



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**HIGH THROUGHPUT TACTICAL WIRELESS
NETWORKING FOR SURVEILLANCE AND TARGETING
IN A COALITION ENVIRONMENT:
AN ANALYSIS OF THE NEXT GENERATION IEEE
802.11n EQUIPMENT AND STANDARD**

by

Gary W Thomason

September 2005

Thesis Co-Advisors:

James Ehlert
Brian Steckler

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<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.				
1. AGENCY USE ONLY		2. REPORT DATE September 2005	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE: High Throughput Tactical Wireless Networking for Surveillance and Targeting in a Coalition Environment: An Analysis of the Next Generation IEEE 802.11n Equipment and Standard			5. FUNDING NUMBERS	
6. AUTHOR(S) Thomason, Gary W.				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES 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.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) This thesis presents a technology review of the emerging IEEE 802.11n standard. A wireless local area network (WLAN) based on state-of-the-art equipment supporting the 802.11n protocol is evaluated in the Coalition Operating Area Surveillance and Targeting System (COASTS). This thesis also provides a brief introduction to COASTS, its support for testing various networking schemes, and their effectiveness in supplying information necessary to reach a decision maker's desired end-state. Also provided is a summary of the current state of the 802.11n proposed standard, the hardware and software used to evaluate the equipment, and the testing methodology. In general, the methodology was to conduct field tests with private vendors and coalition partners to evaluate the capabilities of 802.11n networks that promise large throughput benefits for WLANs. The specific goal of this research focused on testing equipment and network configurations in an IP network. The ultimate goal of this research is to evaluate an evolutionary improvement for our forces to transfer large amounts of data and to maintain the mobility and flexibility to deploy rapidly to areas with little or no infrastructure. With this capability our forces may can gain control of the environment, dramatically improve tactical situational awareness, and attain information superiority.				
14. SUBJECT TERMS IEEE 802.11n, COASTS, Wireless Networking, Belkin Pre-N router, MIMO, Multiple Input, Multiple Output, BreadCrumb, WWiSE, TGn, IXIA, IxChariot			15. NUMBER OF PAGES 83	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

**HIGH THROUGHPUT TACTICAL WIRELESS NETWORKING FOR
SURVEILLANCE AND TARGETING IN A COALITION ENVIRONMENT:
AN ANALYSIS OF THE NEXT GENERATION IEEE 802.11n EQUIPMENT AND
STANDARD**

Gary W Thomason
Captain, United States Marine Corps
BSME, University of Florida, 1995

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

**NAVAL POSTGRADUATE SCHOOL
September 2005**

Author: Gary W Thomason

Approved by: James Ehlert
Thesis Co-Advisor

Brian Steckler
Thesis Co-Advisor

Dr. Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis presents a technology review of the emerging IEEE 802.11n standard. A wireless local area network (WLAN) based on state-of-the-art equipment supporting the 802.11n protocol is evaluated in the Coalition Operating Area Surveillance and Targeting System (COASTS).

This thesis also provides a brief introduction to COASTS, its support for testing various networking schemes, and their effectiveness in supplying information necessary to reach a decision maker's desired end-state. Also provided is a summary of the current state of the 802.11n proposed standard, the hardware and software used to evaluate the equipment, and the testing methodology.

In general, the methodology was to conduct field tests with private vendors and coalition partners to evaluate the capabilities of 802.11n networks that promise large throughput benefits for WLANs. The specific goal of this research focused on testing equipment and network configurations in an IP network.

The ultimate goal of this research is to evaluate an evolutionary improvement for our forces to transfer large amounts of data and to maintain the mobility and flexibility to deploy rapidly to areas with little or no infrastructure. With this capability our forces may gain control of the environment, dramatically improve tactical situational awareness, and attain information superiority.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	BACKGROUND	1
B.	COALITION ENVIRONMENT	2
	1. Current Situation	3
	2. System Summary	3
	3. Capabilities	3
	4. COASTS Support for Principal Mission Areas	4
	a. Direct Action (DA)	4
	b. Tactical Reconnaissance (TR).....	4
	c. Foreign Internal Defense (FID).....	4
	d. Combating Terrorism (CBT)	4
	e. Civil Affairs (CA)	5
	f. Counter-proliferation of Weapons of Mass Destruction (WMD).....	5
	g. Information Operations (IO)	5
	5. 802.11 (2.4 GHz) End-user Tactical Network	6
C.	STATEMENT OF PROBLEM.....	6
	1. Measures of Performance (MOP).....	7
	2. Measures of Effectiveness (MOE)	9
D.	ASSUMPTIONS.....	11
E.	METHODOLOGY	11
F.	ORGANIZATION OF THE THESIS	12
II.	TECHNOLOGY	13
A.	INTRODUCTION TO 802.11n.....	13
	1. IEEE Standards Association.....	13
	2. Brief History of 802.11n	13
B.	IEEE 802.11n PROPOSED STANDARDS	14
	1. WWiSE and TGnSync.....	14
	a. Minimum Throughput.....	14
	b. MIMO.....	14
	c. Efficiency.....	15
	d. Channels.....	15
	2. Belkin Pre-N WWiSE Implementation.....	17
III.	HARDWARE AND SOFTWARE.....	19
A.	HARDWARE	19
	1. Belkin Pre-N Router	19
	a. Physical Description, Protocols, and Standards.....	19
	b. Antenna Suite.....	21
	c. Wireless Cards.....	21
	2. Laptop Computers.....	22
	a. Compaq Presario 2700.....	22

	b.	<i>Dell Latitude</i>	22
	c.	<i>Fujitsu Lifebook</i>	22
B.	SOFTWARE.....		23
	1.	Belkin Pre-N Router	23
	a.	<i>Installation</i>	23
	b.	<i>Network Profiles</i>	24
	c.	<i>Wireless Client Utility</i>	24
	d.	<i>Web-Based Advanced User Interface</i>	26
	2.	IXIA IxChariot.....	30
IV.	FIELD ASSESSMENT PROCEDURES AND METHODOLOGY		33
	A.	PURPOSE	33
	B.	METHODOLOGY	33
	C.	FIELD EXPERIMENTS	33
	1.	Network Operating Area.....	34
	2.	Network Configuration	36
	3.	Equipment Configuration	40
	4.	Environmental Conditions	41
	5.	Comparison Network.....	41
V.	RESULTS		45
	A.	RUN OPTIONS	45
	B.	TEST SETUP	45
	1.	Test 1	45
	2.	Test 2	46
	3.	Test 3	46
	4.	Test 4	47
	C.	THROUGHPUT AND RESPONSE TIME RESULTS	47
	D.	RESULTS SUMMARY	53
	E.	FACTORS AFFECTING RESULTS.....	53
	1.	CPU Speed	53
	2.	Ram and Disk Swapping	54
	3.	Endpoint Operating System.....	54
	4.	Virus Scanners	54
	5.	Network Configuration	54
	6.	Network Activity	54
	7.	Screen Savers.....	55
VI.	CONCLUSIONS		57
VII.	RECOMMENDATIONS.....		61
	A.	IEEE 802.11n STANDARD.....	61
	B.	IXCHARIOT NETWORK EVALUATION SUITE.....	61
	LIST OF REFERENCES		63
	INITIAL DISTRIBUTION LIST		67

LIST OF FIGURES

Figure 1.	COASTS Demonstration Configuration	5
Figure 2.	Expanded View of COASTS Demonstration Configuration	6
Figure 3.	802.11 Frequency Spectrum	16
Figure 4.	Belkin Pre-N Wireless Router and Notebook Card	17
Figure 5.	MIMO Antenna Array (After: Legg)	21
Figure 6.	Router Installation Wizard	23
Figure 7.	Pre-N Wireless Client Utility	25
Figure 8.	Web-Based Advanced User Interface	26
Figure 9.	IXIA IxChariot Console – Endpoint Interaction (after IXIA User manual)	31
Figure 10.	IXIA IxChariot Console Results	32
Figure 11.	COASTS March 2005 Demonstration Locations	34
Figure 12.	COASTS May 2005 Demonstration Locations	35
Figure 13.	Aerial View of COASTS 2005 Operating Area	35
Figure 14.	Laptops Used for the 802.11n Experimental Network	38
Figure 15.	Laptops and BreadCrumbs Seen outside the MCP	38
Figure 16.	Basic Pre-N Network Diagram	39
Figure 17.	BreadCrumb Network Diagram for COASTS Demonstrations	39
Figure 18.	Rajant BreadCrumb SE	42
Figure 19.	Basic Rajant BreadCrumb Network Diagram	43
Figure 20.	Rajant BreadCrumb BCAdmin Network	43
Figure 21.	Test 1 Throughput between Pairs	48
Figure 22.	Test 1 Response Time between Pairs	49
Figure 23.	Test 2 Throughput between Pairs	49
Figure 24.	Test 2 Response Time between Pairs	50
Figure 25.	Test 3 Throughput between Pairs	51
Figure 26.	Test 3 Response Time between Pairs	51
Figure 27.	Test 4 Throughput between Pairs	52
Figure 28.	Test 4 Response Time between Pairs	52
Figure 29.	802.11n and 802.11b End-User to HQ Pipes Comparison	58

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	COASTS Network IP Addresses, Subnet Masks, and Gateways	37
Table 2.	Measures of Performance for System Settings	40
Table 3.	Component MAC Addresses	41
Table 4.	Run Options	45
Table 5.	Summary of Throughput and Response Times for Tests 1 through 4.	53

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

There are many individuals that contributed to the successful completion of this thesis. Among them are my thesis co-advisors, Jim Ehlert and Brian Steckler. Without the opportunities they have provided this and much other work would not have been completed. I owe a debt of gratitude to the material enhancements provided by my thesis editor, Ron Russell. His instruction and guidance on the proper use of the English language was invaluable. A general thank you must go to staff and faculty of NPS and my fellow students. They are the enablers of educating a forward thinking military. Thank you all.

And lastly I must thank my lovely wife, Renee, and the demanding affections of our mutual charge, Marysol. Without their support, the hours of research, travel, experimentation, and writing could not possibly have been as entertaining.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

War is both timeless and ever changing. While the basic nature of war is constant, the means and methods we use evolve continuously. Changes may be gradual in some cases and drastic in others.... One major catalyst of change is the advancement of technology. As the hardware of war improves through technological development, so must the tactical, operational, and strategic usage adapt to its improved capabilities both to maximize our own capabilities and to counteract our enemy's.

-MCDP-1 Warfighting

Modern warfare is a fluid environment that increasingly relies on knowledge and information; therefore, a military's ability to acquire knowledge and information is paramount to its success or failure. In fact, nowadays, a force's ability to gather information drives its ability to acquire knowledge. Consequently, gathering information can lead to knowledge, and this knowledge can lead to success.

Modern wired networking systems are capable of transmitting a vast amount of information. Unfortunately, wired networks stifle mobility and decrease flexibility in a fluid environment. As a result, traditional networking methods are sometimes inadequate to meet the challenges. This thesis focuses on our current need for high throughput wireless networking capabilities that are mobile and flexible.

The human mind processes an incredible amount of data, such as video, to synthesize or extract pertinent information (Birdsong and Helms). Unfortunately, the current state of wireless networking cannot transfer data at the processing rate of the human mind. Rather, the current wireless networks actually strain to maintain coherent video – our richest source of information. The wireless networks must be able to transfer more data so we can rapidly distill knowledge from the gathered information. With new knowledge, one can execute more effective decision making at an increased tempo. In effect, a greater ability to transfer data improves combat effectiveness and mission accomplishment if used properly.

To date, the most successful wireless solutions for transferring large amounts of data are based on the IEEE 802.11 standard. The next generation of the 802.11 standard

is referred to as 802.11n. 802.11n promises an immense leap in data transmission capabilities and is the subject of this thesis.

If our forces can transfer large amounts of data and can maintain the mobility and flexibility to deploy rapidly to areas with little or no infrastructure, they can gain control of their environment or at least dramatically improve tactical situational awareness. That issue is directly addressed by the Coalition Operating Area Surveillance and Targeting System (COASTS) project. COASTS offers an environment for testing various networking schemes and their effectiveness in supplying a decision maker with the information necessary to reach a desired end-state.

B. COALITION ENVIRONMENT

The Naval Postgraduate School (NPS) COASTS research program supports the goals relating to theater security, host nation security, and the War On Terror (WOT) of the following entities:

- U.S. Pacific Command (USPACOM)
- Joint U.S. Military Advisor's Group Thailand (JUSMAGTHAI)
- Naval Postgraduate School
- Thailand Royal Thai Supreme Command (RTSC)
- Royal Thai Armed Forces (RTARF)
- Thai Defence Research & Development Office (DRDO) science and technology research requirements

COASTS leverages and integrates the technological expertise of NPS's education and research resources with the science and technology and operational requirements of the RTARF. COASTS uses Wireless Local Area Network (WLAN) technologies to fuse and to display information from air and ground sensors in a real-time, tactical, coalition-enabled command and control center.

The Thailand-based COASTS 2005 demonstration and series of field experiments served as a mobile field test-bed for R&D, integration, operational testing, and field validation of several emerging wireless technologies and equipment suites. The demonstration allowed the Thai military to support ongoing RTARF missions along the 1800 km long Burmese border (Central Intelligence Agency, 2005) or in peacekeeping missions in Southern Thailand.

1. Current Situation

There is a military demand for low-cost, state-of-the-art, real-time threat warning and tactical communication equipment that is rapidly scaleable based on operational considerations. Most current tactical systems cannot rapidly enable a common operating picture among air, surface, and sub-surface entities through a self-forming, self-healing, self-authenticating, autonomous network. Although commercial-off-the-shelf (COTS) technologies exist that can satisfy some of these requirements, they typically do not meet all of the DoD and coalition partner's requirements associated with WOT and other security missions. The primary objective of COASTS is to demonstrate that the NPS and coalition R&D, in concert with current COTS solutions, can satisfy all technical and tactical requirements. (Ehlert, 2004)

2. System Summary

COASTS is an individual and small unit network-capable communication and threat warning system using an open, plug-and-play architecture. It is also user-configurable, employing air balloons, Unmanned Aerial Vehicles (UAVs), and portable and fixed ground-based sensors, i.e. soldiers equipped with TactiComp or similar PDAs, all communicating via wireless networking technologies.

3. Capabilities

COASTS 2005 provided a mobile field test-bed for the U.S. and Thailand. Further it supported R&D, integration, operational testing, and field validation of several emerging wireless technologies and equipment suites as follows:

- 802.11b and 802.11n
- 802.16 Orthogonal Frequency Division Multiplexing
- Satellite Communications (SATCOM)
- Situational Awareness Overlay Software
- Wearable Computing Devices
- Air and Ground Sensors
- Mobile Command and Control Platforms

4. COASTS Support for Principal Mission Areas

COASTS directly supported organizing, training, and equipping of U.S. military forces and the RTARF in seven principal mission areas as defined by Joint Doctrine:

a. *Direct Action (DA)*

The primary function of COASTS during DA missions was to provide Force Protection. DA missions are typically short-duration, offensive, high-tempo operations that require real-time threat information presented with little or no operator interface. COASTS augmented other capabilities in direct support of the DA from an over-watch position. To support DA, COASTS targeted collection to support threat warnings relevant to that specific operation and to provide automated reporting to the Tactical Operations Center (TOC) for potential threats relevant to a specific mission. COASTS, as it evolves (2006 and beyond), may also be used as the primary source of threat information in the absence of other capabilities. Threat information presented by COASTS is intended to be relevant, real-time, or near real-time, and within its area of operation (Joint Pub 6-0, 1995).

b. *Tactical Reconnaissance (TR)*

The primary purpose of a TR mission is to collect information. COASTS augmented other capabilities to obtain or to verify information concerning the capabilities, intentions, locations, and activities of an actual or potential enemy. COASTS 2005 also supported the full range of information and communication functions. The test-bed allowed operators to collect, process, analyze, and disseminate information rapidly. In this mission, COASTS' performance was affected by meteorological, hydrographic, or geographic considerations. In these scenarios, COASTS primarily supported Force Protection (Joint Pub 3-55, 1993).

c. *Foreign Internal Defense (FID)*

COASTS assisted Host Nation (HN) military and paramilitary to maintain the HN's internal stability (Joint Pub 3-07.1, 2004)

d. *Combating Terrorism (CBT)*

COASTS supported CBT activities to include anti-terrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism) (Joint Pub 3-07.2, 1998).

e. Civil Affairs (CA)

COASTS assisted CA peacetime activities to prevent grievances from flaring into war, and during hostilities, to help ensure that civilians do not interfere with operations, and that they are protected and sheltered in combat zones (Joint Pub 3-57, 2005).

f. Counter-proliferation of Weapons of Mass Destruction (WMD)

COASTS 2005 assisted traditional capabilities to seize, destroy, render safe, capture, or recover WMD. COASTS can provide information to assist U.S. Military Forces and coalition partners to counter threats posed by WMD and their delivery systems (Joint Pub 3-40, 2004).

g. Information Operations (IO)

COASTS 2005 assisted in disrupting adversary information and information systems while defending one's own information and information systems. IO applies across all phases of an operation and the spectrum of military operations (Joint Pub 3-13, 2005).

