Generic factors influencing optimal LAN size for commonly used operating systems maximized for network performance

Shaneel Narayan, Deryn Graham and Robert H. Barbour

Department of Computing
Unitec Institute of Technology, Auckland, New Zealand

Summary
Information technology infrastructure is a critical element in modern day communication. Businesses, organizations, individuals, governments and other social services all rely on global IT infrastructure for reliable and timely communication. At the heart of this infrastructure are numerous hardware and software components, and the performance of each individual element contributes to the overall success of the installation. One such software component that is vital for communication is an operating system (software that makes a computer and network work). With enhancements in technology, these operating systems are becoming more and more sophisticated in their functionality, and at least three mainstream vendor products are available in the market. It is common for software vendors to claim that their product out-perform competitors offerings, in functionality and performance.

This paper reviews the literature for a current project that identifies generic factors that influence performance of a LAN. The focus is on both the performance and the metrics of commonly used operating systems implemented to create IT infrastructure. It identifies performance analysis, Internet protocols and wireless as major themes in literature. A number of gaps in the literature, related to network performance analysis, are identified in Section 4 of the paper.

Key words:
Network Performance, Operating Systems, Local Area Networks (LANs), Performance Metrics.

1. Introduction

Networks and operating systems are at the core of the information communication super-highway. They are part of the crucial infrastructure that facilitates communication for all organizations. With enhancements in technology, numbers of operating systems are increasing as well as becoming more and more sophisticated in their functionality. Different vendors endeavor to provide systems that they claim can out-perform those of competitors in functionality and performance when implemented as a stand-alone solution or used to create a Local Area Network (LAN).

A current research project looks at the generic factors that influence LAN size when commonly used operating systems are maximized for network performance. This research requires an investigation of; the metrics which influence network performance, and how, the optimal LAN size for commonly used operating systems, and the performance of networks and operating systems.

This paper details the literature reviewed for the research project.

2. Literature Review

A cross-section of significant literature related to optimal LAN size and the performance evaluation of networks is presented. Highly relevant issues and themes that exist are discussed and conclusions drawn.

2.1 Performance Analysis

Performance analysis/evaluation of networks and operating systems has been undertaken by researchers for various reasons (Table 1). Data obtained from such studies is useful in verifying service level agreements (SLAs), accounting and billing, resource management, planning and designing of networks (Xiangping & Mohapatra, 2002). These services are essential to support business processes. Therefore, network related parameters that can be measured, known as performance metrics, need to be carefully selected when analyzing performance for both effectiveness and efficiency.

The most common metric evident in literature is throughput. Throughput is defined as the rate at which bulk data transfers can be transmitted from one host to another over a sufficiently long time period (Zeadally & Raicu, 2003). It is the number of items per unit time and indicates the amount of data that is sent across from one network host to another (Killelea, n.d.). This measurement is dependent on several network conditions such as processor capabilities, the hardware used and the processes running on the network. This metric is valuable in understanding a

Manuscript received June 5, 2009
Manuscript revised June 20, 2009

network's total performance because it does end-to-end measurement.

Round Trip Time (RTT) denotes the time taken by the packet to travel from the sending network node around all the network nodes and back (Zeadally & Raicu, 2003). This metric depends on several factors such as the nature of medium used to connect nodes, the distance between the sending and the receiving node, and the quantity of traffic on the cables. RTT is one of the metrics that indicates network latency, defined as the time it takes from initiation of a request till data is returned.

The percentage of CPU utilization of nodes in a network is also a valid metric reported in the literature. While it is obvious that the CPU resources will be utilized by other processors running on the node, this metric provides valuable insight into the overheads created by network and operating systems activities.

Author	Date	Title
Rosenblum, Herrod, Witchel and Gupta	1995	Complete computer system simulation: the SimOS approach.
Allman, Ostermann, Kruse, Hayes and Allman	1997	TCP performance over satellite links.
Khalid	1998	Generation of representative traces for performance evaluation of computer architectures.
Floyd and Paxson	2001	Difficulties in simulating the Internet.
Nahum, Barzilai and Kandlur	2002	Performance issues in WWW servers.
Xiangping and Mohapatra	2002	Performance evaluation of service differentiating Internet servers.
Zeadally and Raicu	2003	Evaluating IPv6 on Windows and Solaris.
Edward	2004	Operating system scenarios as use case maps.
Gotsis, Goudos, and Sahalos	2005	A test lab for the performance analysis of TCP over Ethernet LAN on Windows operating system.
Mohamed, Abusin and Chieng	2005	Evaluation of IPv6 and comparative study with different operating systems.
Killelea	n.d.	Web performance tuning.
Narayan, Kolahi, Brooking, de Vere	2008	Performance Evaluation of Virtual Private Network Protocols in Windows 2003 Environment.
Narayan, Kolahi, Brooking, de Vere	2009	Network Performance Analysis of VPN Protocols: An empirical comparison on different operating systems.

Table 1: Performance Evaluation Research

Throughput, round trip time (latency), and CPU utilization are the most common metrics evident in performance analysis literature. Collecting data related to each is challenging, and there is often a tension between realism and reproducibility (Mogul, 1999), that is, real world effects can make it hard to repeat experiments exactly. Scenario descriptions attempt to model replicable IT systems in a laboratory setting. Within particular scenarios three common performance analysis methods are reported in literature.

