEE 802.11b Radio Installed	With both IEEE 802.11a and 802.11b Radios Installed
Input power requirements	90 to 240 VAC +/-10% (power supply) 48 VDC +/-10% (device)	90 to 240 VAC +/-10% (power supply) 48 VDC +/-10% (device)	90 to 240 VAC +/-10% (power supply) 48 VDC +/-10% (device)
Power Draw	8 watts, RMS	6 watts, RMS	11 watts, RMS



## D. PHYSICAL AND ENVIRONMENTAL SPECIFICATIONS FOR CISCO AIRONET 1200 SERIES ACCESS POINT

Specifications	With IEEE 802.11a Radio Installed	With IEEE 802.11b Radio Installed	With both IEEE 802.11a and 802.11b Radios Installed
Dimensions (H x W x D)	1.660 x 6.562 x 7.232 in. (4.22 x 16.67 x 18.37 cm) Mounting bracket adds 0.517 in. (1.31 cm) to the height	1.660 x 6.562 x 7.232 in. (4.22 x 16.67 x 18.37 cm) Mounting bracket adds 0.517 in. (1.31 cm) to the height	1.660 x 6.562 x 7.232 in. (4.22 x 16.67 x 18.37 cm) Mounting bracket adds 0.517 in. (1.31 cm) to the height
Weight	26 oz (737 g) add 6.4 oz (181 g) for mounting bracket	25.6 oz (724 g) add 6.4 oz (181 g) for mounting bracket	27.6 oz (783 g) add 6.4 oz (181 g) for mounting bracket
Operating Temperature	-4° to 122°F (-20° to 50°C)	-4° to 131°F (-20° to 55°C)	-4° to 122°F (-20° to 50°C)
Operating Relative Humidity	10 to 90% humidity (noncondensing)	10 to 90% humidity (noncondensing)	10 to 90% humidity (noncondensing)

## E. REGULATORY APPROVALS FOR CISCO AIRONET 1200 SERIES ACCESS POINT

Specifications	With IEEE 802.11a Radio Installed	With IEEE 802.11b Radio Installed	With both IEEE 802.11a and 802.11b Radios Installed
Safety	UL 1950 CSA 22.2 No. 950-95 IEC 60950 EN 60950	UL 1950 CSA 22.2 No. 950-95 IEC 60950 EN 60950	UL 1950 CSA 22.2 No. 950-95 IEC 60950 EN 60950
Radio approvals	FCC Part 15.401-15.407 RSS-210 (Canada) EN 301.893 (Europe) ARIB STD-171 (Japan) AS 4268.2 (Australia)	FCC Part 15.247 RSS-139-1, RSS-210 (Canada) EN 300.328 (Europe) Telec 33B (Japan) AS/NZS 3548 (Australia and New Zealand)	FCC Part 15.401-15.407 RSS-210 (Canada) EN 301.893 (Europe) ARIB STD-171 (Japan) AS 4268.2 (Australia) FCC Part 15.247 RSS-139-1, RSS-210 (Canada) EN 300.328 (Europe) Telec 33B (Japan) AS/NZS 3548 (Australia and New Zealand)
EMI and susceptibility (Class B)	FCC Part 15.107 and 15.109 ICES-003 (Canada) VCCI (Japan) EN 301.489-1 and -17 (Europe)	FCC Part 15.107 and 15.109 ICES-003 (Canada) VCCI (Japan) EN 301.489-1 and -17 (Europe)	FCC Part 15.107 and 15.109 ICES-003 (Canada) VCCI (Japan) EN 301.489-1 and -17 (Europe)
Other	IEEE 802.11a FCC Bulletin OET-65C RSS-102	IEEE 802.11b FCC Bulletin OET-65C RSS-102	IEEE 802.11a IEEE 802.11b FCC Bulletin OET-65C RSS-102
SNMP compliance	MIB <sup>1</sup> I and MIB II	MIB I and MIB II	MIB I and MIB II
Wi-Fi Certification	Certified Interoperability for 5 GHz Band at 54 Mbps	Certified Interoperability for 2.4 GHz Band at 11 Mbps	Certified Interoperability for 2.4 GHz Band at 11 Mbps