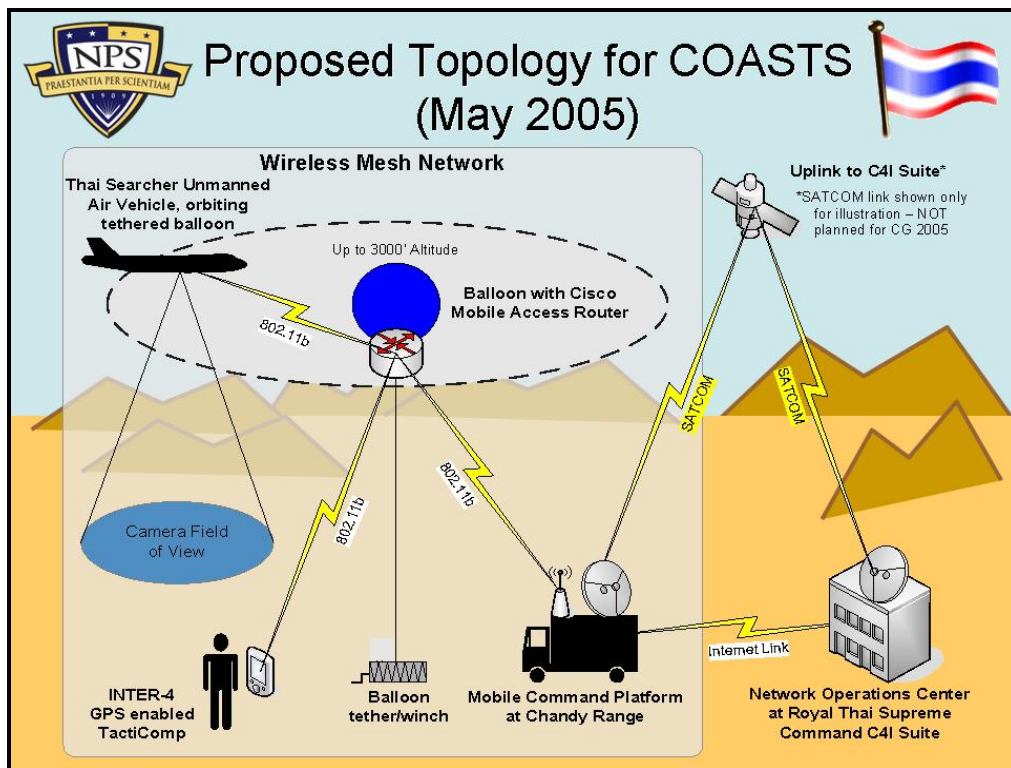


Figure 1. COASTS Demonstration Configuration

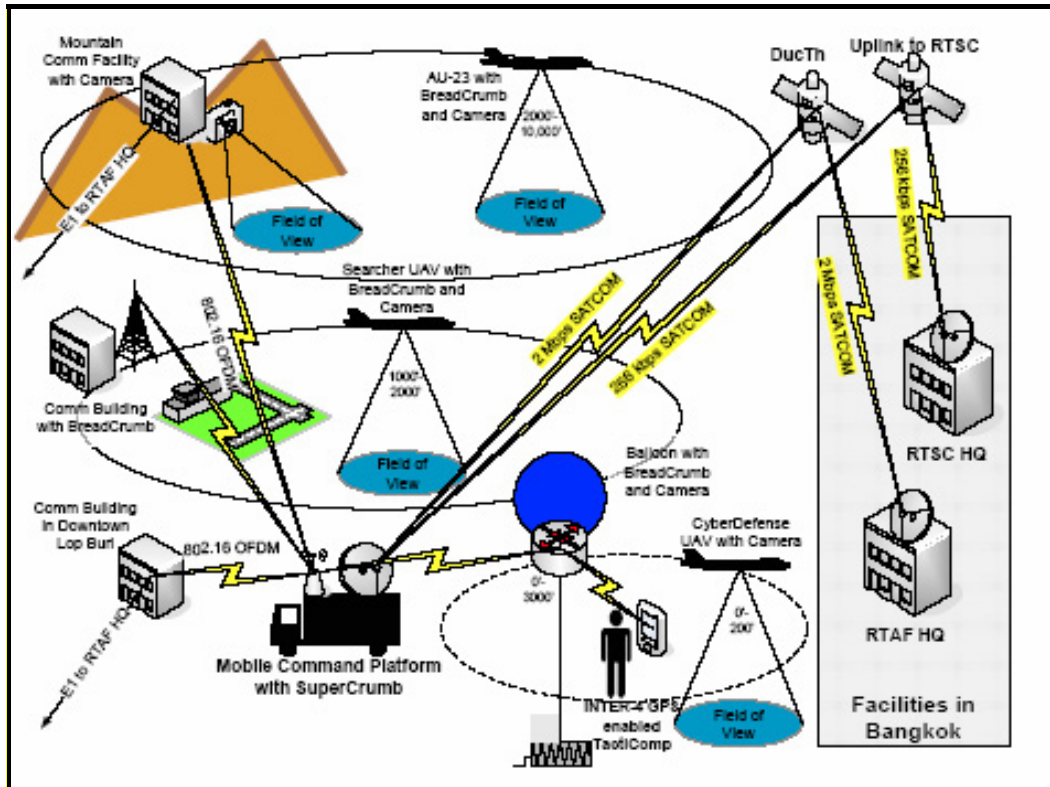


Figure 2. Expanded View of COASTS Demonstration Configuration

5. 802.11 (2.4 GHz) End-user Tactical Network

This local area network consisted of an 802.11 footprint established via a Rajant Technologies 802.11b BreadCrumb XL located on a balloon and several access points on the ground for redundancy. This network connected the situational agent end nodes to a local Mobile Command Platform (Royal Thai Army supplied a 10-ton truck equipped with a variety of communication equipment), which was co-located with air assets at Lob Buri Range. Experimentation was conducted to discover the 802.11 network fielded capabilities compared to a similar network equipped with Belkin pre-802.11n equipment.

C. STATEMENT OF PROBLEM

Would an end-user network based on commercial-off-the-shelf (COTS) equipment using the 802.11n standard allow an inexperienced user to create a tactical network effectively? Further, would the 802.11n network substitute for the current 802.11b based solution in the COASTS network?

1. Measures of Performance (MOP)

The measures of performance (MOP) are quantitative values about a desired system. The following MOPs are researched in order to answer the principle research questions. MOP 1 is addressed in Chapters II and III. MOP 2, MOP 3, and MOP 4 are detailed in Chapter IV. MOP 5 and 6 are referenced in Chapter VI.

MOP 1.0 What were the specifications of the system?

MOP 1.1 Frequency spectrum?

MOP 1.2 Compatibility with previous standards?

MOP 1.3 Coverage area?

MOP 1.4 Status of specification adoption?

MOP 2.0 What were the system settings?

MOP 2.1 AP Mode?

MOP 2.2 MAC addresses?

MOP 2.3 IP Addressing?

MOP 2.3.1 IP pool?

MOP 2.3.2 Lease time?

MOP 2.3.3 Subnet masking?

MOP 2.4 DHCP server?

MOP 2.5 SSID?

MOP 2.6 Wireless Mode?

MOP 2.7 QoS (802.11e) Mode?

MOP 2.8 Protected mode?

MOP 2.9 Wireless channels?

MOP 2.10 ACK mode –

MOP 2.11 Security settings?

MOP 2.11.1 WEP/WAP?

MOP 2.11.2 Key

MOP 2.11.3 Firewall settings?

MOP 3.0 What were the testing environmental conditions?

MOP 3.1 Overall area description?

MOP 3.1.1 Terrain?

MOP 3.1.2 Local vegetation?

MOP 3.2 Weather

MOP 3.2.1 Temperature?

MOP 3.2.2 Humidity?

MOP 3.2.3 Cloud cover?

MOP 3.2.4 Winds?

MOP 3.3 Time of day for testing?

MOP 4.0 What was the common load used for testing?

MOP 5.0 What was the throughput of TCP traffic when tested under a common load?

MOP 5.1 Between two endpoints?

MOP 5.1.1 Average?

MOP 5.1.2 Minimum?

MOP 5.1.3 Maximum?

MOP 5.2 Between two sets of endpoints?

MOP 5.2.1 Average?

MOP 5.2.2 Minimum?

MOP 5.2.3 Maximum?

MOP 6.0 What was the system response time of TCP traffic when tested under a common load?

MOP 6.1 What was the response time between two endpoints?

MOP 6.1.1 Average?

MOP 6.1.2 Minimum?

MOP 6.1.3 Maximum?

MOP 6.2 What was the response time between two sets of endpoints?

MOP 6.2.1 Average?

MOP 6.2.2 Minimum?

MOP 6.2.3 Maximum?

2. Measures of Effectiveness (MOE)

The measures of effectiveness (MOE) are qualitative in nature, describing the end-user's expectations of the system. The following MOEs are researched in order to answer the principle research questions and are referenced in Chapter VI.

MOE 1.0 Did the system transmit data over the network?

MOE 1.1 Did the system transmit data over the Local Area Network (LAN)?

MOE 1.1.1 Did the system transmit text data over the LAN?

MOE 1.1.2 Did the system transmit audio data over the LAN?

MOE 1.1.3 Did the system transmit video data over the LAN?

MOE 1.2 Did the system transmit data over the Wide Area Network (WAN)?

MOE 1.2.1 Did the system transmit text data over the WAN?

MOE 1.2.2 Did the system transmit audio data over the WAN?

MOE 1.2.3 Did the system transmit video data over the WAN?

- MOE 2.0 Did the system function in the desired environment?
 - MOE 2.1 Was the system a fixed or portable solution?
 - MOE 2.2 Did the system need an established infrastructure or can it operate with no previously existing infrastructure?
 - MOE 2.3 Did the system operate in
 - MOE 2.3.1 Urban areas?
 - MOE 2.3.2 Jungle areas?
 - MOE 2.3.3 Plains areas?
 - MOE 2.3.4 Arid environments?
 - MOE 2.3.5 Humid environments?
- MOE 3.0 Was the system user friendly?
 - MOE 3.1 Was the system easy to deploy
 - MOE 3.1.1 Did the deploying unit need special technical knowledge to deploy the system?
 - MOE 3.1.2 Did the deploying unit need special technical knowledge to trouble shoot the system?
 - MOE 3.1.3 Did the deploying unit need special technical knowledge to repair the system?
 - MOE 3.2 What was the experience level needed for the user to operate the system effectively?
 - MOE 3.2.1 Novice?
 - MOE 3.2.2 Intermediate?
 - MOE 3.2.3 Power?
 - MOE 3.2.4 Expert?
 - MOE 3.3 Was the system intuitive to operate?

D. ASSUMPTIONS

There are many assumptions that must be made in order to test any equipment. Below is a list of the assumptions made for this thesis.

- All information is unclassified to allow collaboration with coalition partners.
- End-user networks will continue to be serviced by the 802.11 standard and not be subsumed by the 802.16 standard in the near future.
- Equipment tested is a close approximation of the final 802.11n standard. See Chapter II technologies.
- The form factor of the current pre-802.11n equipment can be engineered into the current BreadCrumb form factor.
- Continued interest from private vendors will result in reengineering of the tested pre-802.11n (or like) equipment and facilitate continued support for the COASTS program (COTS).
- The private LAN, which the equipment is tested on, is nearly identical to a future deployed operational environment.
- Network load will follow the pattern of high use for short periods of time or times of interest (TOI) and low use for long periods of time.
- Various operating systems and software packages will be expected to function across the LAN, so interoperability is an important aspect of the functionality.
- The typical end-user of the network has little knowledge of the specific equipment.
- The network must simplify the ease of setup and maintenance by the end-user.
- Robustness of future equipment is outside the scope of this thesis.

These assumptions helped the author conduct the following methodical and consistent study of the equipment in the prescribed COASTS environment.

E. METHODOLOGY

Throughout research, the focus involved testing equipment and network configuration in an IP network and integrating this into the coalition environment. A literature search for IEEE 802.11n information concluded that at the time research began two proposals were considered for the overall standard. The only available equipment that conformed to one of these proposed standards was acquired for testing. The testing was conducted during two on-site demonstrations of COASTS at Royal Thai Air Force

Wing 2 in Lop Buri, Thailand. Data was captured during periods scheduled specifically for experimentation and at other times as available. Further analysis and consideration was conducted during COASTS planning discussions for future operations in 2006.

F. ORGANIZATION OF THE THESIS

This thesis is organized into seven chapters and a supporting references section.

Chapter II provides an overview of the technologies involved in the thesis. The Belkin and Airgo Pre-n protocol are introduced. A discussion of the IEEE 802.11n protocol, which is currently in committee, follows.

Chapter III details the hardware and software equipment used to conduct the testing for this thesis. This discussion includes information on the antenna suites, wireless cards, access points, laptop computers, and the software suites used. Chapter III also concerns the basic installation of the various hardware and software suites and an overview of the application of those technologies.

Chapter IV details the methodologies used to conduct the observations. This chapter also describes how each component in Chapter III was used in testing and includes the specific architecture of the testing environment.

Chapter V provides the empirical results of the data gathered during testing. And, this chapter provides discussion on various MOPs.

Chapter VI analyzes the results with regard to the MOEs and MOPs to address the capabilities and limitations of the equipment. Conclusions about the principle research questions are made.

Chapter VII recommends future implementation and experimentation in the COASTS environment as it pertains to high throughput tactical wireless networking and the IEEE 802.11n standard.

II. TECHNOLOGY

In this chapter, the Measures of Performance (MOP 1.0) regarding system specifications are addressed. The frequency spectrum of the system (MOP 1.1), compatibility with previous standards (MOP 1.2), coverage areas (MOP 1.3), and the status of the draft 802.11n proposals for adoption (MOP 1.4) are covered.

A. INTRODUCTION TO 802.11n

1. IEEE Standards Association

The Institute of Electrical and Electronics Engineers Standards Association (IEEE) is the leading developer of standards for the information technology industry. IEEE produces the familiar 802 standards for wired and wireless Local and Metropolitan Area Networks (LAN/MAN). In an open balloting process IEEE members, composed of industry and academic leaders in technology, vote on proposals submitted from various organizations. The standards are selected based on technical reliability and soundness (IEEE Standards Association, 2005).

2. Brief History of 802.11n

For the 802.11n standard, over 60 organizations submitted proposals in August of 2004. In January of 2005 at the IEEE meeting in Monterey, CA, the selection was pared down to three complete proposals. By March 2005 only two remained. These two were the leading competitors throughout the process. They are WWiSE and TGnSync. The WWiSE consortium stands for WorldWide Spectrum Efficiency and includes Texas Instruments, Broadcom, Airgo, STMicroelectronics and Conexant. The TGnSync, which stands for Task Group n Synchronization, includes Intel, Sony, Philips, Agere and Atheros.

During the March meeting a down select vote was conducted, which reduced the field to a single candidate, TGnSync at 51%. WWiSE was removed from consideration with 49% of the vote. A confirmation vote was next. The confirmation vote according to the IEEE process requires 75% membership approval. Voters who oppose the proposal provide comments that the competitor addresses at the next meeting for a second confirmation attempt.

The next meeting was held in May of 2005. After the voter comments were addressed, a second confirmation vote was taken, but it failed to achieve a 75% approval. As dictated by the selection process, the previous three proposals from the January meeting were reinstated. In July, updated technical proposals and mergers will be resubmitted and voted upon again (MOP 1.4) (802.11n Work Group, 2005).

B. IEEE 802.11n PROPOSED STANDARDS

1. WWiSE and TGnSync

The two major competitors for the 802.11n standard are WWiSE and TGnSync. These proposals are quite similar on three major aspects, which encompass the heart of high throughput wireless networking. They are minimum throughput, use of Multiple Input / Multiple Output (MIMO), and increased efficiency (Deffree, 2004). The significant differences between the two proposals are the use of channels and the means of achieving higher efficiency (Gast, 2004).

a. Minimum Throughput

The IEEE Task Group N has changed its request for proposals in a significant way. Previous standards have used the theoretical maximum throughput as the measure of performance for the proposed standard. The 802.11n standard instead requires the user to experience a *minimum* throughput for the baseline measure of performance.

This means that the 802.11n standard will not be like previous 802.11 standards. For the 802.11b/g standards 11 Mbps and 54 Mbps are the advertised peak throughput while the user typically experiences approximately 4 to 5 Mbps and 20 to 23 Mbps, respectively, under ideal conditions (Rubin, 2003). The 802.11n standard requires a minimum throughput of 100 Mbps after subtracting all the overhead for protocol management such as preambles, interframe spacing, and acknowledgements.

b. MIMO

Multiple Input / Multiple Output or MIMO (pronounced My-Moe) is an antenna technology that uses an array of antennas for transmitting and receiving. Each complete 802.11n proposal uses a variation of the 2x2 MIMO setup. This setup indicates that two antennas are used for transmitting and two are used for receiving.

