Notice: *The technologies discusses in this report may be significantly different by the time you read this. Please note that this document was written in November 2003.*

BLUE CHIP
TOTAL SYSTEMS SUPPORT

Industrial Training Report

Blue Chip Customer Engineering Lanka (Pvt) Ltd.

From
19th May 2003 to 31st October 2003

Report Submitted by

H. M. N. D. Bandara

00/ED/GI/035

Department of Computer Science & Engineering

Faculty of Engineering

University of Moratuwa

Sri Lanka

Important

Blue Chip Customer Engineering Lanka (Pvt) Ltd is concerned on making sure that none of the content in this report is used to gain any commercial advantage or misuse, other than academic evaluation or any other academic activity.

Acknowledgment

It is a grate pleasure for me to acknowledge the assistance and contributions of all the people who helped me to make my industrial training a success. My training would not have been so successful, without the dedicated assistance given by those individuals.

I would like to give my special thanks to Mr. Mahinda Weerasooriya (Blue Chip Customer Engineering Lanka (Pvt) Ltd), Dr. N A Wijeywickrama (Head of Industrial Training Division – University of Moratuwa) and all the officials of Industrial Training Division and NAITA for placing me at Blue Chip.

I would also like to thank Mr. Shantha Fernando (coordinator for training) Dr. Ashoke Peris, Mrs. Vishaka Nanayakkara and all other Officials of Department of Computer Science and Engineering for the assistance and guidance they given towards this program.

In Blue Chip, I would like to thank my managers, Mr. Kirthi Gunawardane (Head of Engineering Fields and Projects) and Mr. Dhmmika Kapukotuwa (Manager Technical and Projects) for coordination and conducting of events. For their extensive support I would also like to thank Mr. Janaka Gamage, Mr. Vishwantha Welikala, Mr. Ajith Liyanage and Mr. Tikiri Guonetilake for providing necessary facilities, equipments and sharing their knowledge with me.

I must also thank Mr. Udaya Jayasooriya (Accountant) for coordinating the administrative tasks related to my training at Blue Chip and being open minded to hear my observations on Blue chip as a third person.

Finally I would like to thank every individual (who I have not mentioned names above) who gave me even the slightest support (even by words) to make my Industrial training a success.

Thank you every one!

Preface

"There is a difference between knowing the path…and walking the path - Morpheus"

"Engineering graduates are highly competent with their technical skills, but they lack the practical exposure, managerial skills, attitude and interpersonal skills, when they first step in to the industry" – this is a very common phrase within the industry.

The primary objective of industrial training program is to overcome such problems faced by a graduate, and to build up a sound appreciation and understanding of the theoretical principles learnt as an undergraduate, by exposing them to the industrial environment while being an undergraduate. It is oriented towards developing the skills, knowledge and attitudes needed to make an effective start as a member of the engineering profession.

This report presents a brief presentation on gained; technical know-how, experiences, customer interaction, challenges, achievements and failures during my Industrial training. I was placed at Blue Chip Customer Engineering Lanka (Pvt) Ltd, for duration of 24 weeks commencing from 19th May 2003.

I am highly satisfied with the training experience I had, the risk I took perfectly paid at the end. It was a risk, selecting such a training organization because I was the first person to visit Blue Chip as an Engineering trainee, and no one had any idea on what is Blue Chip and what they really do.

It was a difficulty task deciding on what topics to be present in this report and what to be eliminated. I was exposed to whole lot of new technologies and devices that I did not cover during my last few semesters. This report presents detailed explanation only on products and underline technologies that was novel to me. Therefore I feel that I must start those topics in a bit lower level, like explaining all the required keywords before they are used in the rest of this chapter. Again it was difficult to priorities sub chapters on what extent to write because there was whole lot of concepts.

This report is organized in to several chapters which begin with an Introduction to the training organization. Chapter 2 is a brief summery of my training exposure. Next several chapters briefly present some of the theoretical concepts, equipments, there capacities and configurations of the products that I worked with. These chapters cover; Midrange Servers (chapter 3), Network Security aspects (chapter 4) and Wireless networking (chapter 5).

Finally there is a conclusion, which discuss about the training exposure, organizations ability to provide good training, current training program, improvements and few other issues.

Abbreviations explain most of the acronyms being used through the entire report. References include lists of references that helped me during my training and writing this report. Few new references are added for additional reading. In certain section of the report you me see open and closed square brackets (e.g. [2.5]) with a number. This number indicates particular reference (given under References) that reader could refer for more details.

Table of Contents

Figures

Tables

1

Blue Chip Customer Engineering Lanka (Pvt) Ltd

"total systems support"

1.1 Introduction

Blue Chip Customer Engineering Lanka (Pvt) Ltd is a total solution provider, who has developed a comprehensive and integrated nationwide service especially to the mid-range computer industry.

Blue Chip Customer Engineering was founded by ex-IBM Engineering staff in 1987, and are specialists in the maintenance and the support of IBM mid-range computers, peripherals and other related equipment.

The company attributes continued success and growth to a steadfast and dedicated approach to mid-range service and support as applied to the IBM e-Server i-Series (formally AS/400), RS6000 and S3X product groups.

Blue Chip head-office is located in Bedford, England, where the company has invested heavily in the infrastructure necessary to ensure complete support and to provide extended support for customers in the United Kingdom and for fully autonomous operations in Ireland, Scotland, Portugal and Sri Lanka.

1.2 Bit of History

Around 1995 Blue Chip UK (head office) and East-West Marketing (Sri Lanka) established a BOI approved company called ASIA 400. It was necessary to have a local partner in order to register a company in Sri Lanka, so East-West Marketing was selected and given 45% of the shares.

Under ASIA 400, Blue Chip Customer Engineering Lanka (Pvt) Limited was established in 1995 as a company which import used Computers (mainly PCs), refurbish them and export to the international market. Later in 1998 East-West sold all of their shares back to Blue Chip UK. Today ASIS 400 is the holding partner of Blue Chip Sri Lanka, and ASIA 400 is fully owned by Blue Chip UK.

Although it was established only to refurbish computers later other areas like maintaining PBXs, Mid-Range Servers, ATM machines, larger scale printers, electronic repairs, and Structure cabling were introduced.

In 1999 Blue Chip Sri Lanka became an IBM Business partner. Blue Chip Customer Engineering Lanka (Pvt) Ltd is also an ISO 9000 certified company [1.1]

1.3 Presently

Blue Chip's idea is to select few specific products and concentrate on those selected products (be professional), rather than trying to sell or maintain everything in the market. Today Blue Chip have given away maintenance and repairing of PCs, and are only concerned on mid-ranger servers and other related Internet and Intranet solutions.

In present Blue Chip provides range of solutions to their dedicated customers. Main focused business areas are;

- Uncompromised expertise and proven performance in systems integration for the enterprise class & midrange systems.
- Turnkey solutions for customized application development and Enterprise Class information systems.
- Pioneers in the electronic imaging & archival solution.
- Total solution providers for local (LAN, WLAN) & wide Area (WAN) networking and network management services.
- E-mail, Intranet & Internet solutions.
- Security solutions
- Business continuity & disaster recovery services.

Blue Chip is a business partner for some of the top quality products and brand names in the market, such as;

- IBM
- RVI
- GEAC
- Lotus Domino
- FingerTec
- Cisco
- BATM
- Patton
- I-O & I-O wireless
- WatchGuard

1.4 Mission

Mission of the company is in black & white and kept in publicly visible areas such as; company web site [1.1], conference room, customer area and departments for continuous reminder of the mission, for the customers and employees. Fallowing is the mission; and it would motivate the employees when ever they see it.