Firstly, simulation is widely used to provide an environment for exploring real world situations on a computer. It is a constructed and abstract model of the world and as a tool can be either developed by the researcher or may be commercially available. Some examples of tools available in the market are OpNet, x-sim, Network Simulator, REAL, and ns (Allman, Ostermann, Kruse, Hayes, & Allman, 1997). Simulation offers a number of advantages to the researchers as discussed Allman et al., (1997), Floyd and Paxson (2001) and Rosenblum, Herrod, Witchel, and Gupta (1995). Simulations are not equipment intensive and can be used to examine a wide range of scenarios in a relatively small time frame. For example, unusual networks can be tested. With simulated networks output will not be hindered by the physical speed of a given network topology. Complex networks can be created and changes can be easily incorporated into the setup. However, associated with simulations are a number of downsides including; implementation is all researcher-coded and does not include code found in real operating systems, simulations cannot include non-network events like latency, and may be based on assumptions that have shield effects that also hide what may occur in real world.

Secondly, emulation can be used to model particular sections of network path between two real network nodes. Configured as suggested, the environment is a mix of both simulation and a real network (Allman et al., 1997). For example, an emulation environment may have a few real computers that are communicating using real cables, but the router managing traffic may be emulation software. There are a number of studies that have used such environments to gather performance metrics including those of Khalid (1998) and Edward (2004). Emulation allows testing of network equipment and links that may not be too expensive to implement, for example satellite channels. It also allows researchers to easily modify aspects of networks that cannot be changed on a real network due to the implications that the changes may have for the functionality of a real network. On the other hand, emulations are abstract and do not reflect the components of a real network with a real operating system.

Finally, test beds provide an environment to analyze performance of networks and address some of the shortfalls of the other two methods. The test bed method involves using real hosts and network equipment to collect data, so that results will be as close as possible to what would be measured on a real live network.

The results are dependent on the speed and capabilities of the hardware used. Research utilizing a test bed as the platform to gather data is much more expensive than simulation methods. Various aspects of network and operating system performance have been measured using test beds and reported by Gotsis, Goudos and Sahalos (2005); Mohamed, Abusin and Chieng (2005) and Nahum, Barzilai and Kandlur (2002). Collectively, these researchers have analyzed networks that have totally different hardware and physical configurations. Such analyses are difficult to compare in consistent ways.

In summary, performance analysis is the measurement and subsequent examination of quantifiable parameters related to networks and operating systems and known as metrics. The results of performance analyses give an insight into either how an operating performs when compared to other benchmarked values, or how efficiently a network as a whole is able to facilitate communication. Various aspects of an operating system or a network have been performance analyzed (Figure 1) by a number of researchers. These aspects will be discussed next.

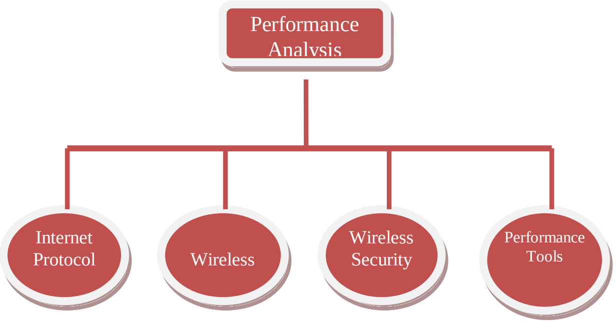


Figure 1: Areas for Performance Analysis

2.2 Internet Protocol

The Internet Protocol (IP) is the basic building block used to enable information technology communication channels the application of which establishes the potential for links between nodes. Improving the performance of the IP stack will increase performance of the overall operating system and the networks on which it is run. IP stack refers to the way IP is implemented in an operating system. Software and hardware vendors are in competition so they continuously evaluate the inner workings of IP with a view to fine tuning its performance on their products. There are two versions of this protocol: IP version 4 (IPv4) and IP version 6 (IPv6).

The Internet Engineering Task Force (IETF) introduced IPv6 with the mission to meet the growing demands of the future Internet (Mohamed, Buhari, & Saleem, 2006). IPv6 is the newer of the two protocols currently being used, and will be the successor of the ageing IPv4. Kaushik (2009) states that the ‘five major areas where IPv6 scores over IPv4 are: addressing and routing, network address translation, administrative workload, security, and support for mobile devices’. One of the major problems with IPv4 is that it has a limited number of addresses (approximately 4.3 billion), but the current global requirements for addresses supersedes that theoretical limit. IPv6 offers the solution by extending the address space from 32 bits (as in IPv4) to 128 bits long allowing for 2^{128} addresses. However, as the number of addresses increase so does the associated overheads (IPv6 has a 40-bit header while IPv4 has a 20-bit header). This increase in header size has major implications for the performance of the newer IPv6.

Draves, Mankin, and Zill (1998) did a throughput evaluation of IPv6 on Windows NT by using two machines running Windows NT which were connected together directly with a cable. This study only focused on throughput and does not mention other parameters such as the influence on performance of different packet size and protocol type. Their study showed that IPv6 had 2.5% less throughput than IPv4 on Ethernet and 1.9% less throughput on Fast Ethernet.