Complex algorithms are used to schedule and to interpret transmitted signals so that a high-rate data stream can be separated into multiple low-rate streams and transmitted from different antennas on the same channel. Through antenna diversity, receiver sensitivity is increased due to multiple receiving antennas where one antenna may receive a better or more complete signal than another. Again, complex algorithms allow the mixing of received signals for overall higher fidelity reception. Further, these algorithms allow effective and beneficial use of multi-path propagation, such as signals bouncing off walls, windows and other obstacles, which varies the arrival time of the signal and which is typically detrimental to wireless LANs (Coffey and others, 2004).

c. Efficiency

Primarily, the proposals increase the efficiency of the allocated spectrum by altering the protocol to minimize overhead. Increasing frame size and block acknowledgements are two of the alterations. By increasing the frame size, the ratio of data bits to overhead bits is increased (more data is sent per overhead bit). Then by allowing an acknowledgement message only for a group or block of received messages, more data messages are transferred compared to overhead messages. This also increases the number of data bits sent per overhead bit.

There are differences, however, in the implementation of frame size, block acknowledgement, and modulation that directly relate to the use of channels, as the following will clarify.

d. Channels

A major difference between the two leading proposals is the use of different channels. Although both proposals indicate compatibility with either a 20 MHz or 40 MHz channel, the TGnSync proposal focuses on 40 MHz channels in the frequency spectrum of 802.11a around 5 GHz. Contrarily, the WWiSE proposal focuses on 20 MHz channels in the 2.4 GHz range used by legacy 802.11b/g devices, as shown in Figure 3 (MOP 1.1).

With 20 MHz channels, the WWiSE proposal uses a peak rate of 135 Mbps and a code rate of 5/6 to achieve the 100 Mbps goal. The TGnSync uses a peak rate of 140 Mbps and a code rate of 7/8 to achieve the same goal. Both can be directly compared at 108 Mbps. This comparison shows a code rate for WWiSE at 2/3 and

TGnSync at 3/4. This supports the argument that WWiSE is more spectrally efficient. The WWiSE proposal can claim further efficiency by the way it uses the channels. Unlike previous schemes that divide the channel into 54 subcarriers and use 48 for data and four as “pilot” (synchronization) carriers, the WWiSE proposal uses 56 subcarriers, 54 for data and two as “pilot” subcarriers. Here each pilot subcarrier transmits across each of the two antennas acting effectively as four pilot subcarriers. Better code rate modulation allows the channels to be used differently and more efficiently.

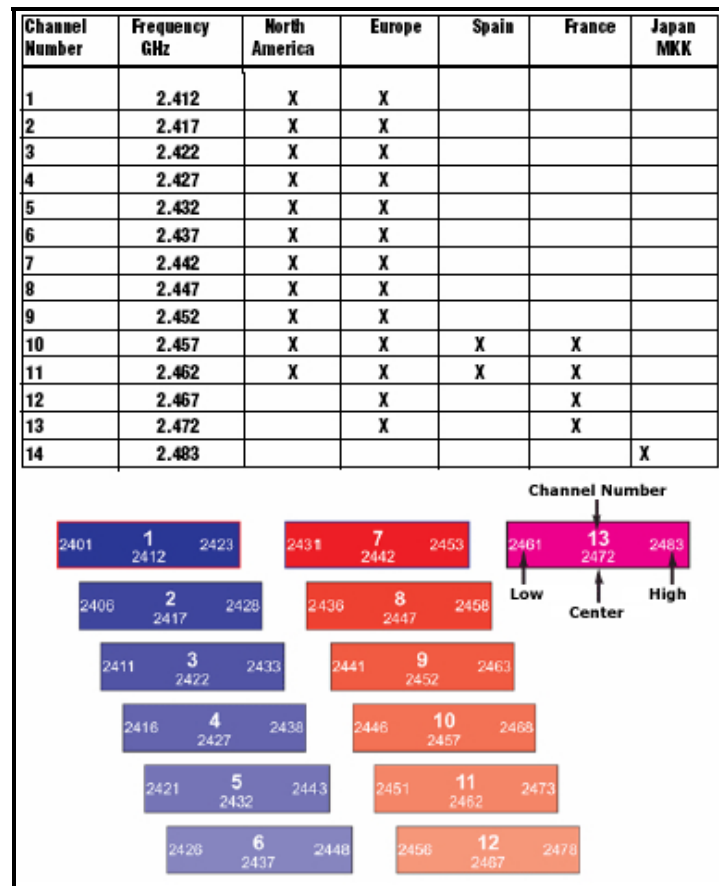


Figure 3. 802.11 Frequency Spectrum

However, the TGnSync proposal has more bandwidth available in the 40 MHz channels. As a result, TGnSync claims that its proposal allows for a much greater increase over the required minimum of 100 Mbps. With the increase from 20 MHz to 40 MHz channels, the TGnSync proposal’s theoretical throughput increases from 140 Mbps

to 315 Mbps. Here the slight difference in code modulation would not seem to make much difference compared to the large increase in theoretical throughput (Mutjaba and others, 2004).

2. Belkin Pre-N WWiSE Implementation

Due to its 20 MHz channels, the WWiSE proposal has significant backward compatibility with current 802.11b/g products on the market (MOP 1.2). Likely to capitalize on the “first-to-market” effect, Belkin offers a wireless router based on the WWiSE proposed standard in a modified form. The Belkin Pre-N router is compatible with all IEEE 802.11b/g equipment. When used with the Belkin Pre-N wireless notebook cards, the Belkin Pre-N Router promises to deliver the higher throughput of the, as yet unconfirmed, 802.11n standard.

The Belkin Pre-N router, shown in Figure 4, employs MIMO technology using three spatially separated dipole antennas. The three antennas provide two simultaneous data streams at a theoretical maximum of 108 Mbps. In addition to the integrated Pre-N wireless access point, other features commonly included in the typical off-the-shelf router are an integrated 10/100 four-port switch, Network Address Translation (NAT), a Stateful Packet Inspection (SPI) firewall, Web-based user interface, built-in Dynamic Host Control Protocol (DHCP), Virtual Private Network (VPN) pass-through, and Medium Access Control (MAC) address filtering.



Figure 4. Belkin Pre-N Wireless Router and Notebook Card

THIS PAGE INTENTIONALLY LEFT BLANK

III. HARDWARE AND SOFTWARE

A. HARDWARE

1. Belkin Pre-N Router

a. Physical Description, Protocols, and Standards

The Belkin Pre-N Router is a consumer-off-the-shelf product. It is packaged with a quick installation guide, installation software, an Ethernet cable, a power supply, and a user's manual. The form factor is similar to other home networking routers. As such, it measures 7" x 6¾" x 1½" with the antennas folded and 7" x 6¾" x 5" with the antennas extended. The router weighs 2.6 lbs. The power supply requires 100-110Vac / 0.4A, 50-60Hz input and outputs 12Vdc / 1A to the router.

The five Ethernet ports on the rear panel support one wide area network (WAN) connection for a cable or DSL modem and four local area connections (LANs) for local clients. All the ports support IEEE 802.3, 802.3u, and 10/100Base-Tx wired networking standards. Other supported protocols include TCP/IP, UDP, Collision Sensing Multiple Access with Collision Detection (CSMA/CD), Dynamic Host Control Protocol (DHCP), AppleTalk, IPX/SPX, and NetBEUI. The LEDs along the top of the router provide indications for power, wireless activity, WAN connection status, LAN connection status (x4), and link speed.

Internet protocol (IP) sharing and firewalling are accomplished via network address translation (NAT). A stateful packet inspection further enhances the firewall capability. Up to 253 total clients, of which up to 25 may be wireless clients, are supported by the DHCP server.

The supported Internet service provider protocols include static and dynamic IP addressing, Point-to-Point Protocol over Ethernet (PPPoE), and Point-to-Point Tunneling Protocol (PPTP). PPTP is further used in conjunction with IPsec Pass-Through for VPNs.

The Belkin Pre-N router is backward compatible with two established IEEE wireless standards (802.11b and 802.11g). They are 802.11b and 802.11g. The Belkin Pre-N router supports the following direct sequence spread spectrum (DSSS) modulation types

for 802.11b: Complimentary Code Keying (CCK), Differential Quadrature Phase-Shift Keying (DQPSK), and Differential Binary Phase-Shift Keying (DBPSK) to achieve 11, 5.5, 2, and 1 Mbps data rates. The following Orthogonal Frequency Division Multiplexing (OFDM) modulation types are supported for 802.11g: True MIMO, Quadrature Amplitude Modulation (64-QAM and 16-QAM), Amplitude and Phase-Shift Keying (APSK), and Binary Phase Shift Keying (BPSK), to achieve 54, 48, 36, 24, 18, 12, 9, and 6 Mbps data rates. When using True MIMO, supported data rates are 108, 96, and 72 Mbps.

The various data rates are wirelessly transmitted across the ISM frequency band of 2400 to 2483.5 MHz using Collision Sensing Multiple Access with Collision Avoidance (CSMA/CA) and acknowledgement media access protocols. Although only the frequency band from 2400 to 2473 MHz, representing channels 1 through 11, are used in the United States.

Supported encryption and security protocols include 64 or 128-bit Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) with Temporal Key Integrity Protocol (TKIP) or with Advanced Encryption Standard (AES). (Belkin, 2004)

The Enhanced Distributed Coordination Function (EDCF) with Wi-Fi Multimedia Enhancements and the Hybrid Coordination Function (HCF) with Wi-Fi Scheduled Multimedia of the draft IEEE 802.11e protocol provide Quality of Service (QoS) for demanding applications such as Voice over IP and streaming media for the Belkin Pre-N router. EDCF is a “best effort” attempt to send higher priority traffic before lower priority traffic. HCF helps to define priority traffic and to administer resources. HCF is supported in hardware while EDCF is software supported. These two components are the minimum required to be compliant with the draft 802.11e standard (WikiMedia, 2005).

The published operating temperature for the Belkin Pre-N router ranges from 32 to 131 degrees Fahrenheit at a maximum of 95% humidity while the storage temperature ranges from -13 to 155 degrees Fahrenheit again at a maximum of 95% humidity.

b. Antenna Suite

The Belkin Pre-N router uses Airgo's True MIMO capability to increase performance. The three 3½ " dipole antennas are mounted to the top of the unit and are not removable but do hinge and rotate at the base. When transmitting at low data rates, the output power is +20dBm (100mW). At high data rates, the output power is +17dBm (50mW).

The three antennas create an array, which dynamically boosts gain in the direction of the desired signals. In addition, this allows the antenna array to decrease gain toward the sources of interference. Figure 5 shows coverage areas that have dynamically changed to allow a larger coverage area for the desired signal and a limited coverage area for interference (MOP 1.3).

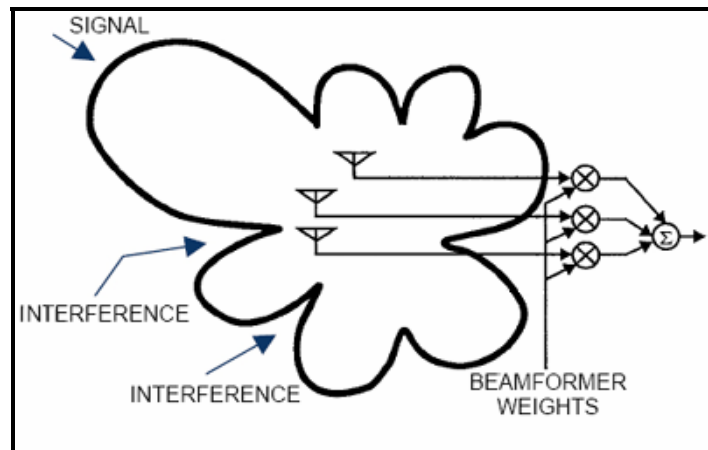


Figure 5. MIMO Antenna Array (After: Legg)

The ability to alter the coverage area dynamically differs from most current antenna implementations. The typical antenna configurations use dual diversity antennas that simply get switched on and off according to which one has the stronger signal (Legg, 2005).

c. Wireless Cards

To gain the maximum benefit of the True MIMO capability the Belkin Pre-N router must be matched with a wireless card with similar capabilities. The Belkin Pre-N wireless cards adhere to all the same standards and protocols that equip the router.

The Belkin Pre-N wireless cards use the standard 32-bit pc card form factor. They have two LEDs for activity and link status.

Using the Belkin Pre-N wireless cards to establish network connectivity is not strictly necessary. Most 802.11b or 802.11g wireless cards will suffice. However, throughput will be limited to the speed of the wireless card thereby negating the faster capabilities of 802.11n implementing True MIMO.

If the case arises that a mixed-mode network is established, for example when a Belkin Pre-N wireless card and an 802.11b wireless card are connected to the same Belkin Pre-N router, the Pre-N connection will continue to operate at its highest capacity throughput. This is unlike current mixed-mode operations in which the entire wireless network is limited by the speed of its slowest standard.

2. Laptop Computers

Three laptop computers were used during experimentation. These laptops were used to configure and to test the network established by the Belkin Pre-N router, as detailed in later sections. The laptops were selected based upon their diversity and use in the established COASTS network. Not only are they representative of the computers used in the comparison network, they are the same computers that operated on the comparison network during operational exercises. The Belkin Pre-N wireless cards furnished laptop connectivity for all network connection on all computers.

a. Compaq Presario 2700

The Compaq Presario was the primary computer running the Windows XP Professional version 2002 with Service Pack 1 Operating System. It has a 1.13 GHz Intel Pentium III processor with 512 MB of RAM.

b. Dell Latitude

The Dell Latitude was set up as a client computer with the Windows XP Home Edition version 2002 and Service Pack 2 Operating System. It has a 1.6 GHz Intel Pentium 4 processor with 256 MB of RAM.

c. Fujitsu Lifebook

The Fujitsu Lifebook was designated as a client computer. It is equipped with the Windows XP Professional version 2002 with Service Pack 1 Operating System. It has a 900 MHz Intel Pentium M processor with 504 MB of RAM.

B. SOFTWARE

1. Belkin Pre-N Router

The Belkin Pre-N router is compatible with Windows 98SE, Me, 2000, XP, Mac OS 9.x, and Mac OS X. The wireless pc cards are compatible with Windows 2000 and XP. The router's user interface is accessed via a web browser using HTTP after installation.

a. Installation

Before establishing a network based on the pre-802.11n standard, installing the router in order to interface with the host computer's network interface card (NIC) is an important first step. Only then is it advisable to install the drivers for the wireless networking cards, followed by the cards themselves, and then the wireless client monitoring software.

Installing the Belkin Pre-N router is straightforward with the included installation software. After inserting the autorun CD into the CD-ROM drive, one merely follows the onscreen dialogs and prompts, as shown in Figure 6. The screens lead the user through the entire router setup process.

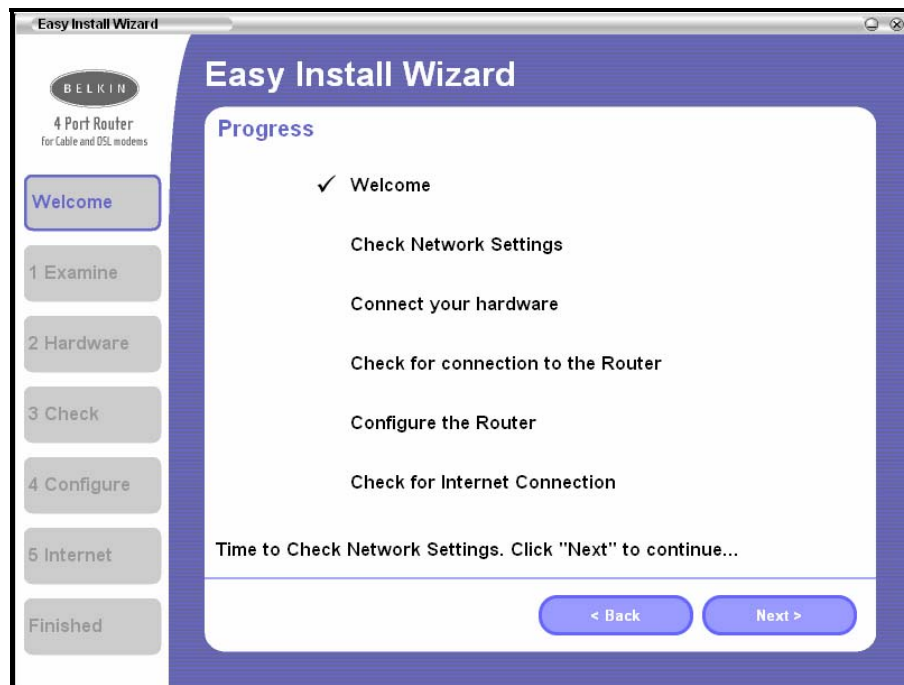


Figure 6. Router Installation Wizard

The network settings are first checked to discover which network adapter to use. If only one NIC is present, then the default selection is used. The user may specify which adapter to use if more than one NIC is present. Then the router must be physically connected via an Ethernet cable to the host computer and powered up. Once the connections are automatically checked, the user may configure the router settings to include wireless modes and channel selection. After that, a connection to the Internet is checked. The router is now connected and the solid green connected LED displays on the router face.