Our Mission

Blue Chip
Customer Engineering (Pvt) Ltd.
is committed to satisfied the
present and future needs
of the customer
by providing high quality
products and services,
and meeting on time delivery,
provide necessary training,
resources and staff,
working environment,
to our employees
to achieve the goal set them

1.5 Organization Structure

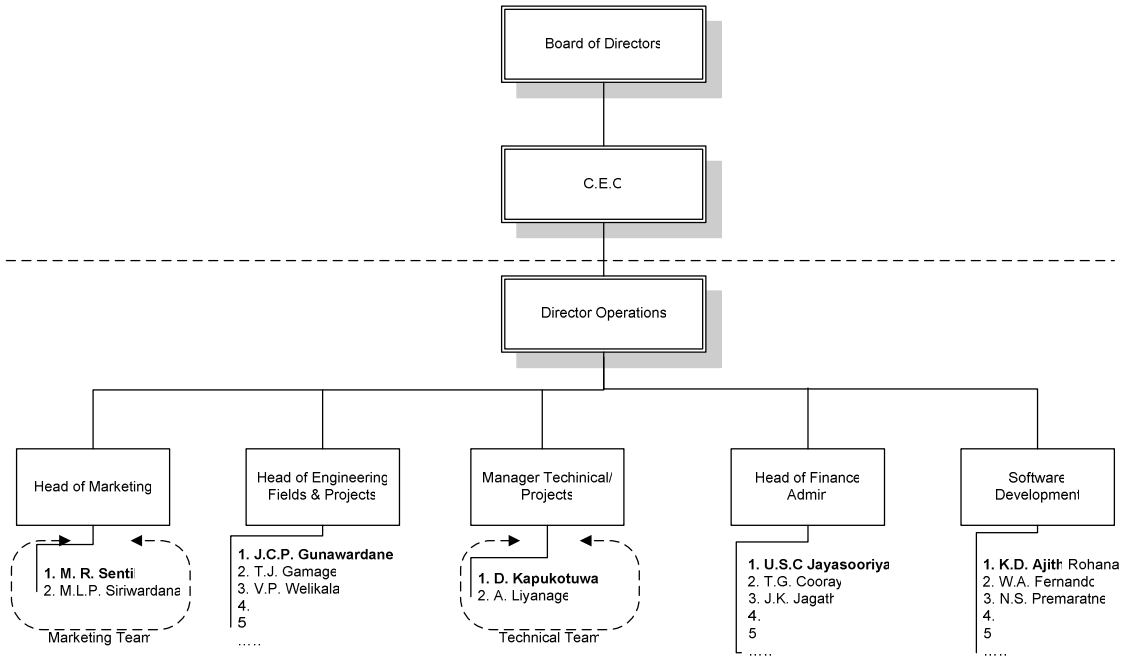


Chart 1-Organization structure

Blue Chip Sri Lanka is relatively a small company with a staff of around 35 employees. It's a combination of directors, managers, engineers, accountants, technicians, and other civil staff. Although its structure is clearly defined and simple to understand, few employees may work under different managers depending on the ongoing projects adding bit of complicity at times.

Blue Chip Sri Lanka can make most decisions (Director Operations) on their own but some times they may have get advices and approval depending on the importance of the issue. Other than officials who occasional visits from head office in UK all the employees are Sri Lankans. Directors hold the highest position in Blue Chip Sri Lanka.

Managing Director - Mr. Romeish de Mel

Director-Operations - Mr. Hugo Wisidagama

After directors, organization is sub divided in to 5 sections based on the type of work they do and managed by five managers. Since it's a small company departmentalization is not purely based on type of work. Thing that goes together are combined in together. As an example well identified departments like Administration and Accounts is combined and called as Department of Finance & Admin. Fallowing is a summery functionality or task of each department.

1.5.1 Engineering - Field and Projects

This is the largest department in the sense of number of employees. It carried out technical tasks like repairing of equipments, installations, maintenance, preventive maintenance (PM)of all supported products. Some employees are all the time on the field (i.e. customer sites) and have to travel all around the country. There is a special disaster recovery team (24x7) for management of Bank ATM machines all around the country. This department brings most of the income to the company. Both workshop and Server Room (Computer room) belongs to this department.

1.5.2 Projects and Technical support team

This is just a logical separation. It consists of only two fulltime employees and mostly does the project planning and designing. When plans need to put in to practice people are borrowed from department of Engineering – Fields and

Projects. There is a team of employees who is assigned to Head of Engineering – Fields and Projects (he performs all the human resource management things as well as technical things) but can work under Head of Technical and Projects (has only power to carryout technical things) when ever required.

1.5.3 Software Department

In here, customized applications are develop to local e-Server i-Series customers. Applications are developed only for e-Server i-Series (AS/400) and System 21 platforms. Some employees work internally and some work on customer sites. As I observed this is the most profitable department.

1.5.4 Marketing Team

They carry out the entire marketing related tasks like introduction of new products, product launches, presentations, exhibitions, and customer awareness. Also do the product pricing as well.

1.5.5 Department of Finance and Admin

Performs all the tasks related to Administration (organizational and human resource), Accounts and Welfare.

1.6 Environment

Since the numbers of employs are limited every one knows each other in the organization, so even the lowest level (in the organization hierarchy) employees get a chance to talk to the director.

It has a friendly and supportive environment but like all other places there is acceptable level of conflict, misunderstanding, personalized ideas, trying to over come others, etc. Still this is at an acceptable level and we have to except such things in any environment where different kinds of people work together.

Management encourage employees to be more professional by providing them necessary training, necessary equipment and even bearing the cost of professional exams such a CCNA, IBM Certification. Employees have really enough freedom of using resources for their professional development.

1.7 Performance and Profitability

Blue Chip employees have a huge potential behind them, most of them are highly technically competent. Blue Chip expect for professionals who have idea on broad range of thing (products they work with) rather than one specific product. It is performing at a good level, but it is not optimum and I feel with bit more management it could improve a lot.

In early day (1995-1999) company was really profitable (according to the statistics) mainly in the field of LAN, WAN and Structured Cabling (they were only few companies at that time). They got much more than they put in. Based on my observations it seems that they are just covering the cost today. With my meeting with the Accountant, I got to know that they are running on a loss mainly because of the economic condition of the country and Structure Cabling is being done by large number of companies. According to yearly summaries, the return they get back is not enough compared to what they put in.

Since Blue Chip deals with original products and really expensive mid-range servers (considering local IT market and PC Servers) company had to cut down their profit margin if they need to gain any business. Still I think (base on what I have seen, heard from customers and comparing other similar products on the market) the profit margin should be reduce bit more if they need to be really competitive in the market.

1.8 Things that need improvement

As a student still I have only theoretical ideas about management that I gained from subjects like Organizational and Human Resource Management. With that theoretical knowledge I manage to observe that there were lots of things that need bit of attention for better performance as an organization.

I discussed my observations as a third person (i.e. seeing the fully story from both sides) with the Accountant (also acting as HR manager) and the Director. I told them how I see those problems, how I feel them what are my suggestions for improvements. They really appreciate my ideas; I hope it would help at least a bit for better future of Blue Chip.

There are few problems with the organization structure (sometimes a conflict occurs when allocating employees to Projects & Technical support team and

Department of Engineering – Fields and Projects department). There was a case of task identification which they try to correct with the support of third party. And several other issues related to human resources. I am not in a position to talk further on such issues because it would affect the integrity of privacy of the company and it is not ethical either.

1.9. Future

As a way of overcoming some of the problems Blue Chip UK has decided to sell 51% of their shares (with the management) to another local partner. So in near future (within two to three months) there will be a management as well as structural change.

I believe Blue Chip has lot of individual potential, if properly utilized and combined together (synergy) it would easily be among the best.

2

Training Experiences

"experience makes a perfect man"

This chapter is a brief presentation of my work plan, work sites and products that I worked with. It also includes type of work I did, capacities of various products and problem encountered and solutions found while making my training a success. I had the opportunity to interact with customers and there were several customer site visits. Further discussion of some of the important topics (as I feel) and products are done in chapters 3 to 5.