Another effort to evaluate the data transmission performance over the two IP versions using IPSec on FreeBSD platform was conducted by Ariga (2000) and the results showed that the end-to-end TCP and UDP throughput with IPv6 is almost the same as that with IPv4. This study was an improvement over the study by Draves et al., (1998), as it looked into the different protocol types, however it did not research the effect of various packet sizes. Zeadally, Wasseem, and Raicu (2004) compared the two IP versions for Windows 2000, Solaris 8 and Linux Red Hat 7.3 operating systems. They concluded that each operating system would have different throughput behavior in the two versions of IP, however the throughput differences decrease with increasing message sizes (from 1024 bytes onwards).

The impact of IPv6 on Windows 2000 and Solaris was looked at by Zeadally and Raicu (2003), who showed that there is a significant difference in TCP throughput between the two IP versions for message sizes less than 256 bytes with IPv4 having three times higher throughput for Solaris. Gotsis et al., (2005) extended this study and found that IPv4 outperforms IPv6 in terms of TCP performance, and that UDP shows better performance than TCP on Windows 95/98/NT/2000 operating systems.

Further, Mohamed et al., (2005) found that Red Hat 9 performed better with IPv6 than Windows 2003. Sanguankotchakorn and Somrobru (2005) suggested that it will take time to change from IPv4 to IPv6 and therefore in the transition there will be networks that will have both

Internet Protocol versions together. They found that when the traffic density of IPv6 sessions increases, the bandwidth of the IPv6 session increases at the expense of the bandwidth of the IPv4 session. Further, the study showed that IPv4 and IPv6 tend to behave differently when packet size and other parameters are changed. Research related to Internet Protocol performance is summarized in Table 2.

Author	Date	Title
Draves, Mankin and Zill	1998	Implementing IPv6 for Windows NT.
Zeadally and Raicu	2003	Evaluating IPv6 on Windows and Solaris.
Zeadally, Wasseem and Raicu	2004	Comparison of end-system IPv6 protocol stacks.
Gotsis, Goudos and Sahalos	2005	A test lab for the performance analysis of TCP over Ethernet LAN on windows operating system.
Mohamed, Abusin and Chieng	2005	Evaluation of IPv6 and comparative study with different operating systems.
Sanguankotchakorn and Somrobru	2005	Performance evaluation of IPv6/IPv4 deployment over dedicated data links.
Mohamed, Buhari and Saleem	2006	Performance comparison of packet transmission over IPv6 network on different platforms.
Narayan, Kolahi, Reid, Waiariki	2007	Performance Analysis of Network Operating Systems.
Narayan, Kolahi, Suranto, Nguyen, Mani	2008a	Performance Comparison of IPv4 and IPv6 on Various Windows Operating Systems.
Narayan, Shang, Fan	2009a	Performance Evaluation of IPv4 and IPv6 on Windows Vista and Linux Ubuntu.
Narayan, Shang, Fan	2009b	Network Performance Evaluation of Internet Protocols IPv4 and IPv6 on Operating Systems.

Table 2: Internet Protocol Research

2.3 Wireless Performance

Wireless Local Area Networks (WLANs) have recently gained popularity because of the advantages offered to users. Computers in a conventional LAN are restricted to a location while WLAN clients have the advantage of increased flexibility and mobility due to the nature of the medium that it uses for communication. With increased usage and popularity, the concern for users about security and performance also increases. These security concerns point to the necessity for recognizing the effects on the performance of different security mechanisms, and the effects of numbers of nodes in networks.

Baghaei and Hunt (2004) have studied the impact of multiple clients on IEEE 802.11 wireless LAN Security performance. This study was carried out on Windows XP and Windows 2000 servers and they used IP traffic as the monitoring tool. The results of this study showed that when the encryption mechanism was added, the performance was negatively affected and the authors concluded that the overheads produced by encrypting each individual packet in congested networks are significantly higher than in an un-congested network. The results also show that throughput of the TCP protocol is significantly lower than the UDP protocol in congested networks, especially when using WEP (Wired Equivalent Privacy) encryption. Vasan and Shankar (2003) extended this study by measuring throughput of 14 wireless clients associated with one access point. They concluded that an increase in the number of nodes will result in decreased throughput. Bing and Subramanian (1997) compared performance of two commercial WLANs using file transfer as the performance metric. They concluded that the type of addressing and the size of an Ethernet frame (data packet size on a wire) are the crucial factors in determining the performance of WLAN transmission. More specifically, WLAN performance increases as Ethernet frame length increases.

The popularity of WLANs is growing rapidly but since they use air as the medium for communication, security implications are significant. Users are aware that security can be easily breached, so multiple security encryption techniques have been created so communication pathways can be offered that maintain confidentiality, integrity and authenticity of the transmitted data. Obviously, as security protocols are implemented with various levels of complexity, the protocols use more resources and that, in turn, affects performance.

There are a number of security protocols that are being used to secure WLANs. WEP has been the security standard for 802.11 networks since 1999, but has many security shortfalls. It is susceptible to a number of attacks including bit-flipping, replay, weak key and forgery attacks (Srinivasan & Michell, 2004). Wireless Fidelity [Wi-Fi] Protected Access (WPA) version 1 addresses some of the shortfalls of WEP, however it is hard to maintain, has extensive processing overheads and is not suitable for battery-operated devices due to resource requirements. WPA2 is the newest of all security protocols for WLANs and provides the highest level of WLAN security that can be attained with the current limitations of technology.