Using the automatic connection wizard is not strictly necessary. One can physically connect and power up the router and then navigate to the Local Area Connection Properties window in Windows XP. Then one clicks on “Internet Protocol (TCP/IP)” and the “Properties” button. Here the simplest solution is to use DHCP by obtaining an IP address and the domain name server address automatically. Otherwise, static IP addressing must be used and the appropriate address must be entered.

Whether one uses the automatic or manual setup options, the selections made create a default profile for the router.

b. Network Profiles

The router runs on an embedded Linux operating kernel specifically designed for the router. All the system settings of the router create a network profile and are saved to a network configuration file within the router. Many distinct network profiles may be saved, but only one may be in use at any time. This allows great flexibility for creating and quickly implementing profiles, as we will see later in Chapter IV.

c. Wireless Client Utility

The client utility is the software program used to retrieve basic network connection information and select which network to connect to from a list of available networks. The client utility provides the current profile in use, the connection quality, the network name, and the type of network in the minimized mode.

When expanded, the wireless client utility also generates a network list, which is used to connect to different networks. The network list provides summary

information on the service set identifier (SSID), signal quality, type of encryption (none, 64- or 128-WEP, or WPA), and network type (ad-hoc or infrastructure). The network list also includes the ability to scan the 802.11 radio bands for newly available wireless networks. The wireless client utility also includes the capability to create, save, edit and delete network profiles from the client list. This should not be confused with altering a network profile or connection profile on the router. These functions are separate. The client profile only affects how the client attempts to connect to the access point or router. The router profile dictates what type of connection will be allowed access.

Further information provided by the client utility, shown in Figure 7, includes the theoretical transmit data rate, the theoretical receive data rate, the actual bytes transmitted and received, the radio band, and the specific channel setting. The security information includes the type of authentication and encryption. Also, the power setting is shown to indicate power consumption on laptop computers.

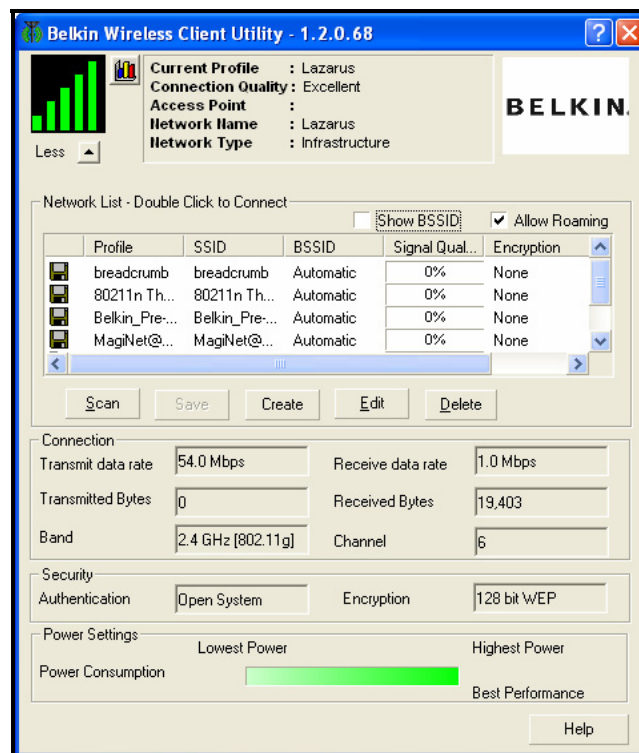


Figure 7. Pre-N Wireless Client Utility

d. *Web-Based Advanced User Interface*

The advanced router controls are accessed through the router's internal web page, shown in Figure 8. The default address is 192.168.2.1 and may be changed at the convenience of the user. From here the user has access to all the options allowed on the Belkin Pre-N router. The controls fall into five general control groups: LAN settings, Internet WAN, Wireless, Firewall, and Utilities.

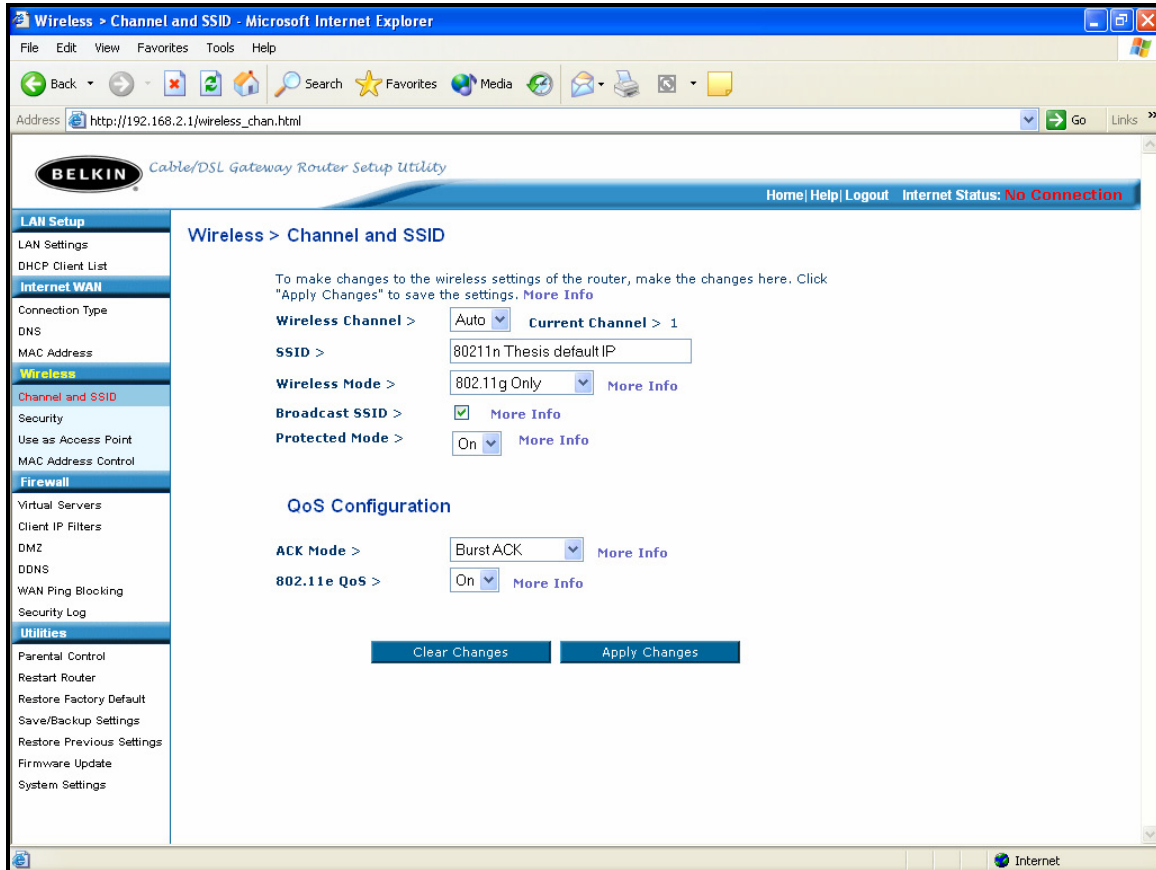


Figure 8. Web-Based Advanced User Interface

The LAN settings affect the operation of the DHCP server and include setting the IP address pool, IP address lease times, subnet masking, and setting a local domain name. Further, setting the internal IP address of the router to a non-routable (or private) IP address is accomplished through the LAN settings. The internal IP address may take the form of 192.168.x.x or 10.x.x.x where x is anything between 0 and 255. From the DHCP client list, a user can see IP addresses, host names, and the MAC

addresses of all the connected computers assigned IP addresses by the DHCP server. This list may show up to 100 IP addresses at a time.

The Internet WAN settings allow the user to specify the Internet connection type and the desired domain name server, and to retrieve or to clone the MAC address of the host computer. These features are primarily important when sharing a connection to the Internet.

The wireless settings allow one to select the transmit channel, SSID, the encryption security, access point mode, and MAC address controls. The SSID is used to identify the wireless network. By default, the SSID is “Belkin Pre-N_” followed by a six-digit number. The SSID may be changed to anything a user would like. Any of the eleven wireless channels may be specified, or the “Auto” select mode can be used. The “Auto” select mode will select the clearest channel on which to transmit when the router boots.

The wireless control group also allows one to select the wireless mode. There are three different modes: “802.11g-only,” “802.11g and 802.11b,” and “off.” In “g-only” mode all devices other than 802.11g and Pre-N compliant devices are not allowed to connect to the network. In “g and b” mode all Pre-N, 802.11g and 802.11b devices may connect to the network. In “off” mode, no devices may join the network. The “off” mode may be used as a security mechanism to turn the network off without unplugging the router, or if a user just wants the wireless features turned off to work solely in wired mode.

The wireless settings allow the SSID broadcast to be turned on and off via a check box. By turning off the broadcast of the SSID, the network name will remain hidden from computers scanning for networks. The option to operate in protected mode also resides here. In protected mode, 802.11g communications are protected from mixed mode operation with 802.11b. The Pre-N communications are not affected by mixed mode operations.

The quality of service mode may be turned on or off and the acknowledgement mode may be toggled between “burst” and “immediate.” These

settings comply with the previously discussed 802.11e standard and also enhance streaming multimedia or VoIP connections.

The security settings accessible through the wireless group allow one to select the security mode, encryption technique, and the pre-shared key. In order for a particular security mode and encryption to be used, the client must have the appropriate support software. The security mode may be disabled, and set to WPA-PSK, 64-WEP or 128-WEP. For all but disabled mode, a pass phrase must be entered (it is called Pre-Shared Key in the case of PSK) on the router and matched on the client in order to allow a connection. The two encryption techniques available are Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

In the wireless settings, the router may be set to access point mode. In access point mode, the DHCP server and the NAT IP sharing are disabled. This is useful if one is working in a static IP address environment, such as COASTS. The IP address of the router must be set to the same subnet mask as the bridged network. Once the access point mode has been enabled, the user does not have access to the Internet WAN and Firewall controls, as these functions no longer apply, until the user disables the access point mode.

The final control in the wireless group is the MAC address control. The MAC address control allows the user to set up ‘allow and deny’ lists. These settings will admit or restrict access to the wireless network based upon the client computer’s twelve character hexadecimal medium access control number, which is unique for every network enabled device. So any client requesting wireless access that is not on the allow MAC list will not be allowed access. Likewise, any client requesting wireless access that is on the deny MAC list will be denied access.

The firewall controls group offers many security feature controls that include virtual server addressing, client IP filters, the creation of a DMZ, ping blocking, and the security log. The router is preconfigured to protect its hosted network from the following attacks:

- IP Spoofing
- Land Attack Ping of Death (PoD)

- Denial of Service (DoS)
- IP with Zero Length
- Smurf Attack
- TCP Null Scan
- SYN Flood
- UDP Flood
- Tear Drop Attack
- ICMP Defect
- RIP Defect
- Fragment Flood

Protection against these attacks is accomplished by masking the common ports that are used for the attacks. When masked, these ports are considered “stealth” ports.

In the firewall control group the firewall may be turned on or off. If turned off, then all stealth ports become open ports and the only protection from attack is based on the routers network address translation, which can be defeated.

The virtual server tab provides controls for application and port forwarding. This enables routing of external traffic through the router to the internal network. Client IP filters are also available. The client IP filter restricts a connected client’s (or group of client’s) access to a port (or range of ports) such as port 80 for Internet, or port 21 for FTP server traffic. Client IP filters may be based on traffic type (TCP, UDP, or both), day of week, and time of day. This may be useful if a specific computer is used for a particular task only at specific times.

If a computer needs to have unfettered access to an outside network, it can be placed in the DMZ. A computer placed in the DMZ does not have the protections of the internal network, but some applications will not run properly when behind the router’s firewall.

The dynamic DNS controls allow compatibility with services such as DynDNS.org. DynDNS.org allows dynamic addresses, like those offered by cable internet companies to mask as a static host name within the DynDNS.org domain space.

WAN ping blocking may be turned on or off from the firewall controls group. Many network attacks begin with an ICMP ping to discover the router or network. By turning off the ICMP ping, there will be no response to any ping received from outside the network.

The final control group on the web-based advanced user interface is the utilities control group. Here the user may set parental control, restart the router, restore factory defaults, save and back up settings, restore previous settings, download firmware updates, and change system settings. These controls are all self-explanatory. Only the system settings will be elaborated on.

The system settings allow the user to enter a new administrator password, establish an administrator login timeout, change the time zone, enable remote management based on an external IP address, and turn the NAT functionality of the router on and off. Also the universal Plug and Play (UPnP) function may be turned on and off. With UPnP set to the “on” position, compliant software programs are allowed to open and close ports dynamically to pass traffic. By default this feature is disabled.

2. IXIA IxChariot

IXIA’s IxChariot is an industrial-grade network evaluation software package. Using scripts to simulate data traffic, IXIA’s IxChariot can test the performance and capacity of network hardware and software. This allows comparisons of competing network products such as 802.11n and 802.11b standard hardware. IxChariot also helps to identify the source of performance problems and provides measures and baselines for typical network operations. This allows verification of the expected performance from the network and service providers.

The IxChariot evaluation software consists of the IxChariot Console and Performance Endpoints. The performance endpoints are distributed across the network and reside as a background service on the client computers. There may be as many performance endpoints as there are network client computers. The IxChariot Console may reside on any client computer. There may be only one IxChariot Console on a network.

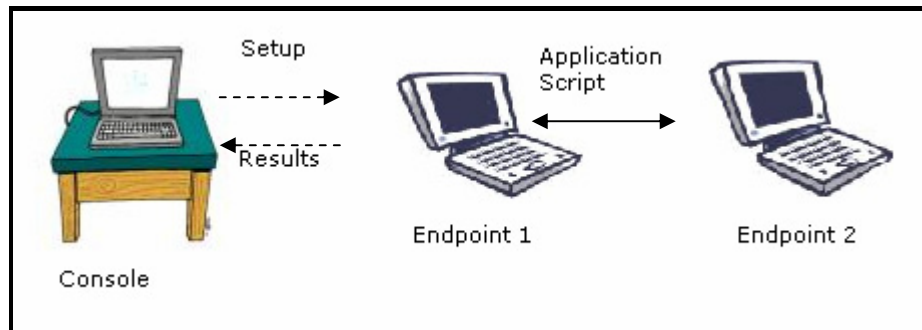


Figure 9. IXIA IxChariot Console – Endpoint Interaction (after IXIA User manual)

IxChariot evaluates the network performance by passing real data between sets of performance endpoints as controlled by the console, as shown in Figure 9. The data that are passed simulate a variety of applications and are determined by the script that is run for each test. The applications for which data is simulated need not be installed on any of the computers. There is a large library of scripts to choose from, ranging from throughput testing to VoIP testing. Each script may be edited or new scripts may be created for specific testing.

For example, The High Performance Throughput script is used to test for maximum throughput on high-performance networks that support speeds of 100 Mbps and greater. This script is appropriate to conduct stress testing for a network such as that based on 802.11n. The script uses TCP to send 10 MBs of data from Endpoint 1 to Endpoint 2. It then waits for an acknowledgment.

Once a test is conducted using a particular script, results are viewed in the console application, as shown in Figure 10. From here all aspects of the test may be explored to include the test setup, throughput, transaction rate, response time, raw data, and the endpoint configuration.

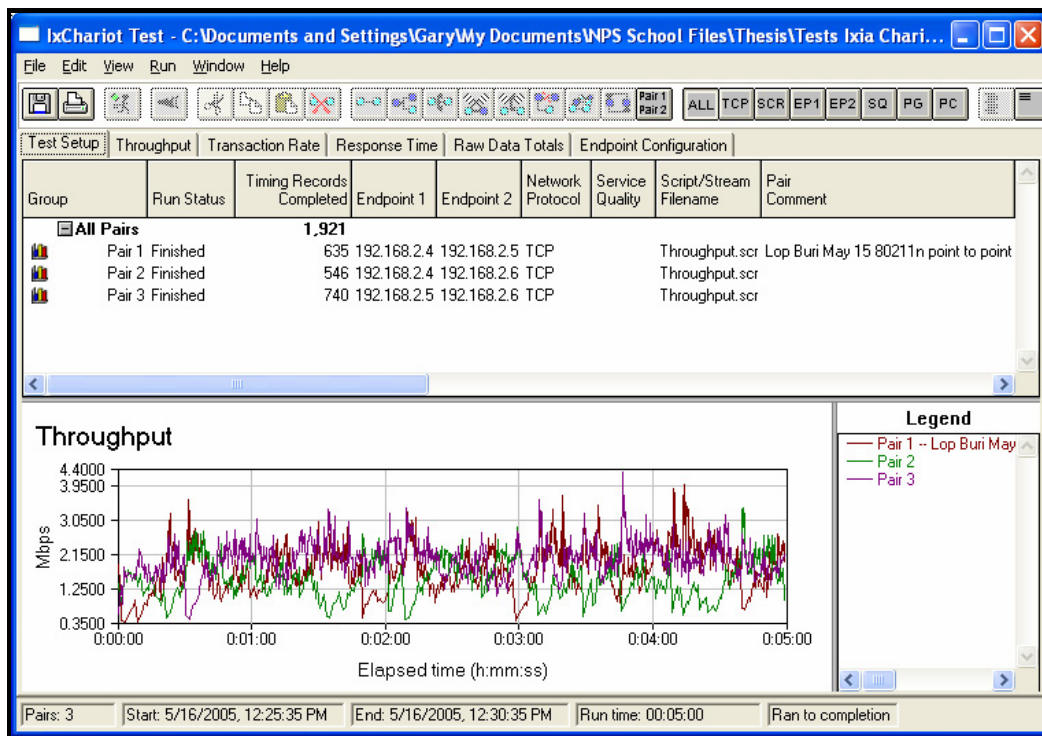


Figure 10. IXIA IxChariot Console Results

The length of each test is user configurable and the results may vary based upon the length of each test. Disabling the screen saver is important when running longer tests, as it can significantly lower the throughput measured by an endpoint. (Ixia, 2004)

IV. FIELD ASSESSMENT PROCEDURES AND METHODOLOGY

This chapter emphasizes the strength of the COASTS environment as a test-bed for technology review. The COASTS environment allows for a dynamic network configuration and operating environment while one is working with coalition and commercial partners. In this chapter, the evaluation process used to review the next generation IEEE 802.11n Equipment and Standard as a High Throughput Tactical Wireless alternative is discussed. As such, a detailed outline of the methodology, network, and equipment configuration is presented. Also, the comparison network operationally used during the COASTS 2005 Demonstrations is briefly introduced.