2.1 Introduction

The whole idea of Industrial Training program is to expose students to the real industry and allow them a get some exposure towards it while they are still an undergraduate. The experience they get both technical and none technical is the vital part of it.

Although Blue Chip does provides total solutions (Software, Hardware and Networking) my keen interest was on Computer Hardware and Networking. Being focused to those subjects I was exposed to whole lot of products, their internal behavior, usage, installation, configuration, testing and trouble shooting. I had the opportunity of interacting with customers, planning solutions to their requirements and presenting my ideas and my own view in certain situations as well.

2.2 My Work Plan

I was the first trainee to had six months (24 weeks) training in the field of Computer Hardware and Networking at Blue Chip. Earlier there were few other trainees (not from University of Moratuwa) but it was either three months training or only in the field of electronics.

There wasn't any specific preplanned training program. I was advised to prepare my own work plan based on the products and resources they had and also based on

my personal interests. I was advised to use the company web site [1.1] as the reference. So I consider all the products and identified several areas to be fallowed. And few other products were kept in my interest list to be fallowed if I have enough time to cover them as well.

A plan was prepared and was send to the manager; with few modifications it was finalized. Table 2.1 shows initially approved plan.

Work Plane			
Duration	24 weeks From 19th May 2003 to 31st October 2003		
Module No	**Target**	**No of Weeks**	**From …. To ….**
1	AS/400 & OS/400 Introduction to mid range servers, Basic concepts, Hardware concepts, etc.	4	19th May to 13th June
2	Workshop training	3	16th June to 4th July
3	Network Security - 1 Structure of the internal network, Organizations Network diagram, etc.	4	7th June to 1st August
4	Communication and cabling Field Study and planning for cabling, communicating equipment, wireless devices, switches, router, etc.	4	4th July to 29th August
5	Network Security - 2 Security threats, Firewalls, ServerLock	2	1st September to 12th September
6	More exposure to AS/400 & OS/400 Site visits, hardware concepts, system planning and installation	4	15th September 10th October
7	SNA, Lotus Domino, etc introduction, basic applications and configurations in AS/400	2-3	13th October to 31st October

Above plan includes several site visits and completion of training report. Certain parts of the plan will be changed due to availability of resources, time and opportunity. If enough time is left other products will also cover

Table 2.1 – My Work Plan

In practice work plan just became a reference model, than a scheduled time table. Due to people being so busy and unexpectedly Mr. Dhammika Kapukotuwa (in charge of me) leaving the company for sometime it became impractical to work according to the plan. Since work plan was indicating the key areas and products I

to be covered, I decide to fallowing things whenever resources or people are available. So within a singe week I interact with different products with time to time. In a way it is good rather than referring a single manual entire week.

After end of 12 week I did a review of the things covered and thing to be covered. I was going at a good rate and I had covered lot (about 75%) from the initial plan. So I had enough time to fallow some of the secondary options (of the initial plan) like Patton Products, FingerTec, etc.

2.3 Work Place

I was attached to the Server Room (Computer room) also called the Disaster Recovery Center during my 24 weeks. Although initial work plan (Table 2.1) indicates there should be 3 weeks of Workshop training it was not done. While staying at the Server Room I attended Workshop from time to time based on the things that was able to involve in.

Due to day to day maintenance of PCs, certain software programs (e.g. virus scanners) I attended every place in the organization. There were lots of site visits during my training. For most of the customer sites I attended with an official (e.g. engineer) and there were few times where I directly visited the customer site.

Although I was attached to the Server Room I worked under two managers. Within first 14 weeks I was mainly working on Mid-Range servers, Structure Cabling, Domino, etc. and during that time Mr. Kirthi Gunawardana was my managers. Remaining 10 weeks I work under Mr. Dhammika Kapukotuwa and during that time I was working with products related Network Security, LAN, WAN and WLAN.

2.4 Exposure

I was not assigned to any specific during my training. But there were lot of small tasks that I have to finish during one or two days. Some of the tasks were preparation of technical documents, broachers, planning and drawing various network diagrams, developing small programs for internal work, etc.

Fallowing few sections will introduce a summery of activities carried out relating to each key product.

2.4.1 Mid-Range Servers

Mid-Range Servers are server machine that used in small to medium scale businesses. I was working with IBM e-Server i-Series servers (AS/400). These machines are significantly different than PCs and PC Servers. There internal architecture, Operating System, Software, Networking concepts was novel to me. I was able to study most of those concepts and compare them to what I had learned in the university (Computer Architecture, Operating Systems, Networking).

Company has several servers of different scales and I was given the opportunity of installing, configuring, trouble shooting and day to day maintenance of those servers. I was given enough freedom to use those machines for my studies. It was really amazing that they were not concerned on any misuse that would happen to such an expensive server.

Mr. Kirthi Gunawardane (manager and engineer), Mr. Janaka Gamage (engineer) and Mr. V.P Welikala (engineer) helped me in completing this section.

2.4.1.1 AS/400 Hardware

I. Introduction
   → Introduction to AS/400 Hardware Architecture
II. Processors
   → RISC & CISC processors, 32 bit → 64 bit → 128 bit computing, Multiprocessors
III. Input Output
   → I/O Technologies, various types of system busses
IV. RAID
   → Different levels of RAID and implementation of RAID V in AS/400
V. Networking
   → SNA (Systems Network Architecture), TCP/IP, Ethernet, Wireless
VI. Devices and accessories
   → Installation of Disk, Tape, Optical Drivers, Terminals, Various I/O Cards, terminals, Modules
VII. Problem Determination
   → How to identify problems, use of error logs, how correct basic problems, disaster recovery

2.4.1.2 OS/400 and other Software

I. Introduction

→ Introduction to basic OS concepts, Advanced Application Architecture

II. Storage

→ Hierarchical storage management, Logical partitioning, Tera space Storage and single level addressing

III. File system

→ Native file system and IFS (Integrated File System)

IV. Concurrency

→ Thread Technology and handling concurrency issues

V. Client access

→ Accessing the system through GUI based Fat Clients (Client Access) and dome terminals (thin clients, Green Screen)

VI. OS and Software Installation

→ Installation of Various OS versions (V4R5, V5R2), Licensed programs, Installation and configuration of Domino

VII. Backups

→ Entire system backup, incremental backups and restoring

VIII. Clustering

→ Application level clustering for higher availability

2.4.1.3 Servers

During my training I had hand on experience on 4 of the 6 servers, all 6 severs were of different models, had different versions of Operating Systems, Licensed programs, and used for different tasks.

Internally machines were identified by there respective model number or nick name assigned to them. Fallowing is the summery of tasks of each server.

AS/400 600

This is the server I first worked with. 600 indicate the model. It is used for testing of devices and training purposes.

e-Server i-Series 150 (Mod150)

Small server which looks like a PC, with every low processing power and capacity. Used for customer site demonstration purposes and testing. Act as the secondary server for Domino mail Cluster.

e-Server i-Series 170 (mail server)

Used for Lotus Domino mail server, Web server as well as DNS server. Is the primary server of the Domino Cluster.

e-Server i-Series 720

Relatively new machine with huge processing power than all the other internal servers. Still being used for testing of both Hardware and Software. In future it will be used as IBM Web Sphere Application Server.