Baghaei and Hunt (2004) researched the impact of different wireless security protocols by measuring network performance for TCP and UDP in the different security levels. The results of their study showed that when each encryption mechanism was added, performance was negatively affected on Windows XP and Server 2000. They concluded that the overheads produced by encrypting each individual packet in congested networks with multiple nodes, are significantly higher than in an un-congested network with one client node. Athanasopoulos et al., (2006) conducted simulations to compare the performance of 802.11b and 802.11g in terms of throughput, bandwidth utilization and media access delay: They concluded that the network capacity in terms of bandwidth utilization is higher when 802.11g was used, and the difference between two standard protocols in terms of network utilization was approximately 20%.

A study undertaken by Leon, Aldeco, and Merino (2005) evaluated the performance of various encryption algorithms to estimate the trade-off between level of security attained and the change in performance. The paper presents some reported vulnerabilities of security protocols and proposes implementation of other cryptosystems using symmetric and asymmetric keys. It concludes that symmetric cryptosystems are more efficient than asymmetric counterparts on a network that has been implemented to maintain confidentiality. Leon et al., (2005) also suggest that different results will be attained if authenticity (and not confidentiality) is the goal of the network designer. Key wireless research papers are summarized in Table 3.

Author	Date	Title
Bing and Subramanian	1997	A novel technique for quantitative performance evaluation of wireless local area networks.
Vasan and Shankar	2003	An empirical characterization of instantaneous throughput in 802.11b WLANs.
Baghaei and Hunt	2004	IEEE 802.11 wireless LAN security performance using multiple clients.
Srinivasan and Michell	2004	Performance of state based key hop (SBKH) protocol for security on wireless networks.
Leon, Aldeco, and Merino	2005	Performance analysis of the confidentiality security service in the IEEE 802.11 using WEP, AES-CCM, and ECC.
Athanasopoulos, Topalis, Antonopoulos, and Koubias	2006	Evaluation Analysis of the Performance of IEEE 802.11b and IEEE 802.11g Standards.
Kolahi, Narayan, Sunarto, Nguyen, Mani	2008	The Impact of Wireless 802.11g LAN Encryption Techniques on Performance of Different Windows Operating Systems.
Narayan, Kolahi, Sunarto, Nguyen, Mani	2008b	The Influence of Wireless 802.11g LAN Encryption Methods on Throughput and Round Trip Time for Various Windows Operating Systems.
Narayan, Feng, Xu, Ardham	2009	Network Performance Evaluation of Wireless IEEE802.11n Encryption Methods on Windows Vista and Windows Server 2008 Operating Systems.

Table 3: Wireless Performance Research

2.4 Performance Measuring Tools

Network performance tools are commonly employed when undertaking performance analysis of networks and operating systems. The choice of the actual tool depends on the way in which data will be collected (simulation, emulation or a test bed), the operating system being tested, the network topology, and the performance metric(s) being measured. In this section, four common tools evident in literature (Table 4) are discussed.

2.4.1 IPerf

Iperf is a performance analysis tool that was originally developed by the Distributed Applications Support Team (DAST) (Tirumala, Qin, Dugan, Ferguson, & Gibbs, n.d.). The sole purpose in developing this tool was to provide support for researchers working with high-performance network applications and to assist with the development of high-performance network applications and tools. At the core of Iperf is a client/server model that operates using command lines. This tool runs on both Linux and Windows platforms with the same command options. Java applets have been developed by a number of software developers, thus providing a GUI interface to the program (Lattner, Cook, & Gibbs, n.d.).

The current version of Iperf is 1.7.0 and is designed to work with both IPv4 and IPv6. Iperf is a shareware programme and can be used at no cost. Thus, a number of researchers employ this as the primary tool for performance analysis. For example, Agarwal and Wang (2005) used it to analyse the impact of security protocols on WLANs, and Wu, Chao, Tsuei, and Li (2005) utilized it to measure network efficiency of TWAREN IPv6 backbone.

2.4.2 Netperf

Netperf is another benchmarking tool that can be used to measure the performance of many different types of networks and it provides tests for both unidirectional throughput and end-to-end latency. It was originally developed by Hewlett-Packard for its clients (Jones, n.d). Like Iperf, Netperf can be used for both TCP and UDP in either IPv4 or IPv6. This tool also can be run on multiple platforms, such as UNIX (all the major variants), Linux, and Windows operating systems, with two separate executable files: one for server side and the other for client side.

Netperf has been used by other researchers, for example Gotsis et al., (2005) used Netperf to analyse the TCP performance over the Ethernet LAN on Windows operating system, and Agarwal, Gill, and Wenye, (2004) studied the wireless security protocol over a mobile IP network by using Netperf. Zeadally et al., (2004) also used Netperf for research into the end-to-end IPv6 protocol stack.