A. PURPOSE

The purpose of the COASTS field tests of the Belkin Pre-N equipment was to setup and to measure the throughput of a network based on the emerging 802.11n standard and to determine its applicability to the COASTS environment through the use of MOPs and MOEs. The MOEs and MOPs, as presented in Chapter I, will be specifically addressed in the next few chapters.

B. METHODOLOGY

Throughout research, the focus involved testing Belkin Pre-N equipment and network configuration in an IP network integrated into a coalition environment. The literature search for IEEE 802.11n information summarized in Chapter II laid the conceptual base for the expectations of the review. The testing was conducted during two on-site demonstrations of COASTS at RTAF Wing 2 in Lop Buri, Thailand. The first occurred in March of 2005 and the second occurred in May of 2005. The network configuration, equipment configuration, and testing results were captured during periods scheduled specifically for experimentation and at other times as available. The network and equipment configurations are presented in the following sections. The test data results are presented in the following chapter.

C. FIELD EXPERIMENTS

In March and May of 2005, two field experiments were conducted on a high throughput wireless network based on the Belkin Pre-N router's 802.11n implementation.

The overall network and equipment configurations are presented below. Further, MOPs 1.0 to 4.0 addressing the underlying research question as enumerated in Chapter I are detailed.

1. Network Operating Area

The work site for the COASTS March and May 2005 Demonstrations was the Khok Kathiam Airfield at N 14.8746 ° E 100.6634 ° and an elevation of 98ft above mean sea level. The airfield is near the town of Lop Buri, Thailand located approximately 60 nm due north of Bangkok, Thailand.

The major network nodes included the Royal Thai Air Force (RTAF) Wing 2 communication facility, the Mobile Command Platform (MCP), and the aerial balloon node. During the initial phase of the COASTS March 2005 Demonstration, these sites were located as shown on Figure 11.

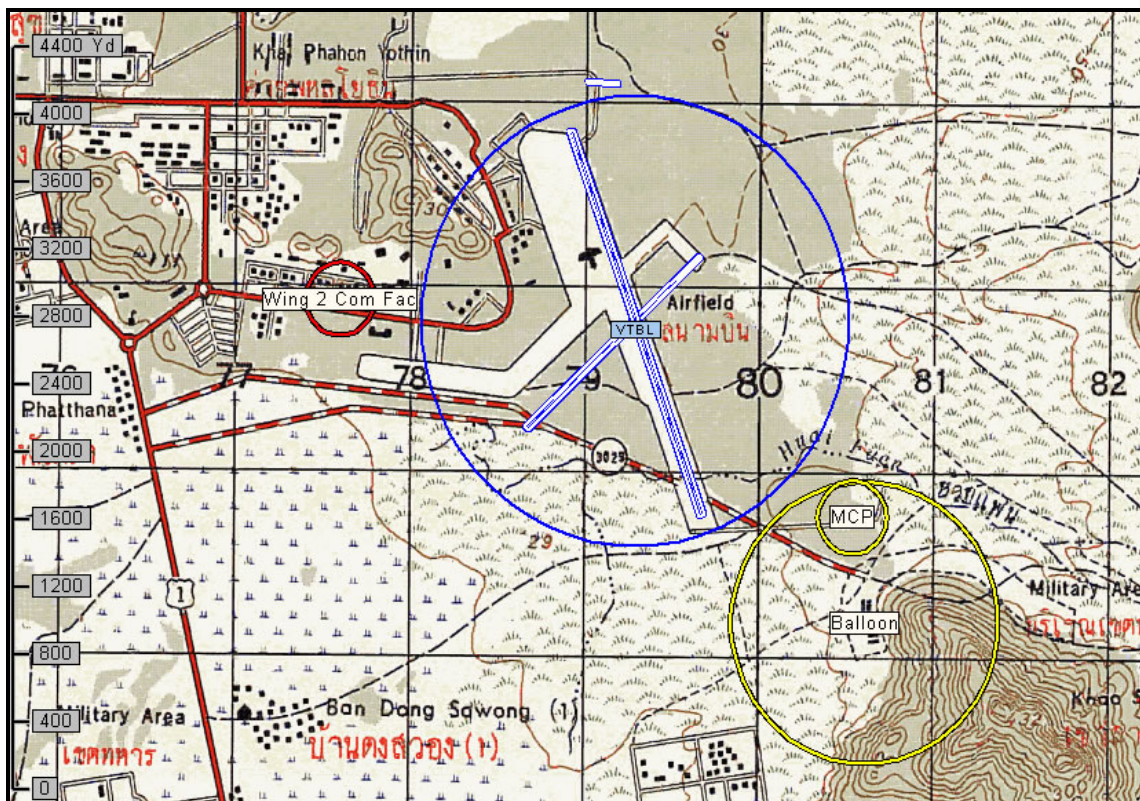


Figure 11. COASTS March 2005 Demonstration Locations

Due to operational constraints, these locations were subsequently moved as shown in Figure 12. These locations remained the primary sites for the network nodes throughout the COASTS May 2005 Demonstration. Figure 13 is an aerial view.

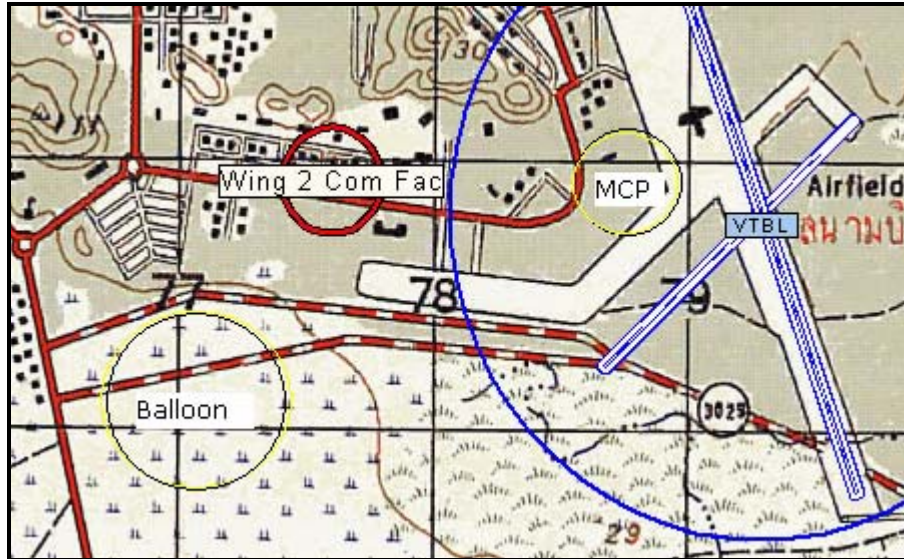


Figure 12. COASTS May 2005 Demonstration Locations



Figure 13. Aerial View of COASTS 2005 Operating Area

The majority of all network operations occurred between the MCP and balloon nodes listed in Figures 12 and 13. The experimentation on the emerging 802.11n network took place primarily at the MCP node.

2. Network Configuration

The entire COASTS network was configured as a static IP network. The various nodes were assigned an IP space, an appropriate subnet mask, and gateway for the duration of the Demonstrations. They are tabulated in Table 1 below.

Node Name: IP Address / Subnetmask		Gateway:
MCP Network: 10.109.2.0 / 255.255.255.0		10.109.2.254
<i>Address</i>	<i>Node Name</i>	
10.109.2.2	TrakPoint / Status server	
10.109.2.3	Mike's Laptop	
10.109.2.4	TrakPoint C2 Laptop	
10.109.2.5	Moteview Laptop	
10.109.2.6	Rotowing Laptop	
10.109.2.8	Francisco's Laptop	
10.109.2.7	Net Mon. Laptop	
10.109.2.9	Sony Cam on Tower	
10.109.2.61	Ryan's Laptop	
10.109.2.100	TrakPoint Demo Server	
Mountain Network: 10.109.4.0 / 255.255.255.0		10.109.4.254
<i>Address</i>	<i>Node Name</i>	
10.109.4.2	AN-50 (At MCP)	
10.109.4.3	AN-50 (At Mountain)	
10.109.4.4	Sony Camera	
BreadCrumb Network: 10.109.3.0 / 255.255.255.0		10.109.3.254
<i>Address</i>	<i>Node Name</i>	
10.109.3.2	Tacticomp (NPS #1)	
10.109.3.3	Tacticomp (NPS #2)	
10.109.3.4	Tacticomp (MDS #1)	
10.109.3.5	Tacticomp (MDS #2)	
10.109.3.6	Balloon Cam (Type TBD)	
10.109.3.7	MCP Webcam	
10.109.3.8	Stargate (Crossbow)	
10.109.3.9	CyberDefense Laptop	
10.109.3.10	Balloon Laptop	
10.109.3.11	Rotowing PDA	
10.109.3.12	Rotowing Flight Controller	
10.109.3.13	Rotowing Spare Address	
10.109.3.14	BCAdmin Laptop (MCP)	
10.109.3.15	AU-23 Webcam Laptop	
10.109.3.16	Rotowing AP	
10.109.3.17	Stefan's Laptop Wifi	

10.109.3.18	Clayton's Laptop Wifi	
10.109.3.19	Rotowing Spare Address	
10.109.3.20	Brian's Laptop	
10.109.3.51	Stefan's Laptop	
10.109.3.61	Ryan Laptop (Res IP)	
10.109.3.123	TrakPoint Demo Laptop	
10.109.3.25	Scenario Cam (Axis 213)	
802.11n Experimental March: 10.109.3.0 /255.255.255.240		10.109.5.254
10.109.3.1	Belkin Pre-N Router	
10.109.3.10 or 40	Laptop1	
10.109.3.11 or 41	Laptop2	
10.109.3.12 or 42	Laptop3	
802.11n Experimental May: 192.168.2.0 /255.255.255.0		Isolated
192.168.2.1	Belkin Pre-N Router	
192.168.2.4	Laptop1	
192.168.2.5	Laptop2	
192.168.2.6	Laptop3	
Downtown Network: 172.16.0.16 / 255.255.255.240		172.16.0.18
<i>Address</i>	<i>Node Name</i>	
172.16.0.20	AN-50 (At MCP)	
172.16.0.19	AN-50 (At Downtown)	
172.16.0.17	Downtown Router	
172.16.0.21	AN-50 config laptop	
RTAF NETORK: 10.109.100.0/255.255.255.0		10.109.100.1
various		
RTSC NETWORK: 10.109.101.0/255.255.255.0		10.109.101.1
various		

Table 1. COASTS Network IP Addresses, Subnet Masks, and Gateways

The address space allocated to the testing of the Belkin Pre-N router and 802.11n network are within the 10.109.5.0 Class C address with a subnet mask of 255.255.255.240. The laptops themselves are shown below in Figure 14. When operating as an aspect of other nodes, in particular as the BCAdmin (10.109.3.14/255.255.255.0) or the airborne AU-23 webcam laptop (10.109.3.15/255.255.255.0), the network configuration was manually changed by accessing the Properties of the Internet Protocol in the Local Area Connection Properties of the Control Panel.



Figure 14. Laptops Used for the 802.11n Experimental Network

In Figure 15, one can see the laptops configured for the 802.11n experimentation at the location previously indicated as the COASTS network MCP node. The airfield tower and the firehouse can be seen in the background for orientation. In the foreground, the Fujitsu and Dell laptops are positioned outside the MCP approximately 150 ft from the hosting Belkin Pre-N router, which is located inside the firehouse. Approximately twenty feet behind the table, one of the antennas for the BreadCrumb 802.11b network can be seen. The BreadCrumb 802.11b network provided the backbone of the LAN used for operations during the COASTS 2005 Demonstrations.



Figure 15. Laptops and BreadCrumb Seen outside the MCP

Overall, a basic network diagram is presented in Figure 16 for the Pre-N LAN. This simplified version offers a clear view of the testing platform. It does not have the complexity of the full BreadCrumb network used during the COASTS Demonstrations, as shown in Figure 17, but a BreadCrumb network comparable to the simpler 802.11n network used for testing was set up as described later. First, the 802.11n equipment configuration will be discussed and the MOPs will be addressed.

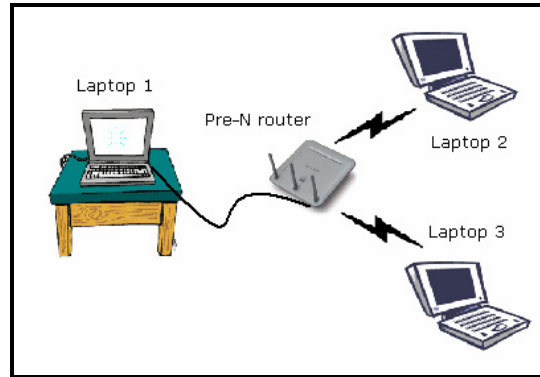


Figure 16. Basic Pre-N Network Diagram

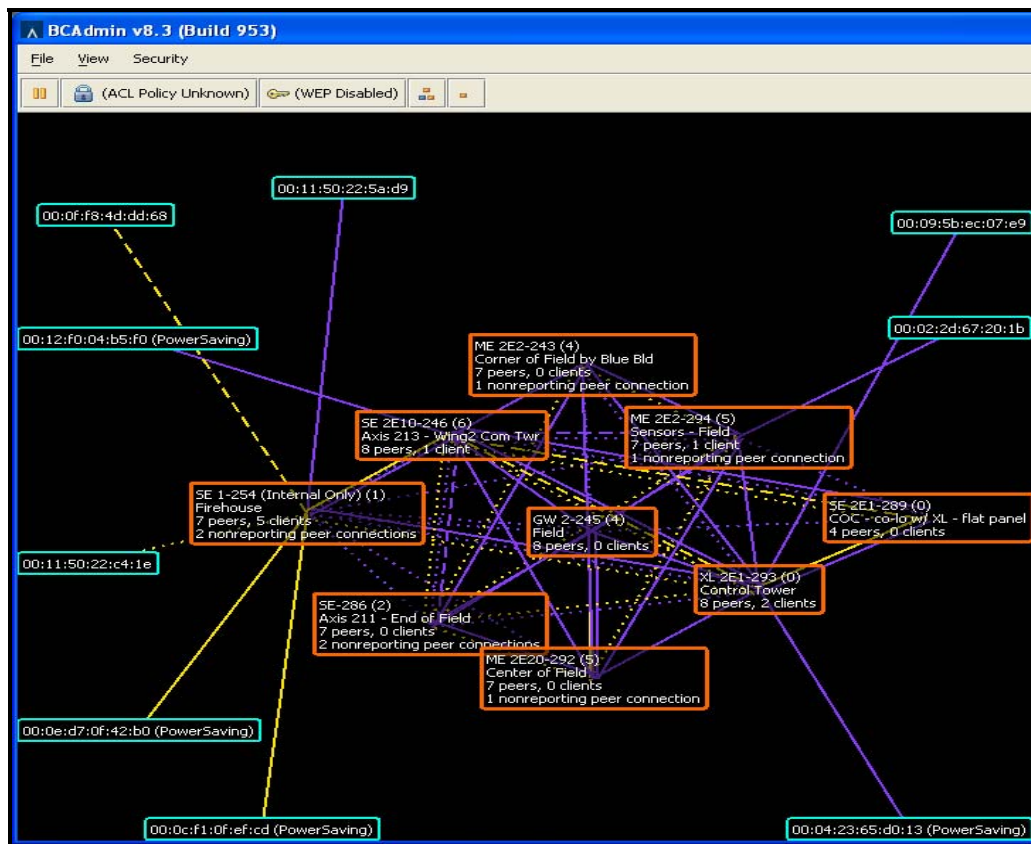


Figure 17. BreadCrumb Network Diagram for COASTS Demonstrations

3. Equipment Configuration

The following Measures of Performance (MOPs) summarize the configuration of the Belkin Pre-N router and network configuration. MOP 2.0 addresses the specifics of the system settings. These settings are shown in Table 2 below:

MOP:	Description:	Setting:	Discussion:
2.0	What were the system settings?	N/A	The system settings are discussed below.
2.1	AP Mode	ENABLED	This defeats the NAT IP sharing and DHCP server for operation in a static IP address environment.
2.2	MAC Addresses	x-x-x-x-x-x	See Table 3.
2.3	IP Addressing	10.109.5.0	As shown in Table 1.
2.3.1	IP Pool	N/A	Class C addresses in the 10.109.5.0 space manually set.
2.3.2	Lease Time	N/A	Lease time only exists for DHCP controlled IP addresses. See MOP 2.4.
2.3.3	Subnet Masking	255.255.255.0	As shown in Table 1.
2.4	DHCP Server	OFF	In order to not interfere with other network activities. Each computer on the 802.11n network is manually configured with an IP address.
2.5	SSID	Set to	"802.11n thesis default IP"
2.6	Wireless Mode	802.11g only	In order to allow only Pre-N and 802.11g compliant devices access the network. This bars the slower 802.11b devices and provides de-confliction with other network operations.
2.7	QoS (802.11e) Mode	ON	Allows HCP and EDCF to prioritize higher priority traffic.
2.8	Protected Mode	ON	The Pre-N capabilities are not affected by this setting. This setting allows 802.11g devices to operate at higher speeds in a mixed-mode environment.
2.9	Wireless Channels	AUTO	Allows automatic selection of clearest channel during AP start up.
2.10	ACK Mode	BURST	Allows "blocking" (grouping) of ACK receive messages and lower overhead for each message.
2.11	Security Settings	DISABLED	IOT provide the most efficient use of the channel bandwidth possible. All encryption and security are set to off.
2.11.1	WEP/WAP	OFF	In order to reduce overhead.
2.11.2	Key	N/A	Only applies if WEP or WAP are on.
2.11.3	Firewall Settings	OFF	No access to outside networks. The firewall is set to off to reduce computational overhead and generate the highest possible throughput.