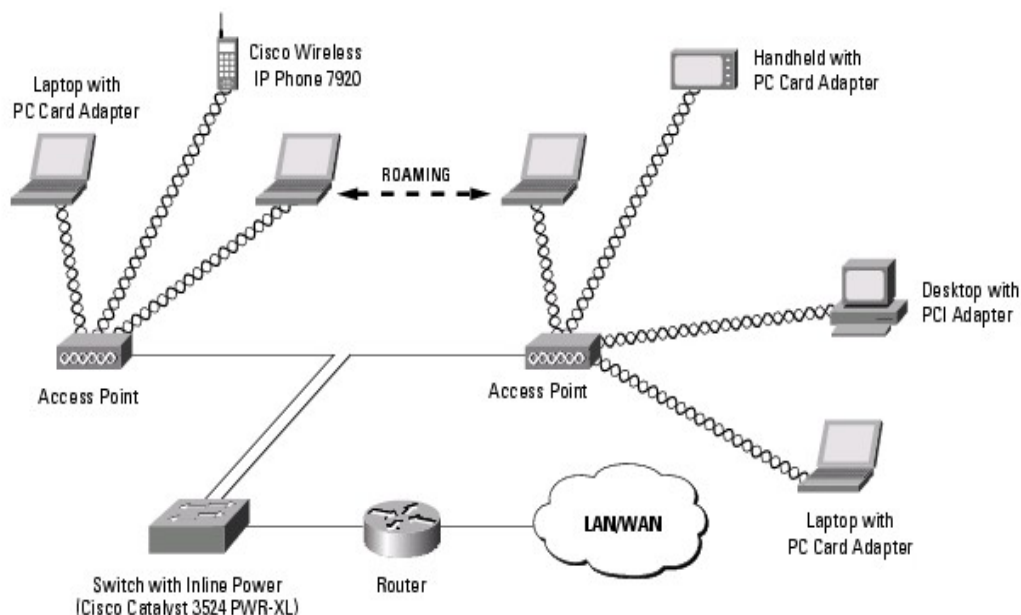
1. Management Information Base

THIS PAGE INTENTIONALLY LEFT BLANK

## APPENDIX B: CISCO AIRONET® 350 SERIES CLIENT FOR THE EDNA

Wireless client adapters are the key to adding mobility and flexibility to an enterprise - increasing productivity by enabling users to have network and Internet access anywhere within a building without the limitation of wires. The Cisco Aironet® 350 Series Client Adapters are a complement to Aironet® 350 Series infrastructure devices, providing an enterprise-ready solution that combines mobility with the performance, security, and manageability that people have come to expect from Cisco.

Wireless client adapters connect a variety of devices to a wireless network either in ad hoc peer-to-peer mode or in infrastructure mode with access points. Available in PC Card (PCMCIA) and Peripheral Component Interconnect (PCI) form factors, Cisco Aironet® 350 Series Client Adapters quickly connect desktop and mobile computing devices wirelessly to all network resources. With this product, you can instantly add new employees to the network, support temporary workgroups, or enable Internet access in conference rooms or other meeting spaces (see Figure 47).



**Figure 47 - Client Devices Equipped With Wireless Client Adapters Can Roam Freely Throughout a Facility Via Communications With Multiple Access Points**

Features include:

- Superior range and throughput
- Secure network communications
- World mode for international roaming
- Full-featured utilities for easy configuration and management
- Compliance with the IEEE 802.11b high-rate standard
- Support for all popular operating systems