2.4.3 D-ITG

Distributed Internet Traffic Generator or D-ITG was developed by Universita' degli Studi di Napoli (Italy). Avallon et al, (2004) carried out several experiments to compare the product to other widely used traffic generators: Mtools, Rude & Crude (Laine, Saaristo, & Prior, n.d.), MGEN (Naval Research Laboratory, n.d.) and Iperf. In all respects, it has been found the researchers listed above that D-ITG provided network analysis results that are the closest to what one can get if using a real live network.

Similar to IPerf and Netperf, D-ITG is a command line tool and requires two separate component calls: ITG-Send and ITG-Receive (Avallone et al., 2004). An innovative feature of D-ITG is that it allows information to be sent from both the sender and receiver nodes. Additionally, DITG enables the sender and the receiver to delegate the logging operation to a remote log server. D-ITG is currently available on Linux, Windows and Linux Familiar platforms and is a freeware performance tool. There is a GUI version of D-ITG which was built by (Semken, n.d.).

Several other researchers have also used D-ITG. For example, a study of IP traffic over television interactive data casting systems was undertaken by Wei, Hong, and Gagnon (2005). Voice performance on single radio multi hop IEEE 802.11b systems with chain topology was researched by Kee, Yin, and Moh, (2005), and Nandivada and Palsberg (2005) analyzed timing of TCP servers for surviving denial-of-service attacks.

2.4.4 IP Traffic

IP Traffic (ZTI Telecom) is commercial software developed by ZTI-Telecom in France. It is a connection and data generation tool for IP networks. Data flows using TCP, UDP or ICMP (Internet Control Message Protocol) protocols can be analyzed with IP Traffic. IP Traffic has a graphical interface and works only on Microsoft platforms such as Windows 98, Windows XP, and Windows 2003, but not for Windows Vista. Unlike the other three tools above, this performance analysis software is a commercial product. Baghaei and Hunt (2004) have used IP Traffic to study the impact of different wireless security on network performance, and Ezedin et al., (2006) have researched the impact of encryption on the throughput of WLAN IEEE 802.11g using IP Traffic. A summary of the key features of the four network performance tools is presented below in Table 4. Research papers related to Network Performance Tools are listed in Table 5.

	Iperf	**Netperf**	**D-ITG**	**IP Traffic**
Interface	Command line	Command line	Command line	GUI interface
Multi-platform	Yes	Yes	Yes	Windows only
User guide	Yes	Yes	Yes	Yes
Protocols	TCP and UDP	TCP and UDP	TCP, UDP, ICMP, DNS, Telnet, and VoIP	TCP, UDP and IGMP
Packet departure Packet delay	No	No	Yes	Yes
Probability distributions	No	No	Yes	Yes
Log file	Yes	Yes	Yes	Yes
Internet Protocol	IPv6 and IPv4	IPv6 and IPv4	IPv6 and IPv4	IPv6 and IPv4
Measurements metrics	Jitter Packet loss Throughput	Jitter Packet loss Throughput	One-way-delay Round-trip-time Packet loss Jitter Throughput	Throughput Round trip time Packet loss Jitters

Table 4: Key features of the four tools

Author	**Date**	**Title**
Baghaei and Hunt	2004	IEEE 802.11 wireless LAN security performance using multiple clients.
Avallone, Guadagno, Emma, Pescape and Ventre	2004	D-ITG distributed Internet traffic generator.
Agarwal, Gill and Wenye	2004	An experimental study on wireless security protocols over mobile IP networks.
Zeadally, Wasseem and Raicu	2004	Comparison of end-system IPv6 protocol stacks.
Agarwal and Wang	2005	Measuring performance impact of security protocols in wireless local area networks.
Wu, Chao, Tsuei and Li	2005	A measurement study of network efficiency for TWAREN IPv6 backbone.
Kee, Yin and Moh	2005	Voice performance study on single radio multihop IEEE 802.11b systems with chain topology.
Wei, Hong and Gagnon	2005	Performance assessment of IP traffic over ATSC interactive datacasting.
Ezedin, Mohammed, Amal, Hanadi, Huda and Meera	2006	Impact of security on the performance of wireless-Local Area Networks
Nandivada and Palsberg	2005	Timing analysis of TCP servers for surviving denial-of-service attacks

Table 5: Network Performance Research

3. Findings

Performance analysis of networks has been a subject of interest to researchers since the early days of computer networks and operating systems. As information technology has progressed and evolved over the years, the study of performance analysis has continually changed from single user operating systems to identifying and analyzing the implications of implementing newer and improved aspects of entire infrastructures. There is a solid body of literature available on the topic, spanning a number of major themes.

Firstly, there is substantial research into defining and operationalizing performance analysis and identifying the measurable variables. There seems to be no agreement on what values should be measured and how data from one network can be benchmarked for comparison with data from a dissimilar network. This situation is evident in the literature, since researchers report using different metrics on networks and operating systems, when in fact a better understanding of network performance may be attained if the same parameters are measured by the same tools. Throughput is definitely the core metric in the majority of the research; however there is no agreement on what other network measurements should be standard.

Secondly, the basic building block for communication (Internet Protocol) has been of interest to a number of researchers. IP is complicated and its implementations on different networks lead to different performance behaviors. IP is at the core of any modern network (peer-to-peer or client/server), and is necessary on networks that communicate on the Internet. IP is a major research area because global information technology is on the verge of changing from IPv4 to IPv6. The underpinning architecture of IPv6 is completely different to that of IPv4. It follows, therefore, that there are many issues that can be researched into the consequences for performance and other aspects of the changes.