Table 2. Measures of Performance for System Settings

Component	MAC
Router WLAN	00-11-50-21-EB-68
Router WAN	00-11-50-21-F3-51
Router LAN	00-11-50-21-F3-50
Belkin Wireless Card 1	00-11-50-22-5A-D9
Belkin Wireless Card 2	00-11-50-22-5C-99
Belkin Wireless Card 3	00-11-50-22-C4-1E

Table 3. Component MAC Addresses

4. Environmental Conditions

Generally, the environmental conditions during the COASTS March and May Demonstrations occurred during the “hot” season in Thailand, which lasts from mid-March to late-May (MOP 3.0). The Lop Buri area is best described as central flatlands with outcroppings of mountains that reach up to 4,000 ft (MOP 3.1.1). The area is vegetated with small shrubs. The local testing area, adjacent to an active airport runway, consisted of low lying grass, plowed, and fallow fields (MOP 3.1.2).

The mornings were typically sunny with humidity in the high 90s (MOP 3.2.2). As afternoon approached, the sky became cloudy with brief periods of intense rain (MOP 3.2.3). The rain showers cooled the area from the highs around 40°C to a sunny evening around 30°C (MOP 3.2.1). Winds were inconsistent in the local area due to the orographic lift generated by the nearby mountains and the convective thermals of the farming fields nearby (MOP 3.2.4)

Tests on the Belkin Pre-N equipment were conducted during the time of cloud build up from 1000 in the morning to 1700 in the evening (MOP 3.3). This period was the hottest and most humid portion of the day. It was also the only period available for testing throughout the COASTS Demonstrations.

5. Comparison Network

In order to conduct a comparison test between equipment based on the emerging 802.11n standard and the current network platform, a common load for stress testing the network was chosen. The IXIA IxChariot network evaluation software presented earlier was used with the *throughput.scr* script. The *throughput.scr* script is recommended for testing maximum throughput on typical networks. This script was adjusted to send 10

MB between each endpoint pair. It then waited for an acknowledgment. The script thus simulated the core file transfer transaction performed by many demanding audio and video applications (MOP 4.0).

The backbone LAN used during COASTS operations in 2005 was based on a COTS product from Rajant Technologies (www.rajant.com) called BreadCrumbs. A full explanation of the operation and technology of the BreadCrumb is beyond the scope of this thesis. Essentially, the BreadCrumb is composed of a weather-resistant case enclosing two 802.11b wireless LAN NICs attached to an amplifier (on some models) and an optional external antenna. The models without the amplifier and external antenna were not used during this testing. The NICs were coupled by an open-source operating kernel and powered by an internal rechargeable battery. The BCAdmin software (shown previously) was used to administer the network. The BreadCrumbs shown in Figure 18 simulate a mesh network and claim simplicity of use as a major attribute.



Figure 18. Rajant BreadCrumb SE

The comparison network was established as shown in Figure 19. Basically, instead of the Belkin Pre-N router functioning in AP mode, as illustrated in Figure 16, the Rajant BreadCrumb was used as the access point. This BreadCrumb was an SE model attached to an optional external 9dBi omni-directional antenna via the amplified connection.

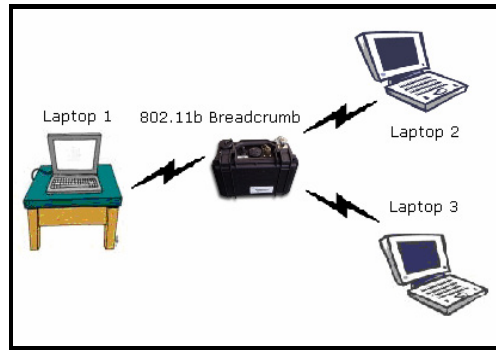


Figure 19. Basic Rajant BreadCrumb Network Diagram

In Figure 20, the BCAdmin view of the network is shown. The large, orange boxes represent the BreadCrumbs; the small, cyan boxes represent client nodes. During testing, only the central dashed, orange box (SE -286) and the cyan boxes labeled: Fujitsu 802.11n test, Dell 802.11n test, and AU-23 Air Node Laptop, were used for testing.

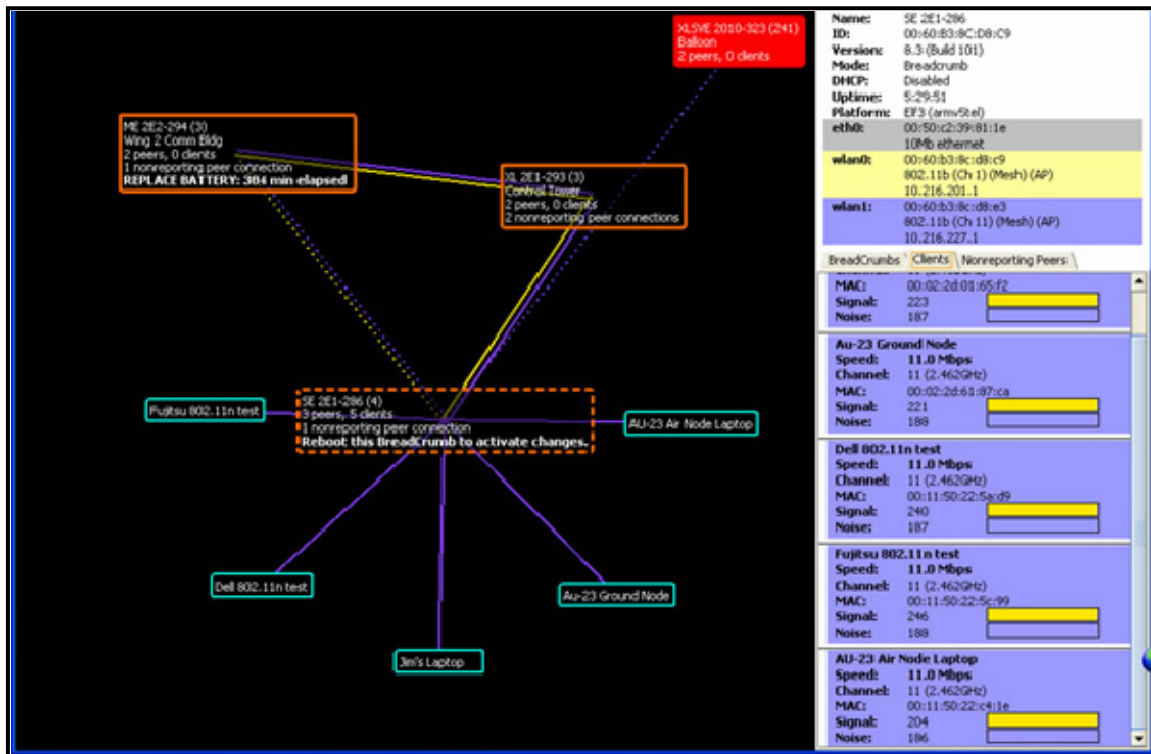


Figure 20. Rajant BreadCrumb BCAdmin Network

In the next chapter, the IXIA IxChariot test results on the Belkin Pre-N and BreadCrumb networks are presented followed by some factors affecting the testing.

THIS PAGE INTENTIONALLY LEFT BLANK

V. RESULTS

This chapter depicts the results of four representative tests on the previously described Belkin Pre-N and BreadCrumb networks. All results were gathered using the Ixia IxChariot network evaluation suite. The settings for each test, called the run options, are described. The endpoint pair configurations, referred to as the test setup, are detailed. In addition, the throughput (MOP 5.0) and response time (MOP 6.0) for each test are given for the system under a common load.

A. RUN OPTIONS

The run options for each test were the same, with the single exception of the run duration. The run duration for each test is given in the description of the tests in the next section. All tests used the same settings are listed in Table 4.

Description	Run Option
End type?	Run for a fixed duration.
Reporting type?	Real-time.
Automatically poll endpoints?	Yes.
Polling interval [minutes]:	1
Stop run upon initialization failure?	Yes.
Connect timeout during test [minutes]:	0
Stop test after this many running pairs fail:	1
Collect endpoint CPU utilization	No.
Validate data upon receipt?	No.
Use new seed for random variables each run?	Yes.
Console Protocol?	TCP.

Table 4. Run Options

B. TEST SETUP

1. Test 1

Test 1 occurred on March 28th, 2005, at 1545. The physical network configuration was as shown in Figure 15. The test ran to completion for one minute and twenty seconds. During this test, two endpoint pairs were evaluated over the BreadCrumb network. The two pairs were 10.109.3.15:10.109.3.41 and 10.109.3.15:10.109.3.42.

2. Test 2

Test 2 also occurred on March 28th, 2005, but at 1615. This test's physical layout was exactly the same as Test 1 and is shown in Figure 15. Similarly, the endpoint pairs were exactly the same as in Test 1. Test 2 ran to completion for one minute and twenty seconds. The difference was that this test ran over the Belkin Pre-N network.

3. Test 3

Test 3 is included as a more interesting run on May 16th, 2005, at 1305. This test had a different physical layout than Tests 1 or 2. Test 3 was a side-by-side comparison, as shown in Figure 14. What made this test more interesting was the detected error and the error's implication on the test results.. A screen saver was activated near the very end of the five-minute test. The three endpoint pairs in this test over the BreadCrumb network were 192.168.2.4:192.168.2.5, 192.168.2.4:192.168.2.6, 192.168.2.5:192.168.2.6.

Sometimes, more is learned from a test with errors than one without errors. This is particularly true when the test with errors still remains representative of the overall performance of a system. The detailed throughput of this test, broken up by nodes, reveals that there is only a very small difference in the test results for the node where the error was detected. Specifically, only a difference of 0.067 Mbps exists. This is to be expected considering 4/5th of the test was completed before the error. Likewise, for the response time, we see the maximum response time increase by a factor of six; however, this is not a part of the measured time that IxChariot uses for calculations (which is explained further in the next section), resulting in very little change overall. A difference of only 0.216 seconds in response time for that single node equates to a 0.072 second difference in the average response time of 1.562 seconds.

The reason for including Test 3 is to demonstrate the robustness and flexibility of the IXIA IxChariot testing strategy. Accurate predictions and conclusion may still be made when one aspect of the evaluation is incomplete if one understands the global impact of those results. In this case, the error can be ignored for two reasons: 1) It is well within the bounds of comparison since the comparisons values are two orders of magnitude larger than the error, and the comparison values themselves are 200% to 300% different from each other, as the results indicate. 2) The calculation scheme used by IxChariot minimizes the effect of endpoint nodes timing out.

4. Test 4

Test 4 returned to more standard results when it was completed on May 16th, 2005, after a five-minute test duration. The physical setup and the three endpoint pairs remained the same as for Test 3, but Test 4 was conducted across the Belkin Pre-N network.

C. THROUGHPUT AND RESPONSE TIME RESULTS

The IxChariot network evaluation suite calculates throughput using the metrics of *bytes sent*, *bytes received*, *throughput units*, and the *measured time* in the following formula:

$$(\text{bytes sent} + \text{bytes received}) / (\text{throughput units}) / \text{measured time}.$$

Bytes sent is the number of bytes sent by endpoint 1 of a pair. *Bytes received* is the number of bytes received by the endpoint of a pair. The variable *throughput units* is set by the user. In these tests, the *throughput units* was Mbps. That equates to 125,000 bytes per second or 1,000,000 bits divided by 8 bits per byte. The *measured time* is the sum, in seconds, of all the timing record durations returned for the endpoint pair. This may be less than the amount of time the script was actually executing. The actual time the script was executing is the elapsed time and is not used in these calculations. This use of *measured time* is the main reason that the values of Test 3 remain valid.

It is important to note that IxChariot measures the throughput associated with packet payload, ignoring headers. This is referred to as Goodput in RFC 3511. Each time the word “throughput” is used, one can assume Goodput is the returned value. In general, the throughput measures how much data moves across the network (Ixia, 2004).

In order to determine how quickly the data moves across the network, IxChariot calculates the response time. The response time has an inverse relationship to the throughput. As the throughput for a set of endpoints increases, the response time decreases. The response time is, literally, the inverse of the transaction rate; it is the time, in seconds, needed for one transaction to occur.

The figures depicting throughput and response time show a general impression of the results. They are not meant to be used to interpolate specific values. Specific values are available from IxChariot via exporting all data into a comma separated values. Only a summary is provided here.

Also of note is the labeling of the pairs in the legend for each figure. Pair 2 connects the same hardware in each test, just as Pair 3 does. For the two test runs (3 and 4) that have three total sets of pairs, the added pair that is not included in the first two tests is labeled as Pair 1.

In Figure 21, the throughput of Pair 2 is seen to be consistently higher than Pair 3, with the exception of one inflection point around the 30 second marker. The average of Pair 2 is estimated at 0.85 Mbps, and the average of Pair 3 is near 1.45 Mbps. The sum of each pair's average is an indication of the throughput for the network. The network throughput was calculated to be 2.28 Mbps. This is a reasonable value for a network based on the 802.11b standard.

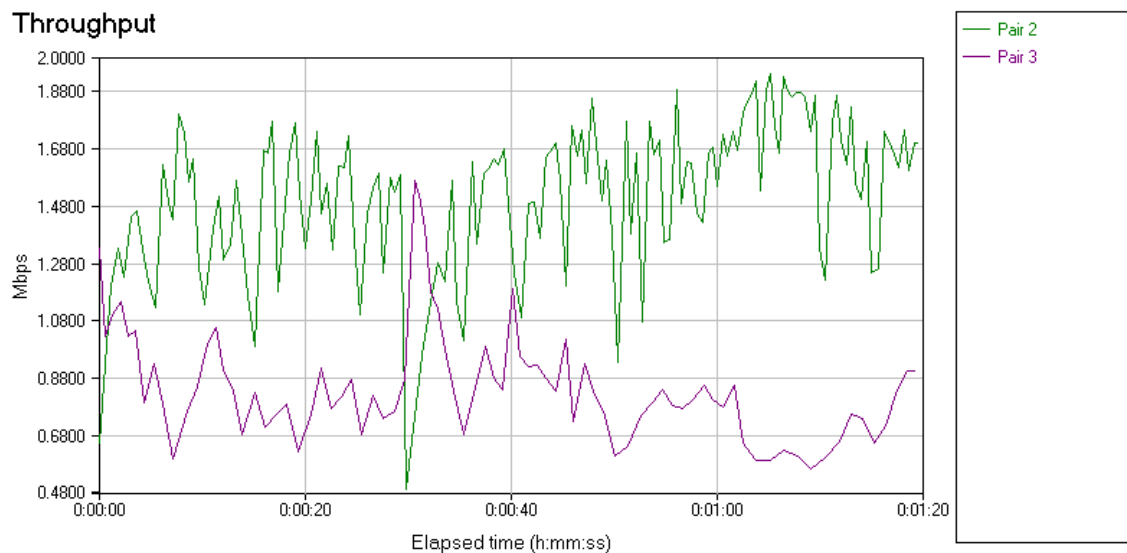


Figure 21. Test 1 Throughput between Pairs

The inflection point is readily apparent in the Test 1 response time, shown in Figure 22. At this point, the network speed between Pair 2 was very low. Pair 3 took advantage of the newly available network bandwidth, as is seen by Pair 3's sudden decrease in response time.