Table 2.2 summarize the capacities of each of those servers

Model	**9401-150**	**9406-170**	**9406-600**	**9406-720**
Nick Name	Mod150/150	170	600	New/720
Serial No	44-L6890	10-3V7XM	10-3YM2M	44-12F2A
Used as	for demonstrations & as study guide	e-Mail/WEB/DNS server	For testing purposes (accessories, drivers & cards)	Intended to be used for WebSphere
Current OS	V4R5	V4R5	V4R5	Now V5R2 (earlier V4R5)
Processor type	2269	2291	2129	2061
Relative System Performance				
CPW – Processor	20.2	115	22.7	240
CPW – Interactive	13.8	25	-	35
No of Processors	1	1	1	1
Main storage Current/Max (MB)	64/192	512/832	192/384	256/2048
Disk Storage (GB)				
Base	4.19	4.19	4.19	4.19
Max Internal	29.9	85.8	175.4	1288.4
Max External	n/a	175.4	n/a	1236.9
Current	4.19 x 4	4.19 x 5	4.19 x 3	4.19 x 10
I/O Slots				
Diskette	0	0	0	0
CD Rom	1	1	1	1
Tape Attachment	¼” Internal/1	¼” Internal/1	¼” Internal/1	¼” Internal/18
Communication				
Max Twinax Devices	7	228	5	2628
Communication Lines	1/5	1/18	0/	1/128
FAX Adapters	0	0	0	0
10/100 Mbps Ethernet Adapters	1/1	1/2	0	1/2
Integrated Netfinity Server	0/1	0/1	0/1	0/1
Cryptographic Processors	0	0	0	0

CPW – Commercial Processing Workload (section 3.9)
n/a – not available

Table 2.2 – Capacities of Servers

I didn’t have any specific projects relating to AS/400. But had few tasks such as testing and determining problem in disk and tape drivers, identifying

malfunctioning hard disk from set of disks using various disks, participated in several problem solving and PMs (Preventive Maintenance) at customer sites.

2.4.2 Network Security

Network security has become a hot topic today due to all sorts of viruses, worms, hacking and denial of service attacks. Blue Chip provides enterprise level security solutions to prevent and minimize threats that come through internet. Blue Chip is the only local reseller for award winning WatchGuard Firewalls.

I study about potential network threats, how to overcome them, functionality and structure of Firewalls, installing and configure WatchGaurd Firewalls, VPN (Virtual Private Network) solutions, planning and designing customized solutions based on WhatchGuard products. Company encourage me to fallow the WatchGuard certification exams and I manger to become a "**WatchGaurd Certified Professional**" for FireBox III and ServerLock

Other than Firewalls I leant about WatchGuard ServerLock which is a way of hardening and locking the Operating system (Windows 2000 Server and Sun Solaris). I did a small research on Enterprise level Anti-Virus solutions from Trend Micro. It was an evaluation of Trend Micro products, because company was interested in buying it.

Mr. Dhammika Kapukotuwa (Manager projects) and Mr. Janaka Gamage (Engineer) helped me in completing this section.

2.4.2.1 Firewalls

Detailed discussion of Firewalls is done in chapter 4. Fallowing list is a summery of thing I leaned

I. Security Threats

→ Identifying security threats, venerability window, counter measures and Intruder Detection (ID), need of a security policy.

II. Firewalling Basics

→ Concepts, Architecture, 3 Generations of Firewalls, Packet filtering, proxies, VPN, NAT, Authentication, logging

III. Adding a Firewall to a network

→ Placing Firewalls on networks (Routed & Dropping modes), configuration

of networks and security polices, planning networks, VPN solutions, Live Security Service®

IV. Organizational Firewall

→ Understanding currently assigned rules, doing various changes, network diagram

V. Research

→ Did a research on TOC (Total Cost of Ownership) for Hardware based Firewalls and software based Firewalls.

VI. Certification

→ Passed the online "WatchGuard Firewalling Basics" exam and became a WatchGaurd Certified Professional

VII. VPN Solution

→ I was asked to met a customer and gather his requirement. It was about VPN solution using ADSL connections with DHCP. On my own I came up with solutions that would satisfy the requirement and prepared a proposal.

Specification of the firewall that I used in my training is given in Table 2.3

Type	
Manufacture	WatchGuard Technologies Inc
Type	Firebox 700
Part No	WG30700
Specification	
Packet Filter Throughput	150 Mbps
3DES VPN Throughput	5 Mbps
Total VPN Tunnels	150
Authenticated Users	250
Mobile User VPN	Unlimited
VPN Manager	Not available
Ethernet Interfaces	3 RJ45 – 10/100 TX
Hardware Warranty	1 Year
Features and Benefits	
Packet Filter	Dynamic stateful packet filtering
Security Proxies	Protect through SMTP, FTP, HTTP, DNS proxies
Monitoring, Reporting and Logging	Secure encrypted colorized logging, historical report generation and real time monitoring.
Branch office User VPN	Encrypted VPN tunnel between offices with Firebox or other IPsec devices
NAT	Support dynamic, static & 1 to 1 NAT
Authentication	NT, Radius, SecureID, Crypto Card, PKI
URL Filtering	Restrictions by user, group, time of day or site type via regularly updated database

Guard Against Attacks	Blocks spoofing attacks, port space & address space attacks, IP option attacks and SYN flood attacks

Table 2.3 – Firebox 700 specification sheet

2.4.2.2 Server Lock

Serve Lock is a software program that is installed on the servers to protect misuse and unauthorized modifications to the important Operating System Files (password files, drivers, access lists), registry keys and user files. See section 4.4.1 for more detailed explanation. Got the certification for WatchGuard ServerLock as well.

2.4.2.3 Trend Micro Products

Company was interested in buying Trend Micro "NeatSuite", an enterprise level anti virus solution for total protection from Internet Gateway to Desktop PC. "NeatSuite" is a collection of integrated products. Several demo versions of those products were installed and tested. Fallowing is a brief summery of work done;

I. Installation

→ Installation and configuration of OfficeScan® (centrally managed desktop anti-virus solution) ScanMail® (mail server protection for Domino) and ServerProtect® (virus scan for PC servers).

II. Client installation, applying policies, maintenance and troubleshooting

→ Day to day maintenance, troubleshooting and installation of client version through remote access. Scanning Serves and client machine and removal of viruses.

III. Testing

→ Testing against various internal and external (from Internet) file transfers, e-mails with viruses attachments. It was proven that Real-time Scan was not up to some of the other competitive products in the market. Another issue was ScanMail was removing MIME Contents from e-Mails

IV. Technical Support

→ Contacted respective technical support teams in India and Singapore and resolved some of the problems above mentioned problems

Refer section 4.51. for more detailed explanations.

2.4.3 LAN, WAN and WLAN

I also had the opportunity of studying concepts, planning, implementing and troubleshooting of Local Area Networks (LAN), Wide Area Networks (WAN) and Wireless LANs (WLAN). I did also lean about Structured cabling, configuring of CISCO Routers, ADSL and other xDSL connections.

Wireless Networking is further discussed in chapter 5. Mr. Ajith Liyanage (engineer), Mr. Tikiri Guonetilake (engineer) and Mr. Janaka Gamage were helping me a lot to cover this section. Fallowing is a summery of tasks carried out.

I. Designing LANs and WLANs, drawing diagrams (wired and wireless), proper placement of Modems, CSU/DSU, Routers, switches, hubs, etc.
II. Allocation of IP addresses, subnets, assigning Subnet Mask
III. Trouble shooting network problems using various software tools as well as cable testing equipments.
IV. Identifying crossover cables, straight cables, wiring sequence for R J45 male/female connectors
V. Understanding and drawing the organizations network diagram
VI. Router configuration, NAT configuration
VII. Configuration of drivers, devices such as PCMCIA cards, Access points
VIII. Prepared a technical paper to be presented to customers about I-O Wireless products

2.4.4 Patton Products

Patton Electronics [5.1] has range of products for all sorts of connectivity (end to end ADSL connectivity, fiber optic connectivity, lease line, extension of LAN over copper cables, etc.) media converters (serial to Ethernet convectors, RS485 to RS232 converters, etc.) and surge protectors (DB 9/15/25 surge protectors, RJ 11 RJ 12 RJ 45 surge protectors, coax and twinax surge protectors, etc.).