Thirdly, there are numerous publications on the wireless networks/protocols with associated variations. This technology is widely used by both business and domestic consumers and its popularity is growing rapidly. Because of the nature of technology, wireless security can easily be compromised. For this reason, there are a number of new advances being made in the area of improving wireless security, and consequently these changes are seen as a window of opportunity by performance analysis researchers. One of the fundamental methods of enhancing WLAN security, is to increase the length of the secret key used in the encryption protocol. However, as security is enhanced, there are implications on the performance of the network and the operating systems. Examination of how security enhancements affect performance has been a popular research area.

4. Gaps in the Research

The evolving nature of information technology implies that performance analysis will remain an area of research that will not be short of challenges for researchers. Looking at the current literature, there is definitely a gap in research related to standardizing performance metrics. By standardizing metrics, results from various networks can be sensibly compared to give a better understanding of performance-related issues. Secondly, there is little research into why different network performance tools produce results that vary when used on networks and operating systems that are configured similarly. This variance in results is a major concern because performance analysis results gathered using different tools do produce different results. Thirdly, there is no literature that compares data from similar network set-ups collected using different methods (simulation, emulation and test beds).

There are a number of technological developments that, either have been introduced recently, or will definitely be introduced in the near future. They will all open further avenues of research in performance analysis. Some of these technological enhancements are:

- Release of new operating systems (Microsoft Windows Vista was introduced in February 2007, Microsoft Server 2008 range has just been released, Microsoft Windows 7 in October 2009 and new Linux versions and distributions are released regularly).
- Introduction of new security protocols (for example, WPA2 was introduced in late 2006, however, there is no sign yet of research related to it).
- IPv6 on a wireless network (currently there are no wireless devices compatible with IPv6).

To date, little has been published about these enhancements. Each is challenging in its own right, and is a valid area of research. Further areas of research will arise when one technological enhancement is interoperated with another. For example, implementing WPA2 or IPv6 in a Microsoft Server 2008 environment may have implications for performance.

5. Summary

The literature search has identified several gaps for further research. The proposed research will involve setting up test beds in a laboratory representing computer networks using different software and topologies. Scenario, representing typical configurations will be created to test IT systems. Data will be collected (using performance measurement tools) for each implemented scenario and analyzed to make generalizations regarding optimal LAN size of common operating systems. This research will contribute knowledge in the field of LAN and operating system performance analysis. Performance analysis information about both networks and operating systems is crucial for designing a network infrastructure for an organization. Efficient networks boost productivity and reduce the total cost of ownership, therefore establishing common metrics, comparison relationships and size relationships will contribute to:

- choosing the best operating system for an organization based on verifiable performance.
- deciding what can be tweaked in an operating system to optimize network performance on a particular network.
- selecting optimal size of LAN that does not degrade performance on a particular network.

This research will extend the work already reported on optimal LAN size and performance analysis of networks. The results will provide a foundation for future work in this area. It is anticipated that the generalizations made about optimal LAN size and network performance analysis will open avenues for future research into application data exchange that is the basis for Service Orientated Architectures.

References

[1] Agarwal, A. K., Gill, J. S., & Wenye, W. (2004). *An experimental study on wireless security protocols over mobile IP networks.* Paper presented at the 60th IEEE Vehicular Technology Conference, VTC2004-Fall.

[2] Agarwal, A. K., & Wang, W. (2005). *Measuring performance impact of security protocols in wireless local area networks.* Paper presented at the 2nd International Conference on Broadband Networks.

[3] Ariga, S. (2000). Performance Evaluation of Data Transmission Using IPSec over IPv6 Networks. Paper presented at the 10 Annual Internet Society Conference (INET2000).

[4] Allman, M., Ostermann, S., Kruse, H., Hayes, C., & Allman, R. (1997). *TCP Performance Over Satellite Links*. Proceedings of the 5th International Conference on Telecommunication Systems.

[5] Athanasopoulos, A., Topalis, E., Antonopoulos, C., & Koubias, S. (2006). *Evaluation Analysis of the Performance of IEEE 802.11b and IEEE 802.11g Standards.* Paper presented at the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, ICN/ICONS/MCL 2006.

[6] Avallone, S., Guadagno, S., Emma, D., Pescape, A., & Ventre, G. (2004). *D-ITG distributed Internet traffic generator.* Paper presented at the First International Conference on the Quantitative Evaluation of Systems.

[7] Baghaei, N., & Hunt, R. (2004). *IEEE 802.11 wireless LAN security performance using multiple clients.* Paper presented at the 12th IEEE International Conference on Networks.

[8] Bing, B., & Subramanian, R. (1997). *A novel technique for quantitative performance evaluation of wireless local area networks.* Paper presented at the 8th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications 'Waves of the Year 2000'. PIMRC '97.

[9] Draves, R. P., Mankin, A., & Zill, B. D. (1998). *Implementing IPv6 for Windows NT.* Paper presented at the 2nd USENIX Windows NT Symposium, Seattle, Washington.