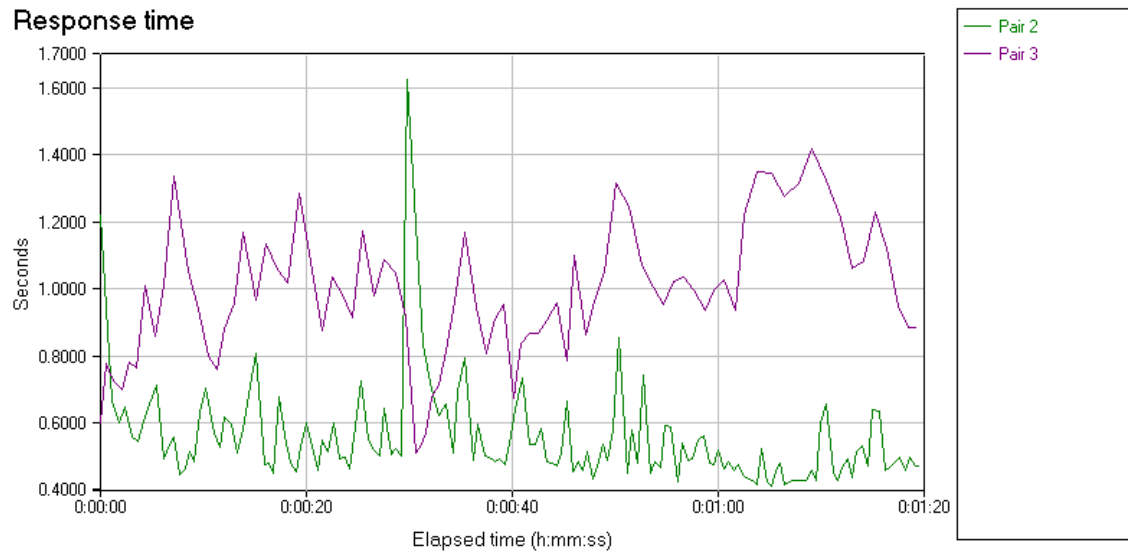


Figure 22. Test 1 Response Time between Pairs

In Figure 23, rapid variation in the throughput of each endpoint set is shown for the Belkin Pre-N network. This is reasonable considering the MIMO configuration. Each antenna transmits at different rates to maximize the overall throughput and to isolate interference. Here we see a larger throughput for each endpoint set and for the network. The calculated value of the Belkin Pre-N network throughput was 6.304 Mbps. This is much less than the promised theoretical maximum of 108 Mbps, but not unexpected.

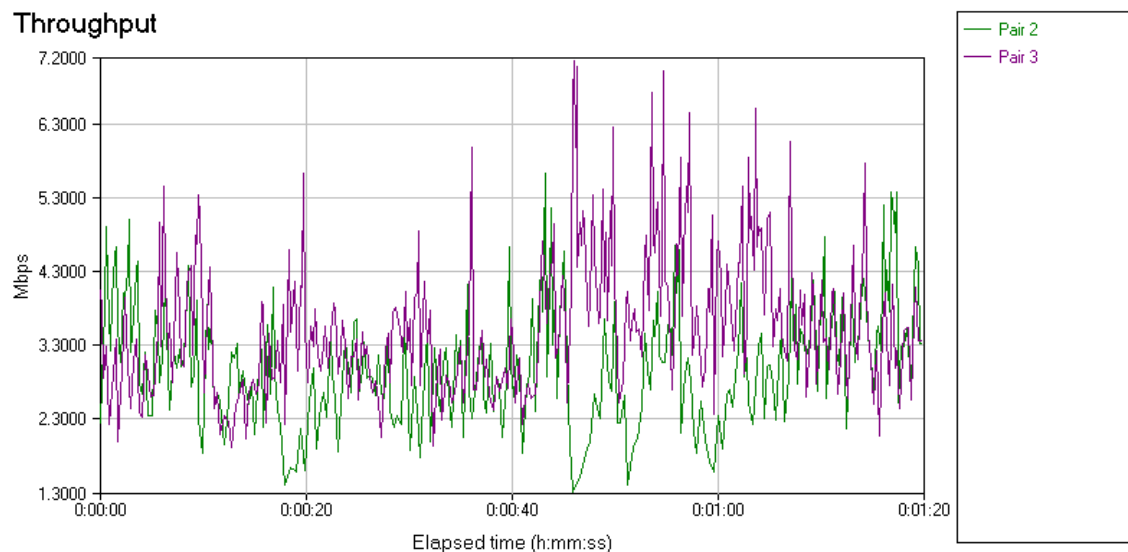


Figure 23. Test 2 Throughput between Pairs

Likewise, Figure 24 shows significantly decreased response times for the Belkin Pre-N network than for the BreadCrumb network. Alas, this is expected considering the promised increase in throughput offered by the adoption of 802.11n draft standards.

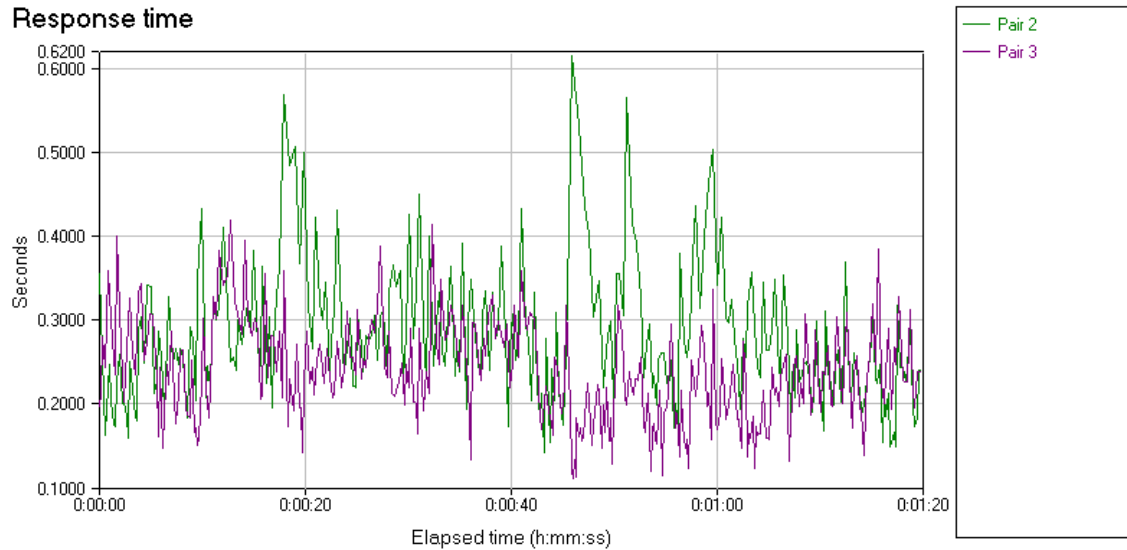


Figure 24. Test 2 Response Time between Pairs

In Figure 25, the Test 3 throughput results have an error due to a non-reporting station. This station stopped reporting when its screen saver was activated. We can see the trend of data for the three sets of endpoints on the BreadCrumb network shows around a 0.62 Mbps throughput for each endpoint set. This is consistent with a more heavily loaded network than in Test 1. Also, the test duration of five minutes was cut short by approximately one minute; however, this does not affect the results of the previous four minutes of testing, as discussed earlier.

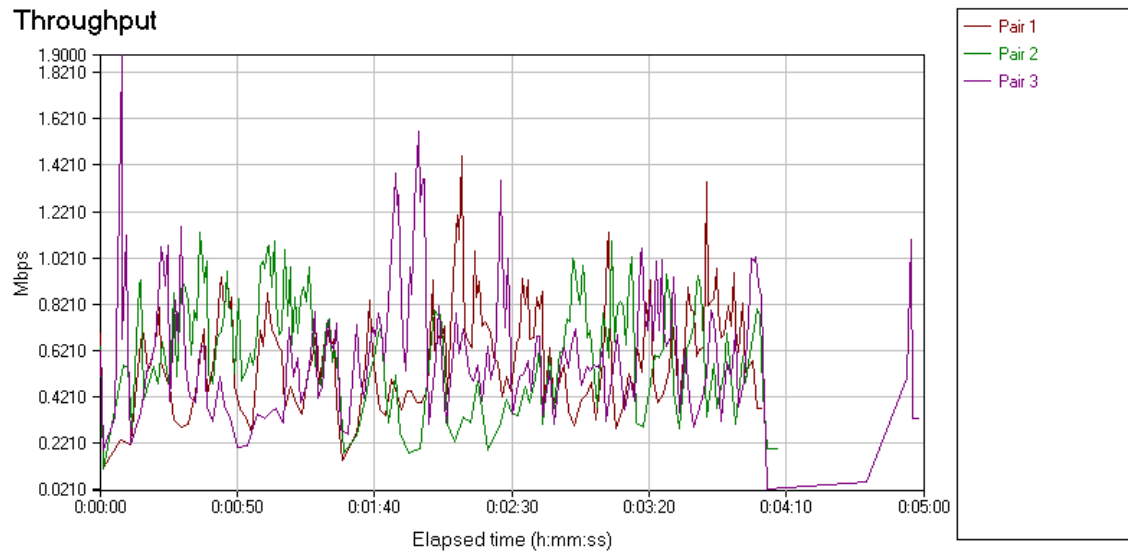


Figure 25. Test 3 Throughput between Pairs

In Figure 26, the rapid increase of response time associated with the non-reporting endpoint can be seen.

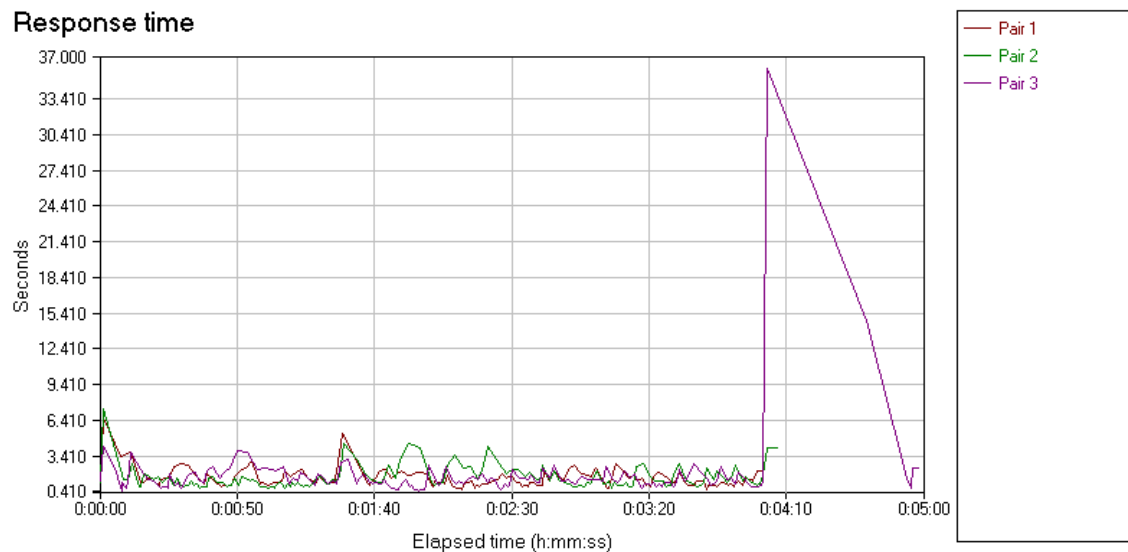


Figure 26. Test 3 Response Time between Pairs

Figure 27 displays the throughput results of Test 4. The three endpoint pairs show similar network loading characteristics of the previous test, but each endpoint set maintains a much higher throughput with the Belkin Pre-N network than with the BreadCrumb network.

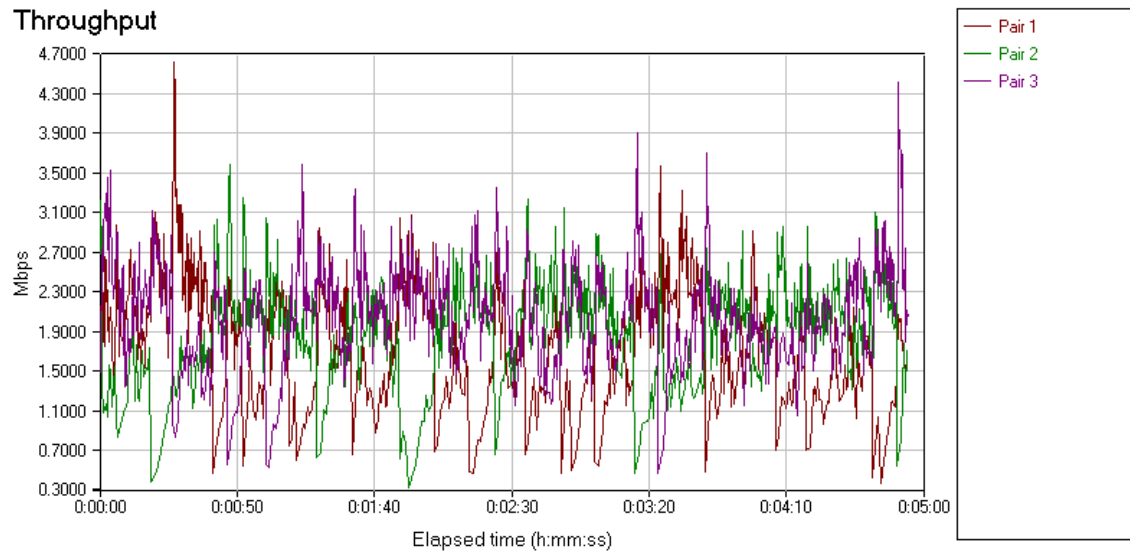


Figure 27. Test 4 Throughput between Pairs

The data in Figure 28 verify the expectation that the response time of the Belkin Pre-N network is much less than that for the BreadCrumb network even when both are under a heavier load than in Test 1 and 2. Also, generally, there is a tighter distribution of response time for the Belkin Pre-N network compared to the response time for the BreadCrumb network of Figure 26 before the four-minute mark.

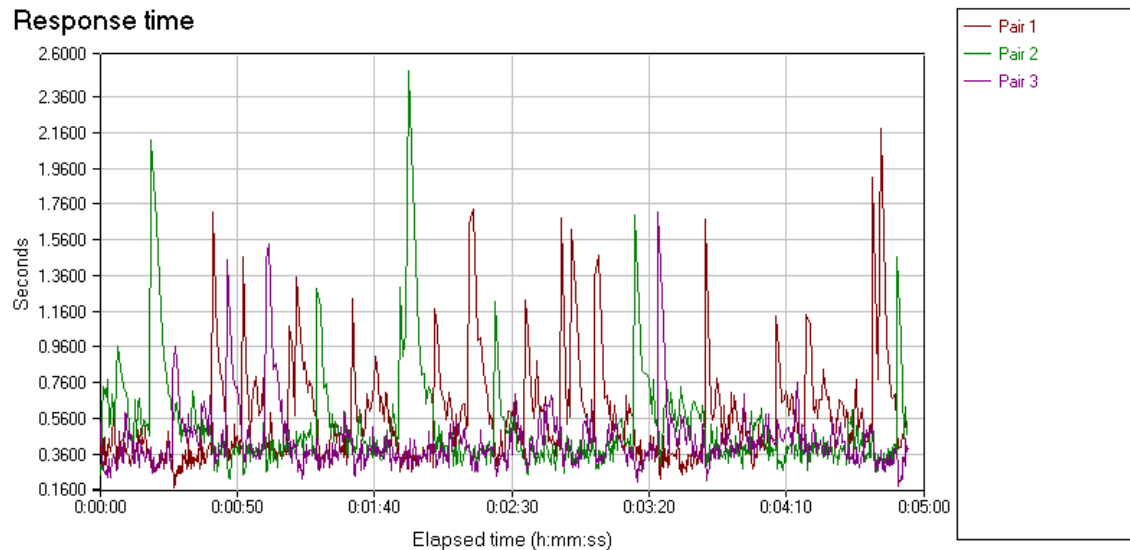


Figure 28. Test 4 Response Time between Pairs

D. RESULTS SUMMARY

A summary of the throughput and response time results calculated by IxChariot is displayed in Table 5 (MOP 5.0 to MOP 6.0, all inclusive). The average throughput is the sum of the average of all pairs' throughput whereas the average response time is the average of all pairs' response times. The minimum and maximum throughput and response time represent the lowest and highest value for any one pair, respectively.

Test	Type	Throughput [Mbps]			Response Time [seconds]		
		Minimum	Average	Maximum	Minimum	Average	Maximum
1	B/C	0.492	2.280	1.942	0.412	0.762	1.625
2	Belkin	1.301	6.304	7.143	0.112	0.255	0.615
3	B/C	0.022	1.348	1.896	0.422	1.562	36.027
4	Belkin	0.319	5.397	4.624	0.173	0.447	2.508

Table 5. Summary of Throughput and Response Times for Tests 1 through 4.