I. I studied about some of the products (most thing were bit advanced for me because I didn't had any idea about high end ADSL, xDSL, ISDN devices)
II. Draw few network diagrams indicating proper placement of various surge protectors
III. Prepared several product broachers

2.4.5 Other projects and products

I had some exposure to fallowing products as well;

I. Thin client

→ Is a diskless work station with inbuilt Windows CE and Internet Explorer 4.0. It can work with AS/400, Windows Terminal services and x-Windows. [6.1]

II. ADSL

→ Studied about various DSL (xDSL) technologies, ADSL connections and Modems that company was interested in. [7]

→ Company gave up the idea of an ADSL connection because SLT is not willing to provide static IPs with ADSL connections.

III. Personal Computers

→ Hardware and software troubleshooting of internal PCs

→ Installation of Operating Systems such as Windows 98, Windows 2000 Advance Server, Windows 2003 Server, Read Hat Linux 7.1 & 8.0

→ Configuration of Terminal Services on the PC server

IV. FingerTec

→ FingerTec [8.1]is a range of biometrics Access control and Time Attendance systems which use finger print for identification. Studied bit about its functionality, various types of devices, various connectivity options, etc.

V. Software Development (ATM Logger)

→ Develop a simple program to keep track of ATM call logs (call for repairs of ATM machines) for the workshop. Since it was a small program no specific requirement analysis or planning was done. It was developed using Visual Basic and had a Microsoft Access database.

→ Its task if to keep track of all the calls and pop up a message when call for a same machine come within 45 days (repeat of an earlier repair) of the last call. It supports user login and database backup facilities.

→ Configured it to work on a Thin clients through Terminal Services

2.4.6 Exhibitions

During my stay at Blue Chip, they participated in two exhibitions. I actively participated to those two exhibitions.

I. Garment Times 2003

→ Held as SLECS for 3 days (18/09/2003 to 20/09/2003) and was for people who are interested in local apparel industry

→ Company presented several Software solutions and FingerTec.

II. IT Office 2003

→ Held at BMICH from 26/09/2003 to 28/09/2003. Its was about computer related products to office environments

→ Company presented 5 products (WatchGuard, FingerTec, I-O Wireless, Thin Client and Patton products)

→ I was involved with all the activities. I planed the dummy network to be used at the stole integrating all the 5 products. Then inter connect all the products and testes them day before the exhibition.

→ Stayed at the exhibition for all three days and was able to actively present all 5 products to customer.

→ Developed a small program to register customers online

→ Draw several diagrams indicating various options and total office solution using those 5 products.

Also participated and help to the WatchGuard product launch conduct by Mr. Vishak Raman from India.

2.4.7 Site Visits

There is lot of site visits during my training where I lean a lot, specially how to interact with customers. It was a grate experience especially when I visited customer sites alone.

I. Abans Environmental Services

→ Visit several times to see the progress of structured cabling, draw several network diagrams related the LAN

→ Install Trend Micro ServeProtect and OfficeScan, scan workstations for viruses with the OfficeScan client program and removed virus infections on those machines

II. Growth Lanka

→ Visit for a rejection of a jammed tape in a tape driver

III. SPC

→ Helped in a PM (Preventive maintenance) of a e-Server i-Series 170 machine

IV. Peoples Bank

→ Visit for a configuration of network connection between AS/400 server and a PC through a dial-up connection using two V90 modems

→ Participated to a presentation about WatchGuard products conduct by Mr. Vishak Raman

V. EDNA

→ Visit for a disaster recovery of a Hard Disk. Hard Disk had developed bad sectors all its data was pumped in to a new disk and damaged disk was replaced.

VI. Lanka Bell

→ Participated to a presentation held at Lanka Bell. It was about some of the

products that Blue Chip is dealing with.

VII. Lankem

→ Participated to a Lotus Domino 6.0 installation and configuration

VIII. Janashakthi Insurance

→ Problem identification and correction of the LAN.

IX. CIC

→ Remote locations were unable to connect to the server due to incorrect IP address assignment. Problem was resolved by correcting IP addresses

X. Department of Examination

→ Disaster recovery of hard disk. One hard disk had stopped responding but the system was running because of RAID

XI. CTC Eagle

→ Installation and configuration of an I-O Module and a TFT Screen for demonstration purposes.

XII. Suntel

→ Install WatchGuard Firewall for testing purposes at the customer site

XIII. Mr. Harrik

→ Met customer and had a discussion on his requirement. He was interested in a VPN solution through ADSL connection.

2.5 Problems encountered

There are no specific problems that I encounter while completing above sections either work or person related. As indicated earlier there were small problems such as not having a proper plan and getting help from people at right time. But in my view I am not considering it as a draw back or problem because it did not really affect me.

I encountered two problems related to products. This is what happened in brief.

I. Trend Micro

→ I felt that Real-time scan of both OfficeScan and ServerProtect (Trend Micro products) were not really performing what it suppose to do. I checked this with transferring files with know viruses (of course with proper safety precautions)

→ I contacted Technical support Team in India and ask about my observations. They replied me saying that my observation is correct and there are some limitations in the product

→ They were saying that

i. Real-time scan (scanning of file real-time when they transfer) check file only when it was accessed by user

ii. It scans only when file is fully downloaded to the system

iii. Real-time Scan is unable to check POP3 mails.

→ These limitations were not quite acceptable compared to other competitive products in the market

II. VPN Solution

→ One of our customers (Mr. Harrik) wanted to have a VPN solution using WatchGuard SOHO model. But there was an issue since he is not willing to have a leased line due to its high cost. He wanted to do it with ADSL and DHCP. We were not in a position to provide VPN through dynamic IPs (SLT does not give static IPs with ADSL).

→ We have to come up with a solution that would satisfy his requirement, after some referring on web we came up with a solution. There is a free service on the web which keeps both IP addresses and hostnames in a table. A program in the server (with a dynamic IP), informs to the central location when machine IP get change. So if some one wants to find any machine with a dynamic IP he just needs to know only the host name. Host name should not change any time because mapping is done based on the unique host name.

→ We were able provide him the solution with dynamic IPs and according to him we were the first to come up with such a solution from all the solution providers he had contacted in Sri Lanka.

3

Mid-Range Servers

"The right tool for the right job."

If spent more time on a single module it is for the studying, installing and configuring of AS/400 and OS/400. System was so huge that it would not be even possible to cove in one year. I only learned about hardware related thing, installing OS and Licensed programs and configuration of network properties (TCP/IP).

This chapter presents an introduction to its evolution, architecture, basic OS concepts, features, high availability and how to install OS/400. It is impractical to present everything related to AS/400 in a small report or at least what I have learnt, therefore this chapter is just an overview of AS/400 and what sort of exposure I had towards it.

3.1 Introduction

Server is a computer who provides services to clients in a network environment. Services may be either application services, Database services, and file & printer services or combination of all. Servers can be categorized in to four major types. Most common category is small scale PC based servers, which provide services to about maximum of 10 users. Second type is midrange servers, which are much more powerful than PC servers in all extents. Third types of servers are Mainframes, which is suitable only for very large organizations with over 1,000 users or so. Supercomputers are the most advanced type of servers; there capabilities are unmatched to any of the above types.

Mid-Range servers are capable of meeting the demands (in terms of processing power, adapting to rapid technology changes, e-solutions, etc.) forced by 99% of the enterprises, either there are small to medium or medium to large. Enterprises may need one or more mid-range servers with various capacities depending on their requirement. It depends on the **number of departments**, **branch offices** and **type of application**. Critical systems require backup systems for higher availability.

During my training period I had the opportunity of using, configuring, installing and maintaining AS/400 and IBM e-Server i-Series Midrange servers. Those servers are considered to be the most stable midrange servers available today (because of proven 99.9x% uptime).

3.2 AS/400

AS/400 stands for Application System 400. IBM introduced AS/400 in 1988, which was a combination of System/36 (know for easy of use) and System/38 (know for advance architecture). The AS/400 is designed and build as a total system, fully integrating all the hardware and software components that any business demands. It is a general purpose business and network system and optimized for environments such as banks, commercial organizations, etc. It was a real success because of its easy of user, higher reliability, flexibility, expandability and adaptability. In June 1995 first AS/400 models, based on 64-bit RISC Power PC AS processors were announced. AS/400 was one of the first systems to use RISC architecture.