[10] Edward, A. B. (2004). *Operating system scenarios as Use Case Maps.* Proceedings of the 4th international workshop on Software and performance. doi:http://doi.acm.org/10.1145/974044.974087

[11] Ezedin, B., Mohammed, B., Amal, A., Hanadi Al, S., Huda, K., & Meera Al, M. (2006). Impact *of Security on the Performance of Wireless-Local Area Networks*. Paper presented at the Innovations in Information Technology.

[12] Floyd, S., & Paxson, V. (2001). *Difficulties in simulating the Internet.* IEEE/ACM Transactions on Networking, 9(4), 392-403.

[13] Gotsis, K. A., Goudos, S. K., & Sahalos, J. N. (2005). *A test lab for the performance analysis of TCP over ethernet LAN on windows operating system.* IEEE Transactions on Education, 48(2), 318-328.

[14] Jones, R. *Netperf 2.4.3.* Retrieved 1 October 2008 from http://www.netperf.org/netperf/

[15] Kee, N. T., Yin, F. K., & Moh, L. S. (2005). *Voice performance study on single radio multihop IEEE 802.11b systems with chain topology*. Paper presented at the 13th IEEE International Conference on Networks. Jointly held with the IEEE 7th Malaysia International Conference on Communication.

[16] Kaushik (2009) *E-Commerce with IPv6.* Retrieved 15 June 2009 from http://www.ipv6.com/articles/mobile/Mobile-Ecommerce-with-IPv6.htm

[17] Khalid, H. (1998). *Generation of representative traces for performance evaluation of computer architectures.* Paper presented at the IEEE International Performance, Computing and Communications, IPCCC '98

[18] Killelea, P. *Web Performance Tuning.* Retrieved 1 June 2009 from http://www.amazon.ca/Web-Performance-Tuning-Patrick-Killelea/dp/product-description/059600172X

[19] Kolahi, S., Narayan, S., Sunarto, Y., Nguyen, D., & Mani, P. (2008). *The Impact of Wireless 802.11g LAN Encryption Techniques on Performance of Different Windows Operating Systems.* Paper presented at the 13th IEEE Symposium on Computers and Communications, July 6-9. Marrakech.

[20] Laine, J., Saaristo, S., & Prior, R. *Rude & crude*. Retrieved 1 November 2008 from http://rude.sourceforge.net/

[21] Lattner, T., Cook, D., & Gibbs, K. Jperf. Retrieved 1 November, from http://dast.nlanr.net/projects/jperf/

[22] Leon, M., Aldeco, R., & Merino, S. (2005). *Performance analysis of the confidentiality security service in the IEEE 802.11 using WEP, AES-CCM, and ECC.* Paper presented at the The 2nd International Conference on Electrical and Electronics Engineering.

[23] Mogul, J. C. (1999). *Brittle metrics in operating systems research*. Paper presented at the Hot Topics in Operating Systems, 1999. Proceedings of the Seventh Workshop on.

[24] Mohamed, S. S., Abusin, A. Y. M., & Chieng, D. (2005). *Evaluation of IPv6 and comparative study with different operating systems.* Paper presented at the Information Technology and Applications, 2005. ICITA 2005. Third International Conference on.

[25] Mohamed, S. S., Buhari, M. S., & Saleem, H. (2006). *Performance comparison of packet transmission over IPv6 network on different platforms*. Proceedings of the IEE transactions on Communications, 153(3), 425-433.

[26] Nahum, E., Barzilai, T., & Kandlur, D. D. (2002). *Performance issues in WWW servers.* IEEE/ACM Transactions on Networking, 10(1), 2-11.

[27] Nandivada, K. V., & Palsberg, J. (2005). *Timing analysis of TCP servers for surviving denial-of-service attacks.* Paper presented at the 11th IEEE, Real Time and Embedded Technology and Applications Symposium, RTAS

[28] Narayan, S., Kolahi, S., Reid, M., & Waiariki, R. (2007). *Performance Analysis of Network Operating Systems*. Paper presented at the 6th World Scientific and Engineering Academy and Society (WSEAS) Conference on Information Security and Privacy, 14-16 December, Tenerife. Proceedings of the 2nd WSEAS Conference on Computer Engineering and Applications, pp 186-189, Acapulco: WSEAS Press.

[29] Narayan, S., Kolahi, S., Brooking, K., de Vere, S. (2008). *Performance Evaluation of Virtual Private Network Protocols in Windows 2003 Environment.* Paper presented to the IEEE International Conference on Advanced Computer Theory and Engineering (ICACTE), 20-22 December, Phuket.

[30] Narayan, S., Kolahi, S., Sunarto, Y., Nguyen, D., Mani, P. (2008a). *Performance Comparison of IPv4 and IPv6 on Various Windows Operating Systems.* Paper presented to the 11th IEEE International Conference on Computer and Information Technology (ICCIT), 25-27 December, Khulna.

[31] Narayan, S., Kolahi, S., Sunarto, Y., Nguyen, D., & Mani, P. (2008b). *The Influence of Wireless 802.11g LAN Encryption Methods on Throughput and Round Trip Time for Various Windows Operating Systems.* Proceedings of 6th IEEE Conference on Communication Networks and Services Research Conference (CNSR) 171–175. Halifax.