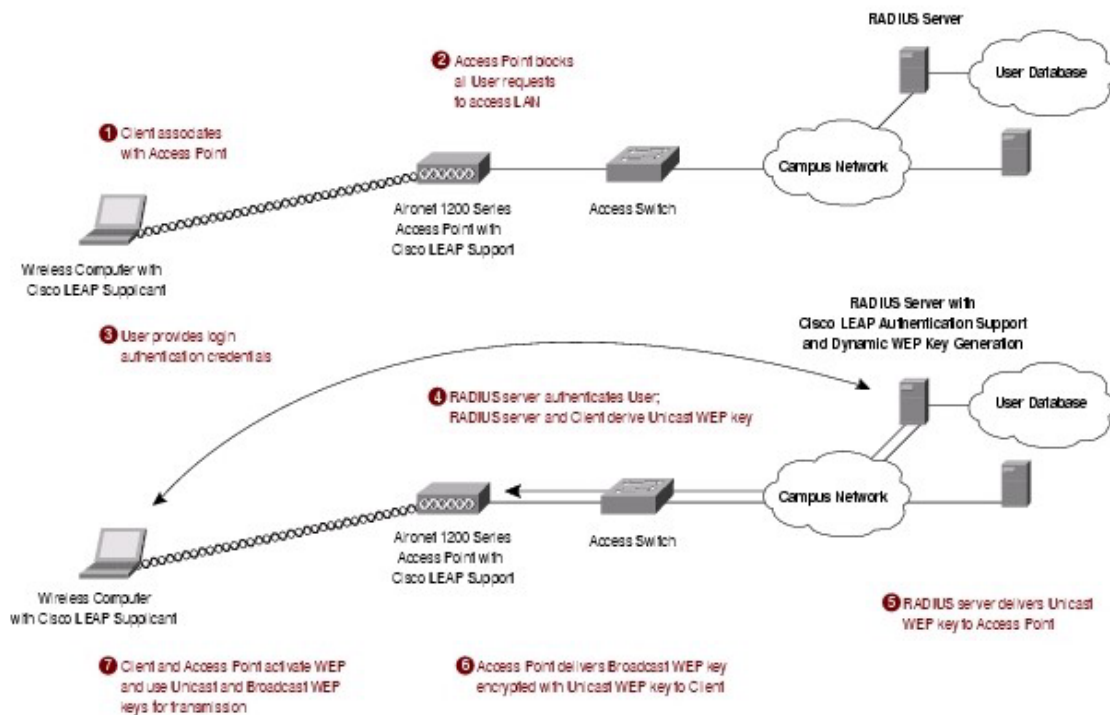
#### **A. ETHERNET SPEED AND IMPROVED RANGE**

With a full 100 milliwatts (mW) of transmit power and the best receive sensitivity in the industry, the Cisco Aironet® 350 Series Client Adapters provide the longest range and best reliability available for wireless clients. Advanced signal processing in the Cisco Aironet® 350 Series helps manage the multipath propagation often found in office environments. Intelligent filtering addresses ambient noise and interference that can decrease network performance. Building upon Cisco leadership in wireless LAN (WLAN) performance, the Cisco Aironet® 350 Series Client Adapters provide the greatest throughput available so users can enjoy virtually the same connectivity they gain from wire-line connections. Based on direct sequence spread spectrum (DSSS) technology and operating in the 2.4 GHz band, the Cisco Aironet® 350 Series Client Adapters comply with the IEEE 802.11b standard - ensuring interoperability with all other compliant WLAN products.

#### **B. ENTERPRISE-CLASS WIRELESS LAN SECURITY**

Wireless LAN security is a primary concern. Cisco Aironet products secure the enterprise network with a scalable and manageable system featuring the award-winning Cisco Wireless Security Suite. Based on the 802.1x standard for port-based network access, the Cisco Wireless Security Suite takes advantage of the Extensible Authentication Protocol (EAP) framework for user-based authentication (Figure 48).

The Cisco Wireless Security Suite interoperates with a range of client devices. It supports all 802.1x authentication types, including Cisco LEAP, Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) and types that operate over EAP-TLS, such as Protected Extensible Authentication Protocol (PEAP), EAP-Tunneled TLS (EAP-TTLS) and EAP-Subscriber Identity Module (EAP-SIM). A wide selection of Remote Access Dial-In User Service (RADIUS) servers, such as the Cisco Secure Access Control Server (ACS), can be used for enterprise-class centralized user management. Enhanced features such as Temporal Key Integrity Protocol (TKIP) per-packet key hashing, message integrity check (MIC) and broadcast key rotation are integral to the Cisco Wireless Security Suite.