Figure 3.1 – Range of IBM e-Server i-Series machines

3.3 IBM e-Server i-Series

In February 1999 the next generation AS/400 servers were introduced with a new brand name called IBM e-Server i-Series (also called as AS/400e or e-Server). e-Server was not just another machine; it is an integrated business solution [2.1]. The introduction of OS/400 Version 4 release 4 (V4R4) and other system software offer enhanced functions in notable areas of server consolidation, web services, network security, Java support, higher availability, e-Commerce and Database management.

i-Series is reliable, scalable, and recognized as one of the most flexible, easy to use systems in the industry with the ability to run multiple environments and quickly deploy applications. These attributes position i-Series as one of the best platforms

(not tight to OS/400, can also support Linux and Windows NT/2000) to manage the complexity and cost of e-business enablement. i-Series solutions also deliver leading total cost of ownership, extreme availability of data and applications, IT staffing productivity and user productivity.

Rest of this chapter the term i-Series refers to only the latest models and term AS/400e is used when referring to all 64-bit RISC based AS/400 models both older any new i-Series ones.

3.4 AS/400 Advanced Application Architecture

AS/400 Advanced Application Architecture is a brilliant, technology neutral architecture, enabling business to readily exploit the latest hardware and software technologies without causing disruption to existing application software. In simple words it is fully backward compatible and no need of either rewriting or recompiling current applications.

AS/400 is atypical in that it is defined by software rather than hardware. When an application program presents instructions to the machine interface for execution it see the interface as the pure hardware. But in reality it is not, it has to pass through a layer of microcode before those instructions to be understood by the hardware.

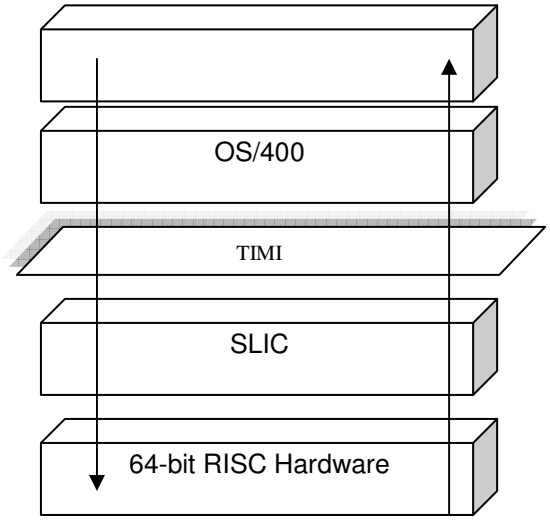


Figure 3.2 – The layered structure of AS/400 & AS/400e Server

This design insulates application programs and users from changing hardware characteristic through this comprehensive layer of microcode. When a different hardware technology is to be deployed, IBM rewrites section of microcode to absorb the new changes, while keeping the interface presented to the applications

intact. This interface is known as Technology Independent Machine Interface or TIMI (see figure 3.2) and the microcode layer is known as System Licensed Internal Code or SLIC. Java Virtual Machine provides portability in similar way, keeping the application interface intact (API) while changing the internals of the VM deepening of the OS.

The brilliance of this design was dramatically illustrated when AS/400 change its processor technology from CISC processors to 64-bit RISC processors in 1995. With any other system to move from CISC to RISC would involve recompiling (possibility some rewriting) of programs and even then older programs would run in 16-bit (or 32-bit) mode on the new 32-bit (or 64-bit) hardware. This was a significant problem when Windows move from 16-bit computing to 32-bit computing. But thanks to the concept of TIMI, IBM was able to port to new technology within just a weekend.

On the customer side, they were asked to save the application, upgrade SLIC and restore their applications. Programs would run with out any problems, but they were acting as fully 64-bit programs. In future IBM expects to use this TIMI layer when updating to 96-bit or 128-bit processors in near future.

3.5 Object Based

In AS/400 environment everything is considered as an object. An object is a container, everything the system uses, user and system data structures is packaged in one of these containers. The objects are encapsulated; meaning that you can not see inside. Object has a name and a type. All objects are structured with a common object header, and a type dependant functional portion.

Object based approach work only with names, not on addresses; this will make sure possibility of object misuse is minimum, compared to other systems without an object based approach. There are two important consequences of object based design [2.2]. First system built around object based model supports machine independence since it works with names. Secondly such a design delivers high level of system integrity.

3.6 Other Hardware concepts

3.6.1 64-Bit Computing

64-bit computing is the use of 64-bit processors for computers, which are twice faster (theoretically) than today's well known 32-bit processors. But the problem is what do we do with exciting software? Two answers are available; one is to make sure that new processor is capable of executing older software (backward compatible) or existing software should be rewritten or recompiled using 64-bit compilers. Second solution is not really commercially feasible. AS/400 TIMI layer allows above problem to over come as explained in section 3.4.

32-bit processors use 32-bit wide registers and 64-bit processors have 64-bit wide registers, so during a single data transfer they can move data twice as fast as 32-bit microprocessors, but the data must be longer than 32-bits to take advantage of it.

Scientific and Engineering workloads use a lot of numeric data. Numeric data types like integers and single-precision floating-point numbers are readily represented with 32-bits. They must be converted to 64-bit data types to take advantage of 64-bit computing. Extending them to 64-bits enables larger, higher precision numbers, but numbers that big and precise are rarely needed. Commercial workloads use character strings. Commercial workloads frequently use data that is much longer than this and most common operation is to move them from place to place. Moving 64-bits at a time is much faster than 32-bits. [2.4.1]

64-bit process support larger address space than 32-bit ones. Latest processors (Northstar) use IBM's Silicon on Insulator (SOI) (Figure 3.3) technology which improves performance dramatically.

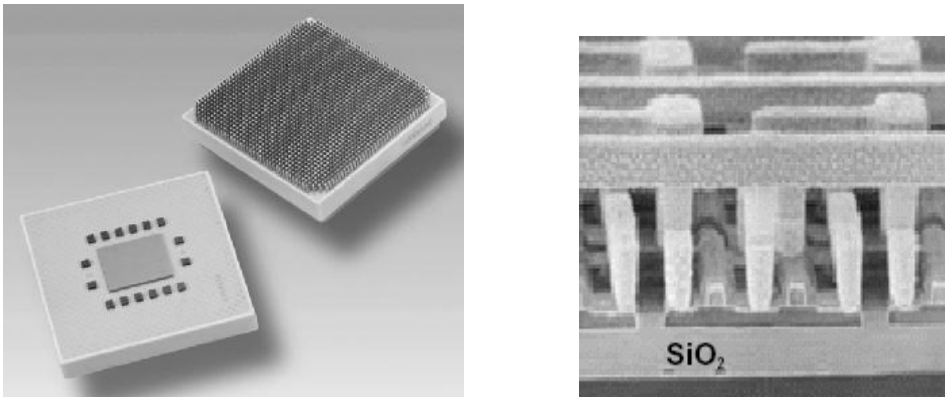


Figure 3.3 – **left** – 64-bit Northstar processor [2.3] **right** – magnified view of the internal circuit

Applications that use multimedia or that manages huge databases are becoming more common. These applications benefit greatly from the ability to address and manage large amounts of data with virtually no size limits. The ability to manage very large amounts of physical memory also increases performance. OS can be converted to support larger memories, but applications must also be converted to use 64-bit addresses to take full advantage of 64-bit computing.

3.6.2 Hierarchy of Microprocessors

As most of the other systems AS/400 also uses several sets of processors such as various disk controllers, I/O controllers. Main processor performs tasks such as numerical computation, logic and issuing commands to sub processors and responding to events. When main process encounters that data need to be written or read from any I/O devices that request is delegated to the appropriate microprocessor which is attached to the particular device. Mean while main processor continues to execute another process. The controlling and commanding process has to fallow the fallowing hierarchy (figure 3.4).