[32] Narayan, S., Feng, T., Xu, X., Ardham S. (2009). *Network Performance Evaluation of Wireless IEEE802.11n Encryption Methods on Windows Vista and Windows Server 2008 Operating Systems*. Presented at the 6th IEEE International Conference on Wireless and Optical Communications Networks (WOCN), April 28-30, Cairo.

[33] Narayan, S., Shang, P., Fan, N. (2009a). *Performance Evaluation of IPv4 and IPv6 on Windows Vista and Linux Ubuntu.* Presented at the IEEE International Conference on Networks Security, Wireless Communications and Trusted Computing (NSWCTC), April 25-26, Wuhan.

[34] Narayan, S., Shang, P., Fan, N. (2009b). Network Performance Evaluation of Internet Protocols IPv4 and IPv6 on Operating Systems. Presented at the 6th IEEE International Conference on Wireless and Optical Communications Networks (WOCN), April 28-30, Cairo.

[35] Narayan, S., Kolahi, S., Brooking, K., de Vere, S. (2009). *Network Performance Analysis of VPN Protocols: An empirical comparison on different operating systems.* Presented at the IEEE International Conference on Networks Security, Wireless Communications and Trusted Computing (NSWCTC), April 25-26, Wuhan.

[36] Naval Research Laboratory. *Multi-Generator (MGEN).* Retrieved 1 Nov, from http://cs.itd.nrl.navy.mil/work/mgen/index.php

[37] Rosenblum, M., Herrod, S. A., Witchel, E., & Gupta, A. (1995). *Complete computer system simulation: the SimOS approach.* IEEE Parallel & Distributed Technology: Systems & Applications, 3(4), 34-43.

[38] Sanguankotchakorn, T., & Somrobru, M. (2005). *Performance Evaluation of IPv6/IPv4 Deployment over Dedicated Data Links.* Paper presented at the Fifth International Conference on Information, Communications and Signal Processing.

[39] Semken, V. *Graphical user interface for D-ITG 2.4.* Retrieved 5 November, from http://www.semken.com/projekte/index.html

[40] Srinivasan, K., & Michell, S. (2004). *Performance of state based key hop (SBKH) protocol for security on wireless networks.* Paper presented at the IEEE 60thVehicular Technology Conference, 2004. VTC2004-Fall.

[41] Straub, D., Gefen, D., and Boudreau, M.-C.(2004). *The ISWorld Quantitative, Positivist Research Methods Website.* Retreived 3 March 2009 from http://dstraub.cis.gsu.edu:88/quant/

[42] Tirumala, A., Qin, F., Dugan, J., Ferguson, J., & Gibbs, K. *Iperf.* Retrieved 1 December, from http://dast.nlanr.net/Projects/Iperf/

[43] Vasan, A., & Shankar, A. U. (2003). An empirical characterization of instantaneous throughput in 802.11b WLANs. Technical Report, CS-TR-4389.

[44] Wei, L., Hong, L., & Gagnon, G. (2005). *Performance assessment of IP traffic over ATSC interactive datacasting systems.* IEEE Transactions on Consumer Electronics, 51(1), 54-62.

[45] Wu, T.-Y., Chao, H.-C., Tsuei, T.-G., & Li, Y.-F. (2005). *A measurement study of network efficiency for TWAREN IPv6 backbone*. International Journal of Network Management, 15(6), 411-419. http://dx.doi.org/10.1002/nem.582

[46] Xiangping, C., & Mohapatra, P. (2002). *Performance evaluation of service differentiating Internet servers.* Transactions on Computers, 51(11), 1368-1375.

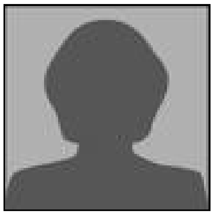
[47] Zeadally, S., & Raicu, L. (2003). *Evaluating IPv6 on Windows and Solaris.* IEEE Internet Computing, 7(3), 51-57.

[48] Zeadally, S., Wasseem, R., & Raicu, I. (2004). *Comparison of end-system IPv6 protocol stacks.* Proceedings IEE Communications, 151(3), 238-242.

[49] ZTI Telecom. *IP Traffic - test & measure.* Retrieved 20 November 2008 from http://www.zti-telecom.com

About the Authors

Shaneel Narayan is currently a lecturer and a doctoral candidate at Unitec Institute of Technology in Auckland, New Zealand. He holds a Bachelor of Engineering and a Masters in Management. Shaneel's current teaching and research interests are mostly in computer network management, data security, network and operating system performance, and performance metrics identification.



Deryn Graham is currently an Associate Professor at the School of Computing, Unitec Institute of Technology, New Zealand, and a Visiting Fellow at the School of Computing and Mathematical Sciences, University of Greenwich, UK. Dr Graham's teaching and research interests are in diverse application areas of Computer Science and Artificial Intelligence; Modelling, Networks, Information Visualisation, e-Learning, and Interaction Design, in which she has both published and held grants.

Robert Barbour has degrees in Social Science and an interdisciplinary DPhil that involved building a computer-based learning environment in which to test Pask's Conversation Theory. A career educator, he has taught at all levels of education, and is currently teaching and supervising research in a professional doctorate program in Computing. His research interests span the use of computing applications in areas such as performance metrics for networked augmented-reality simulation systems, advanced driver education, cellular automata, four-valued logic and post-graduate pedagogies.