**Figure 48 - The Cisco Wireless Security Suite is an Enterprise-Class Security System Based on the 802.1x Architecture**


**C. SPECIFICATIONS FOR CISCO AIRONET® 350 SERIES CLIENT ADAPTERS [FROM 16]**

Data Rates Supported	1, 2, 5.5, and 11 Mbps
Network Standard	IEEE 802.11b
System Interface	AIR-PCM35x: PC Card (PCMCIA) Type II AIR-PCI351x: peripheral component interconnect (PCI) Bus
Frequency Band	2.4 to 2.4897 GHz
Network Architecture Types	Infrastructure and ad hoc
Wireless Medium	Direct Sequence Spread Spectrum (DSSS)
Media Access Protocol	Carrier sense multiple access with collision avoidance (CSMA/CA)
Modulation	DBPSK @1 Mbps DQPSK @ 2 Mbps CCK @ 5.5 and 11 Mbps
Operating Channels	North America: 11 ETSI: 13 Japan: 14
Non-overlapping Channels	Three
Receive Sensitivity	1 Mbps: -94 dBm 2 Mbps: -91 dBm 5.5 Mbps: -89 dBm 11 Mbps: -85 dBm
Delay Spread	1 Mbps: 500 ns 2 Mbps: 400 ns 5.5 Mbps: 300 ns 11 Mbps: 140 ns

<p>Available Transmit Power Settings</p>	<p>100 mW (20 dBm)  50 mW (17 dBm)  30 mW (15 dBm)  20 mW (13 dBm)  5 mW (7 dBm)  1 mW (0 dBm)</p> <p>Maximum power setting will vary according to individual country regulations.</p>
<p>Range (typical)</p>	<p>Indoor:  130 ft (40 m) @ 11 Mbps  350 ft (107 m) @ 1 Mbps</p> <p>Outdoor:  800 ft (244 m) @ 11 Mbps  2000 ft (610 m) @ 1 Mbps</p>
<p>Compliance</p>	<p>Operates license free under FCC Part 15 and complies as a Class B device; complies with DOC regulations; complies with ETS 300.328, FTZ 2100, and MPT 1349 standards</p>
<p>Operating Systems Supported</p>	<p>Windows 95, 98, NT 4.0, 2000, ME, XP, CE 2.11, CE 3.0, CE .NET (CE 4.0, CE 4.1), Mac OS 9.x, Mac OS X, MS-DOS and Linux</p>
<p>Antenna</p>	<p>AIR-PCM35x: Integrated diversity dipoles</p> <p>AIR-LMC35x: Two MMCX connectors (antennas optional, none supplied with unit)</p> <p>AIR-PCI35x: External, removable 2.2 dBi Dipole with RP-TNC Connector</p>

Encryption Key Length	128-bit
Security	<p>Cisco Wireless Security Suite including:</p> <p>Authentication:</p> <p>802.1X support including Cisco LEAP, PEAP, EAP-TLS, EAP-TTLS, and EAP-SIM to yield mutual authentication and dynamic, per-user, per-session WEP keys</p> <p>MAC address and by standard 802.11 authentication mechanisms</p> <p>Encryption:</p> <p>Support for static and dynamic IEEE 802.11 WEP keys of 40 bits and 128 bits</p> <p>TKIP WEP enhancements: key hashing (per-packet keying), message integrity check (MIC) and broadcast key rotation</p>
Status Indicators	Link Status and Link Activity
Dimensions	<p>AIR-PCM35x: 2.13 in. (5.4 cm) wide x 4.37 in. (11.1 cm) deep x 0.1 in. (0.3 cm) high</p> <p>AIR-LMC35x: 2.13 in. (5.4 cm) wide x 3.31 in. (8.4 cm) deep x 0.1 in. (0.3 cm) high</p> <p>AIR-PCI35x: 6.6 in. (16.8 cm) wide by 3.9 in. (9.8 cm) x .5 in. (1.3 cm) high</p>
Weight	<p>AIR-PCM35x: 1.6 oz (45g)</p> <p>AIR-LMC35x: 1.4 oz (40g)</p> <p>AIR-PCI35x: 4.4 oz (125g)</p>