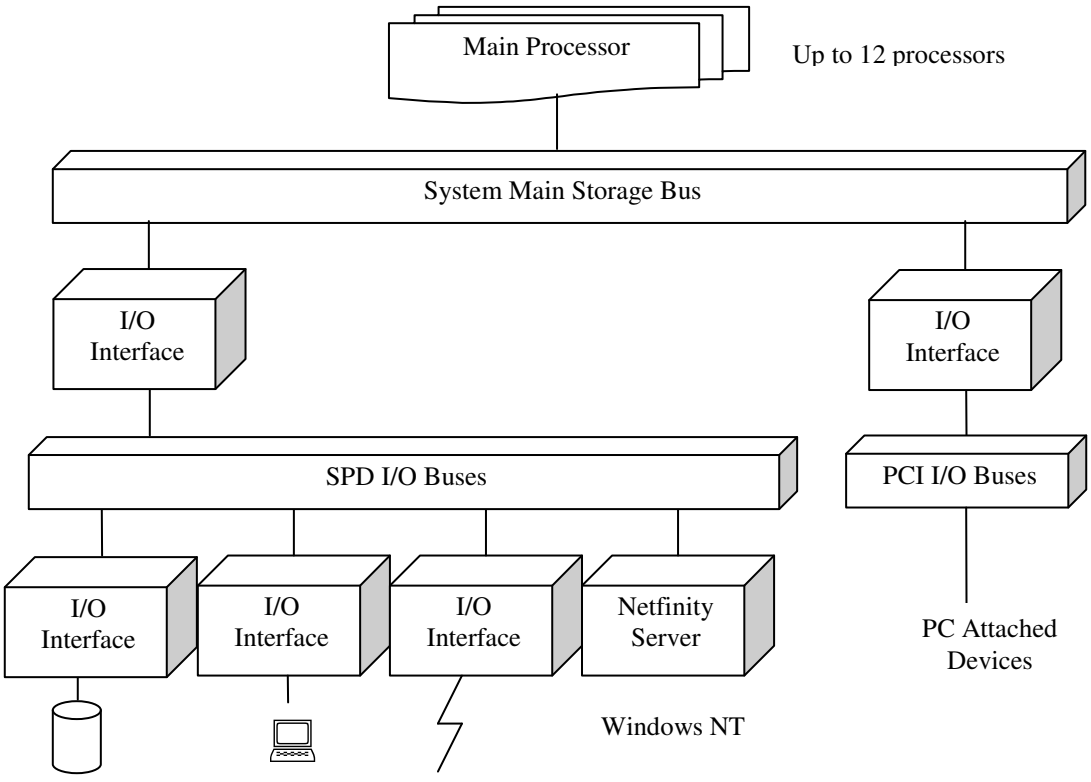


Figure 3.4 – Hierarchy of Processors

AS/400 is designed for business computing, one of the main characteristics of such an environment is it is highly I/O intensive, therefore large number of I/O

processors are required for better performance. There can be up to 12 main processors in the system, and range of other sub processors each dedicated to a particular I/O device type. A single large AS/400 configuration can have well over 200 processors.

3.6.3 Integrated Storage

Earlier on most high end servers, storage was not an integrated part of the system, it was a kept as a separate unit (in an external disk racks) and connected to the server through a high speed bus. If server had any disk inside it was only for the OS not for data. This approach cause lots of problems although there were few advantages; and became a bottleneck when trying to increase the overall performance. Taking advantage of the existing AS/400 system structure, the storage section becomes an integral part of the overall system architecture (storage controllers were kept inside the system) in industry it is named as integrated storage.

The storage shares the same system packaging to reduce costs and improve reliability. It allows AS/400 to spread work across different levels of system resources to help improve overall performance. The tight coupling with OS/400 storage management allows the delivery of enhanced function and usability. Packaging offers several advantages like faster response, sharing of same package and power, simplicity of the package and ease of management.

3.6.4 RAID

RAID stands for Redundant Array of Independent Disks (or Redundant Array of Inexpensive Disks) is a term used to describe the technique of improving data availability through the use of arrays of disks and various data-striping methodologies. Disk arrays are groups of disk drives that work together to achieve higher data-transfer rates than those provided by single large drives. An array is a set of multiple disk drives plus a specialized controller (an array controller) that keeps track of how data is distributed across the drives. Data for a particular file is written in segments to the different drives in the array rather than being written to a single drive. Arrays can also provide data redundancy so that no data is lost if a single drive in the array fails. [2.6]

Depending on the RAID level, data is either mirrored or striped. RAID algorithms can be implemented as part of the Operating System's file system software, or as part of a disk device driver. Hardware RAID adapters generally provide better performance than software RAID because embedded processors offload the main system processor by performing the complex algorithms, sometimes employing specialized circuitry for data transfer and manipulation.

Data striping

Is the process of dividing the data (to be written) in to fixed size blocks (strips) and writing each block in a different disk. Most of the time data stripping is done at the OS level. Increase both data reading and data writing speeds.

Data mirroring

Each set of data to be written is save as multiple copies in different disks. Done by disk controller and improves fault tolerance by higher availability

Parity

Refers to the method by which one data stripe at a time is taken from each of a set of disks and through the use of an XOR algorithm creates redundant information for the group of data stripes and saving this parity information is a separate disk. Incase of single disk failure, the parity with association of data remaining disks can be used to recreate the missing data.

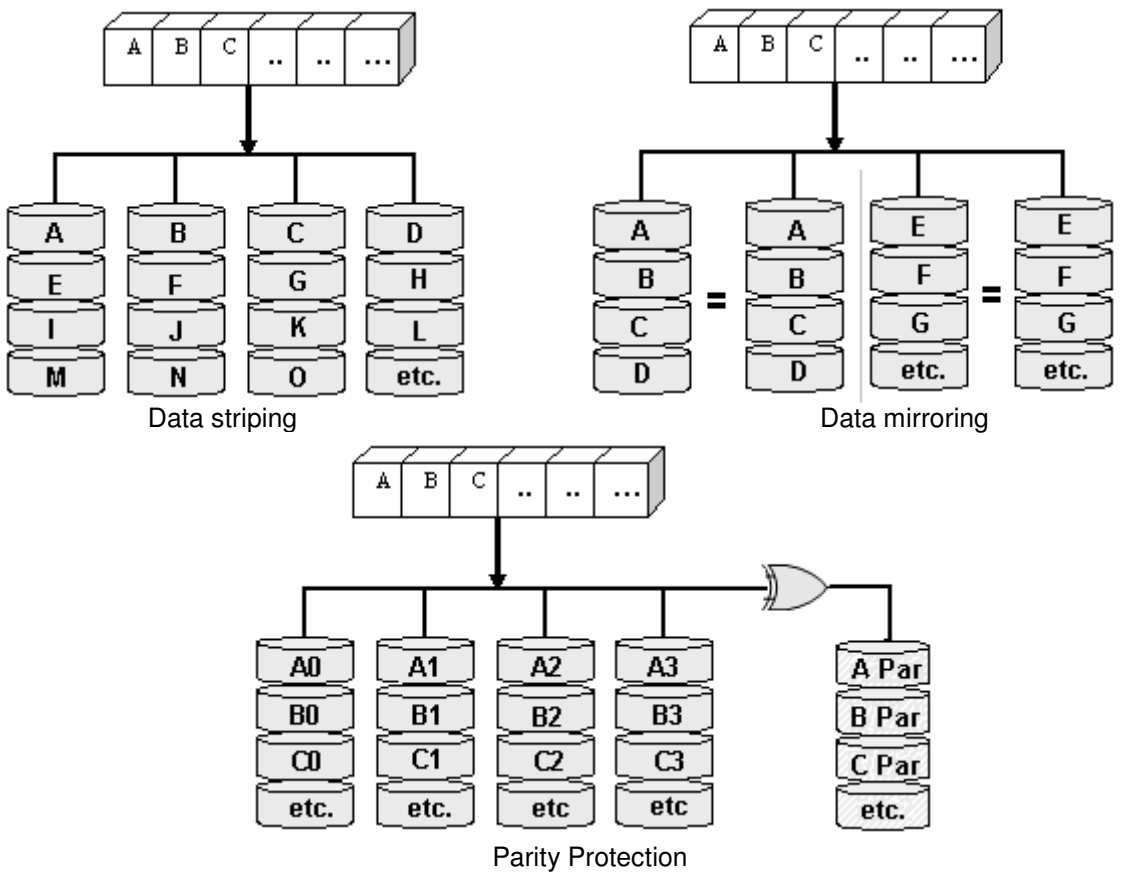


Figure 3.5 – Data striping, mirroring and parity protection

In Figure 3.5 we can see how does a file with several blocks (A, B, C, …) is saved in an array of disks using stripping, mirroring and parity protection.