From this table, it is apparent that the Belkin Pre-N network had a performance advantage over the BreadCrumb network in a similar configuration. For throughput, there was a 176% advantage for the Belkin Pre-N network during Test 1 and 2 and a 297% advantage for the Belkin Pre-N network during Test 3 and 4. Since the response time is proportional to the throughput, the Belkin Pre-N network realized a 199% response time advantage during Test 1 and 2. Likewise, during Test 3 and 4, the Belkin Pre-N network demonstrated a 249% advantage in response time.

E. FACTORS AFFECTING RESULTS

The results of the IxChariot evaluation suite are indicative of typical network operations. The performance of any network is based upon the performance of all its components and their relation to one another. Similarly, the gathered test results are affected by factors involving the network components and interactions. Here some of those factors and the steps taken to mitigate their effects are considered.

1. CPU Speed

The endpoint service installed on each endpoint laptop executes only as fast as the CPU will allow. By maintaining the same hardware for each endpoint and maintaining the same endpoint connections the effects of the various CPU speeds of the laptops result in a systemic bias. Therefore, each test may be equitably compared to the other tests.

2. Ram and Disk Swapping

If a test is conducted on a system that has insufficient RAM, then a large amount of disk swapping continuously occurs. Disk swapping will degrade the performance of the endpoint potentially to the point of failure. Also, similar issues such as those for CPU speed must be considered. All tests were accomplished with no programs other than the Ixia endpoint service and virus scanning software active. The test itself emulates the data traffic of programs and routines that access the network connection. The RAM and Disk Swapping on each piece of hardware introduced another systemic bias. As such, the test results may be readily compared.

3. Endpoint Operating System

The same arguments and mitigations that were applicable to CPU speeds, RAM, and Disk Swapping are applicable to operating systems. Each operating system handles the TCP stack differently; some are more efficient than others, so the software loaded and running on each laptop was not altered between tests.

4. Virus Scanners

In terms of running software, virus scanners consume a considerable amount of the CPU power. Each laptop had Symantec AntiVirus Corporate Edition 8.0.1.425 with scan engine 4.1.0.22 and virus definition file version 3/25/2005 revision 9 installed and running. Anti-virus software was active on each endpoint of the COASTS operational networks, by continuing to run the anti-virus software a higher-fidelity test, in terms of operational correlation, was achieved. Also, since this software was running on each client differences between endpoints was minimized.

5. Network Configuration

Altering router settings and the physical configuration of the network may potentially change test results. For this reason, each test was conducted with the same hardware, software, and configuration settings. The comparison tests were also conducted back-to-back in the same physical locations.

6. Network Activity

Other network activity can affect the performance of the test. Other computers on the network will compete for network resources. To eliminate this potential, the Belkin Pre-N tests were configured as an isolated network using the private address space. The

BreadCrumb network was configured on a separate sub-network and tested during times when other network operations were not conducted. In the case of the March COASTS Demonstration, this was during the tear-down phase of the operation. During the May COASTS Demonstration, testing was performed during specifically reserved periods.

7. Screen Savers

As discussed earlier, screen savers can cause an endpoint to stop reporting. This is due to the consumption of CPU resources. It is important to ensure screen savers are not active during testing. Otherwise, incomplete test results, such as during Test 3, will occur. These test results may remain valid depending upon the specific test conditions, but if the test goal is to gathering data over a specific time period, then results may vary.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS

In this chapter, conclusions about the qualitative aspects of the system, as captured in the measures of effectiveness, are reviewed. Also, general conclusions are expressed about the utility of the analyzed equipment and standards.

During both experimentation phases of the COASTS March and May Demonstrations, the Belkin Pre-N router effectively transmitted data, as simulated by the IxChariot network evaluation suite, across all nodes of the local area network (MOE 1.1). As previously described, the IxChariot network evaluation suite mimicked the transfer of text, audio, and video data using the *throughput.scr* to analyze the network's throughput and response time (MOE 1.1.1, 1.1.2, 1.1.3), as shown in the previous chapter. Since the evaluation was limited to only a local area network, no testing was conducted across a larger wide area network (MOE 1.2). No difference in capabilities is expected across a WAN, given the ISO layered architecture standards and compatibilities, as described in Chapter II.

Compliance with standards allows the Belkin Pre-N router to operate in conjunction with other compliant networks assuming employment of the proper routing and configuration. This allows the device to network across most previously established infrastructures or to operate without any previous network infrastructure (MOE 2.2). In regard to physical characteristics, the Belkin Pre-N router is certainly portable, but only to the extent of the nearest power supply (MOE 2.1). The lack of an internal battery (or other self-sufficient power supply) limits the device's usefulness in austere locations. There were no problems operating in the humid plains of Lop Buri, Thailand, during the COASTS March and May Demonstrations (MOE 2.0, 2.3, 2.3.3, 2.3.5). Results may vary in other operating environments due to thermal overload or signal interference. The device is expected to operate tolerably well if one does not mind the limited range imposed by obstacles such as vegetation and building walls (MOE 2.3.1, 2.3.2, 2.3.4). However, the equipment was not tested in other environments.

The Belkin Pre-N router is fairly user friendly (MOE 3.0). The level of the user's experience to deploy the network in other than a home networking environment must be

much greater than that of a novice or intermediate level user, but not quite so high as an expert in the subject matter (MOE 3.1). This is exemplified by the software setup wizard, which allows for easy connection in a home network environment; however, a much greater knowledge of network configuration is necessary to deploy the equipment in an austere location or to connect to other pre-established infrastructure (MOE 3.1.1). This is the realm of the power user. This is especially true when one is attempting to troubleshoot and to repair the network. Special knowledge of the network architecture, IP addressing scheme, and router configuration are particularly important (MOE 3.1.2 and 3.1.3). Once the network is established, an end-user will enjoy a more robust network than other networks based on the previous 802.11b and 802.11g standards and require only novice networking operations skill (MOE 3.2). The reason for this is simple. The user has more throughput available, leading to faster transfers of data, which result in shorter response times for inquiries across the network. Take, for example, a network environment such as was established during the COASTS March and May Demonstrations. In this environment the end-user is connected to higher headquarters via a local area network (either 802.11b or 802.11n) passing data to a wide area network using 802.16 and then via an Ethernet enabled headquarters installation (802.3). Data can be thought of as analogous to water flowing through pipes. This is shown in Figure 29.

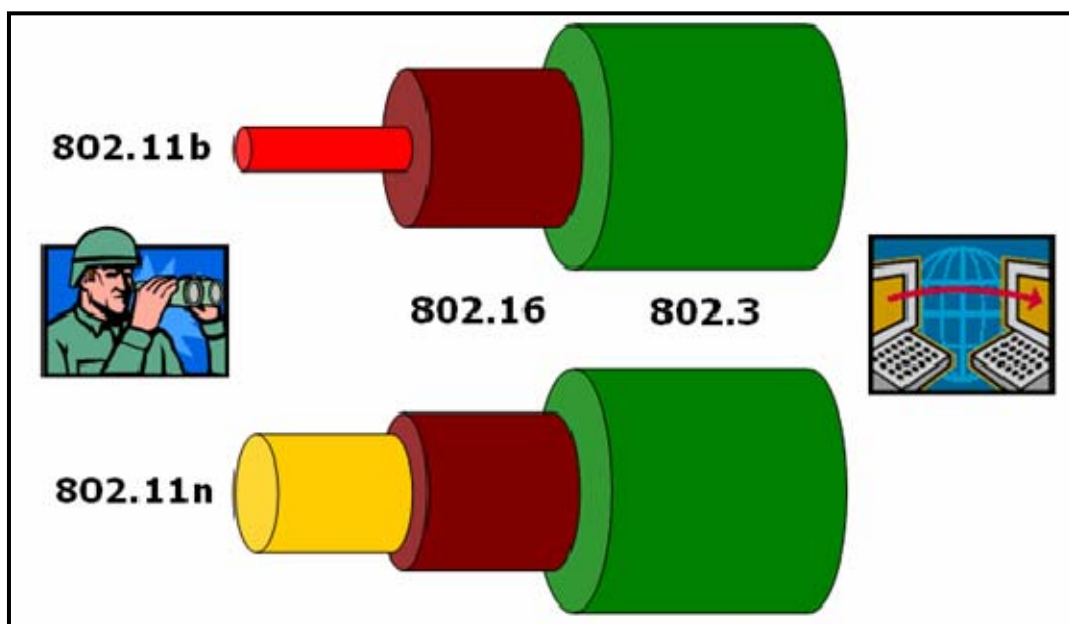


Figure 29. 802.11n and 802.11b End-User to HQ Pipes Comparison

The end-user network is obviously the weak link in the chain. The 802.11n based network more closely matches the throughput capabilities of the other downstream networks and thus reduces the negative effects of the LAN bottleneck. This allows the data to flow more freely. It increases the potential for creating more information which ultimately may become the knowledge required to gain information superiority over an opponent.

Although the Belkin Pre-N router is fairly intuitive to operate and configure, the equipment is only a partial implementation of the emerging 802.11n standard (MOE 3.3). As such, it is not yet an appropriate solution for the COASTS environment. The form factor must be more readily deployable. Particularly, this equipment should be ruggedized and simplified for an expeditious environment. The simplifications should include the internal batteries, the one button instant-on capability, and the multiple access point connections allowed with the BreadCrumb network, but enjoy the MIMO and throughput enhancements promised by the future 802.11n standard. The Belkin Pre-N router fulfils part of the 802.11n promise in terms of high throughput but totally lacks the rugged and simplified aspects of other successfully fielded military equipment.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. RECOMMENDATIONS

The COASTS environment offers an excellent test-bed for evaluating emerging technology. The scenario-driven demonstrations incorporate multiple information technology solutions in a dynamic and coalition enabled manner. This allows for interaction among commercial vendors, coalition governments, coalition militaries, NPS faculty, NPS staff, and NPS students. During the COASTS Demonstrations, the scenarios drive the need for exploring and for expanding LAN, WLAN, and WAN capabilities to include operational use in air, on land, and on sea.

As a technology review, this thesis has considered the proposed IEEE 802.11n standard to transfer larger amounts of data than currently exists in the COASTS WLAN domain. And, primarily, the current state-of-the-art equipment available to enable a High Throughput Tactical Wireless Network for Surveillance and Targeting in a Coalition Environment has been evaluated in detail.

Specific recommendations for enhancing the utility of the WLAN domain during future COASTS Demonstrations fall into two categories: 1) Use the emerging 802.11n standard. 2) Use the IxChariot network evaluation suite.

A. IEEE 802.11n STANDARD

Once the IEEE 802.11n standard is finalized, COASTS should incorporate equipment that conforms to that standard. This advanced standard for high throughput wireless networks has shown great promise and provides superior throughput even in its infant instantiation as the Belkin Pre-N router. The vendor partners of COASTS should be solicited to incorporate this emerging standard into their equipment to receive the benefit of higher throughput across the WLAN. Each 802.11 standard is eventually outdated by its successor. COASTS has an opportunity to remain ahead of the bow wave and should take advantage of it.

B. IXCHARIOT NETWORK EVALUATION SUITE

As the dynamic COASTS network changes, each new iteration should be compared to the previous one in order to measure the effect of altering the network components or structure. In order to make an objective comparison, specific and

consistent metrics must be collected. The IxChariot network evaluation suite offers a robust capability for measuring the salient factors of a network. As such, it is a wonderful tool that can aid in concrete analysis. Using such a tool will define results based on measurable aspects of performance rather than nebulous impressions when the network components and configuration is altered. Further, the IxChariot network evaluation suite is capable of expanding testing into such interesting areas as IPv6 and VoIP, which will be mandated for future DOD networks in the Joint Technical Architecture (JTA 2004, 36).

LIST OF REFERENCES

- 802.11n Work Group. "Status of Project IEEE 802.11n." Available at http://grouper.ieee.org/groups/802/11/Reports/tgn_update.htm accessed 12 August 2005.
- Belkin Corp. *Belkin Wireless Pre-N Router User Manual*. 19 October 2004. Also available from <http://web.belkin.com/support/download/download.asp?download=F5D8230-4&lang=1&mode=m>; accessed 12 August 2005.
- Birdsong, Lynn and Greg Helms. "Visual Universe: Data into Sight." Available from <http://edmall.gsfc.nasa.gov/99invest.Site/VISUALIZATION/visualization.html>; accessed 12 August 2005.
- Central Intelligence Agency. "Thailand." *World Factbook 2005*. Central Intelligence Agency, Office of Public Affairs. Available from <http://www.cia.gov/cia/publications/factbook/geos/th.html>; accessed 12 August 2005.
- Coffey, Sean and others. "WWiSE Overview, Update, and Comparison." Presentation dated 15 November 2004 subsumed by "WWiSE 802.11n Proposal." March 2005. Available from www.wwise.org/11-05-0150-02-000n/WWiSE/proposal/complete/presentation.ppt; accessed 12 August 2005.
- Ehlert, James, Brian Steckler, and Gary Thomason. *Coalition Operating Area Surveillance and Targeting System Project: Concept of Operations*. 9 September 2004.
- Deffree, Suzanne. "802.11n: The Next WLAN Frontier." *Electronic News*. 19 August 2004. Available from <http://www.reed-electronics.com/electronicnews/article/CA445702>; accessed 12 August 2005.
- Gast, Matthew. "A Look at the WWiSE Proposal for 802.11n." *O'Reilly Wireless Devcenter*. 24 October 2004. Available from <http://www.oreillynet.com/pub/wlg/5786>; accessed 12 August 2005.
- IEEE Standards Association. "About the IEEE Standards Association." Available from <http://standards.ieee.org/sa/index.html>; accessed 21 July 2005.
- IXIA. *IxChariot Console Version 5.40 User's Guide*. December 2004.

- Joint Pub 3-07.1: Joint Tactics, Techniques, and Procedures for Foreign Internal Defense (FID)*. 30 April, 2004. Available from <http://www.dtic.mil/doctrine/doctrine.htm>; accessed 12 August 2005.
- Joint Pub 3-07.2: Joint Tactics, Techniques, and Procedures for Antiterrorism*. 17 March 1998. Available from <http://www.dtic.mil/doctrine/doctrine.htm>; accessed 12 August 2005.
- Joint Pub 3-13: Joint Doctrine for Information Operations*. 9 October 1998. Available from <http://www.dtic.mil/doctrine/doctrine.htm>; accessed 12 August 2005.
- Joint Pub 3-40: Joint Doctrine for Combating Weapons of Mass Destruction*. 8 July 2004. Available from <http://www.dtic.mil/doctrine/doctrine.htm>; accessed 12 August 2005.
- Joint Pub 3-55: Doctrine for Reconnaissance, Surveillance, And Target Acquisition Support For Joint Operations (RSTA)*. 14 April 1993. Available from <http://www.dtic.mil/doctrine/doctrine.htm>; accessed 12 August 2005.
- Joint Pub 3-57: Joint Doctrine for Civil-Military Operations*. 8 February 2001. Available from <http://www.dtic.mil/doctrine/doctrine.htm>; accessed 12 August 2005.
- Joint Pub 6-0: Joint Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations*. 30 May 1995. Available from <http://www.dtic.mil/doctrine/doctrine.htm>; accessed 12 August 2005.
- JTA: Joint Technical Architecture Version 6.0, Final*. 3 October 2003. Available from https://disonline.disa.mil/a/DISR/DISR_archives.jsp; accessed 12 August 2005.
- Kaven, Oliver. "Belkin Wireless Pre-N Router." *PCMag.com*. 10 October 2004. Available from <http://www.pcmag.com/article2/0,1895,1668063,00.asp>; accessed 12 August 2005.
- Legg, Gary. "Smart Antennas: A New Boost for Wireless LANs." *TechOnline*. 3 March 2005. Available from http://www.techonline.com/community/tech_group/37714; accessed 12 August 2005.
- MCDP 1 Warfighting*. Washington, D.C.: U.S. Government Printing Office. Also available from <https://www.dctrine.usmc.mil>; accessed 12 August 2005.

Mujtaba, Syed and others. "TGn Sync Complete Proposal." Presentation dated 14 September 2004 subsumed by "TGn Sync Complete Proposal." March 2005. Available from www.tgnsync.org/techdocs/11-04-0888-11-000n-tgnsync-proposal-presentation.ppt; accessed 12 August 2005.

Rubin, Ross. "802.11g Demonstrates White Lies of Wi-Fi." *eWeek.com*. 11 June 2003. Available from <http://www.eweek.com/article2/0,1759,1497868,00.asp>; accessed 12 August 2005.

WikiMedia Foundation, Inc. "IEEE 802.11e" *Wikipedia*. Available from <http://en.wikipedia.org/wiki/802.11e>; accessed 12 August 2005.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Fort Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. Marine Corps Representative
Naval Postgraduate School
Monterey, California
4. Director, Training and Education,
MCCDC, Code C46
Quantico, Virginia
5. Director, Marine Corps Research Center,
MCCDC, Code C40RC
Quantico, Virginia
6. Marine Corps Tactical Systems Support Activity
(Attn: Operations Officer)
Camp Pendleton, California