Environmental	<p>AIR-PCM35x and AIR-LMC35x: -22° to 158° F (-30° to 70° C)</p> <p>AIR-PCI35x: 32° to 131° F (0° to 55° C)</p> <p>10 to 90% (non-condensing)</p>
Input Power Requirements	+5 VDC +/- 5%
Typical Power Consumption (at 100 mW transmit power setting)	<p>Transmit: 450 mA</p> <p>Receive: 270 mA</p> <p>Sleep mode: 15 mA</p>
Warranty	Limited lifetime
Wi-Fi Certification	 <p>The image is a Wi-Fi Certified logo. It features the 'Wi-Fi' logo at the top, followed by the word 'CERTIFIED'. Below that, it says 'Certified Interoperability for:'. There are two rows of options: '2.4 GHz Band' with a checked box and '11 Mbps', and '5 GHz Band' with an unchecked box and '54 Mbps'. At the bottom, the website 'www.wi-fi.org' is listed.</p>

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF REFERENCES

- [1] White paper on 802.11: Wireless Networking – A guide to Wireless Networks and 802.1x Technologies and Standards, Accton Engineering, 2003.
- [2] Stagg Newmann, Broadband Access Platform – FCC Tutorial for Communications Networks and Services, McKinsey and Company, April 2002.
- [3] <http://www.scramble.nl/sg.htm> accessed on October 15, 2003.
- [4] <http://www.cisco.com/warp/public/102/wlan/multipath.html> accessed on October 7, 2003.
- [5] <http://www.prostarnotebook.com/faq/TM-0149.htm> accessed on October 7, 2003.
- [6] White paper on Wireless LANs from P&C Communications Limited, 2003.
- [7] <http://buffy.eecs.berkeley.edu/~linnartz/wireless/ofdm/index.html> accessed on October 8, 2003
- [8] <http://www.purchon.com/physics/electromagnetic.htm> accessed on October 14, 2003
- [9] [http://www.lightpointe.com/pdf/wp\\_hybrid\\_fso\\_microwave\\_comm\\_nets.pdf](http://www.lightpointe.com/pdf/wp_hybrid_fso_microwave_comm_nets.pdf) accessed on October 14, 2003
- [10] New Local Business Access Opportunities for AT&T using Free-space optical Technology that Complements Existing Millimeter-Wave Radio Technology, D. M. Britz, AT&T Labs, Research.
- [11] John W. Sprague, Free-Space Optics and Wireless Broadband Radio Frequency Technology: Bringing High Speed Network Access to the last mile, Master's Thesis, Naval Postgraduate School, Monterey, California, March 2002.
- [12] [http://www.geocities.com/CapeCanaveral/3900/rsaf\\_hist.html](http://www.geocities.com/CapeCanaveral/3900/rsaf_hist.html) accessed on October 15, 2003.
- [13] [http://www.f-16.net/reference/users/f16\\_sg.html](http://www.f-16.net/reference/users/f16_sg.html) accessed on October 15, 2003.

- [14] <http://www.stanford.edu/group/networking/NetConsult/wireless/80211a.html>  
accessed on October 7, 2003.
- [15] Stallings William, Wireless Communications and Networks. Prentice Hall, 2002.
- [16] Technical Specifications on Cisco Aironet® 350 Series Client Adapters from  
[http://www.cisco.com/en/US/products/hw/wireless/ps4555/products\\_data\\_sheet09186a0080088828.html](http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_data_sheet09186a0080088828.html), accessed on November 4, 2003.
- [17] Grier, Jim. Minimizing WLAN Security Threats. <http://www.wireless-nets.com/bio.html>, accessed on November 12, 2003.

## INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center  
Ft. Belvoir, Virginia
2. Dudley Knox Library  
Naval Postgraduate School  
Monterey, California
3. Chairman  
Information Sciences Department  
Naval Postgraduate School  
Monterey, California
4. Professor Bert Lundy  
Department of Computer Science  
Naval Postgraduate School  
Monterey, California
5. Professor Donald V. Z. Wadsworth  
Department of Electrical and Computer Engineering  
Naval Postgraduate School  
Monterey, California
6. Major Ow Keong Meng  
Singapore