Different RAID levels are defined and each level has its own merits and demerits, each level is suitable to specific environments and applications. Some levels use mirroring, striping, parity or combination of these three. Table 3.1 summarizes well known RAID levels.

Level	Technology	Optimized for	Applications
RAID 0	Data striping	Higher data transfer rates	Applications requiring high bandwidth, such as Video Production and Editing
RAID 1	Data mirroring	Higher availability	Application requiring very high availability, such as financial applications
RAID 2	Hamming Code ECC	Speedy access + availability &	No commercial implementation exist
RAID 3	Data striping + Parity	Speedy access + availability	application requiring high throughput, such as Video Production and live streaming
RAID 4	Parity	Faster access than RAID 3 slower writing	Rarely used due to bottleneck caused by single parity disk
RAID 5	Distributed parity	Increased performance than RAID 4 & higher availability	Applications that manipulate small amounts of data, such as transaction processing applications
RAID 6	Distributed parity	Extension of RAID 5, higher fault tolerance	No commercial implementation exist
RAID 7	Data striping + Parity + Real-time OS	Speedy access + higher fault tolerance	No commercial implementation exist because higher cost per bit & short warranty
RAID 0+1	Data striping + Data mirroring	Higher data transfer rates + higher availability	File servers & imaging applications but very expensive

Table 3.1 – Different levels of RAID

3.6.4.1 Implementation of RIAD in AS/400

RAID-5 is the best suitable RAID solution for the AS/400 environment, but the actual implementation differs slightly from standard RAID 5. In real implementation parity is distributed within data disks (but not in the same disk containing the data block) than a separate parity disk. RAID 5 requires parity to be spread between all the disks, but in AS/400 it is among several disks only. If data parity was distributed among all disks it would be hard to incrementally add new

disks to the system. To optimize performance, the AS/400 automatically spreads objects across multiple disk drives as well.

3.6.5 I/O Technology

AS/400 is in the process of transitioning its I/O structure from its original SPD bus to the high performance RIO (remote I/O) and industry standard PCI (Peripheral Component Interface) buses. This is being done in a controlled fashion with options to maintain the customer's investment in recent technology. AS/400 has also converged on an I/O subsystem structure that leverages the best of industry technology while maintaining the robustness and ease of use that AS/400 is known for. This structure is well positioned to integrate advances in technology with minimal effort. [2.7]

3.7 OS/400

OS/400 is the Operating System used in IBM AS/400 midrange servers. OS stands for Operating System. It is the only Operating System that can be installed in AS/400 machines and no other computer (Intel x86, Spark, Alpha) can run OS/400 as well. OS/400 is a proprietary Operating System that only IBM has control on it.

“The combination of OS/400 and the AS/400 has an odd mix of advanced and old-fashioned approaches to computing. On the one hand, the object-oriented approach of treating system resources and their interaction as objects and messages exists in few other OSs used on a large scale in the business world but will be seen more and more in the coming years. On the other hand, certain aspects of OS/400 and the AS/400 show their roots in aging technology, such as IBM's encouragement of developers to use RPG and COBOL and the inclusion of an 8” or 5¼” disk drive without an option for 3½” disk drives”.

Above was a paragraph extracted from “The Operating System Hand Book” by Bob DuCharme. But it has proven to be wrong and AS/400 is still considered to be the best solution for ever demanding e-business. It has evolved from a dumb terminal to a GUI based terminal or Fat client (Client Access), moving from proprietary SNA (Systems Network Architecture) to TCP/IP, adding all sorts of Optical, CD-ROM, DVD ROM drives. Today IBM highly encourages use of Java

instead of languages like COBOL or RPG. Only limitation is it is specifically designed only for commercial environment.

OS/400 is a single entity. Once you have bought an AS/400, you do not have to continue to shop for system software components before it is ready to run any business. All the necessary software components for Relational Databases, comprehensive security, communication with broad range of diverse systems, mail servers, web serves and all sorts of internet capabilities and many more are already there. These components are not just fully integrated but also fully tested as well.

Most people think they need higher quality hardware to keep higher availability but most of times forget the impact caused by malfunctioning software. Most system fails are caused by software, so testing up to its extreme is necessary and would be better if single vendor could provide all the things rather than going for many third party vendors.

Next few sections discus some of the OS concepts such as processes, threads, file system, deadlocks, memory management, networking.

3.7.1 Processes and threads

Multithreaded programming is a technique to allow concurrent and/or parallel operations within a program. With the introduction of the Java, the number of multithreaded applications in the industry has dramatically increased. The AS/400 architecture is ideal for supporting an integrated threads model. The AS/400 architecture eliminates many of the limitations and restrictions imposed by other platforms that support threads.

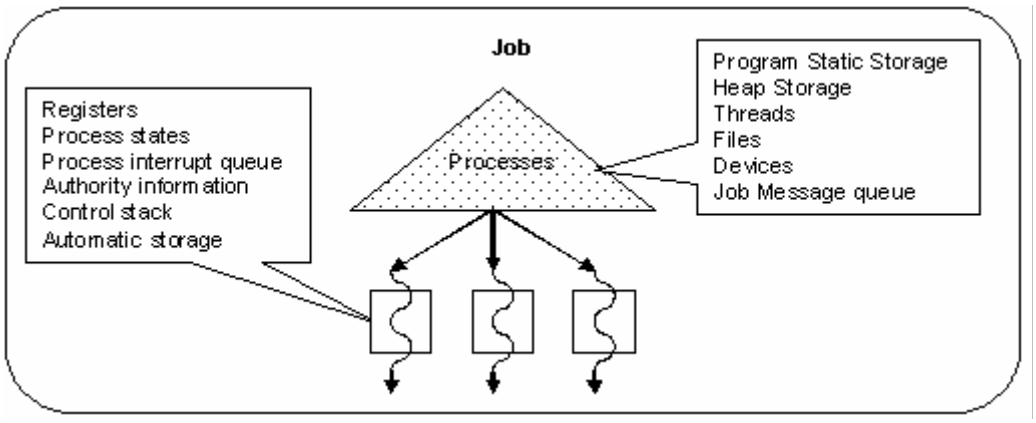


Figure 3.6 – Structure of a Job

The OS/400 uses jobs to manage a unit of work submitted by the user (figure 3.6). A job is an OS/400 construct that contains a process structure and other structures that are used to manage the system resources required to complete the unit of work.

AS/400 supports kernel level threads. In the kernel threads model, each thread within the process is a separate task (figure 3.7). With kernel threads, true concurrent operation occurs in a multiprocessor environment. Threads compete for scheduling with all other threads in the process and threads in other processes. The selection of the next thread to run in the processor is based on its priority (priority based scheduling). Unlike other platforms, there is no limitation to the number of threads that may be associated with a process.

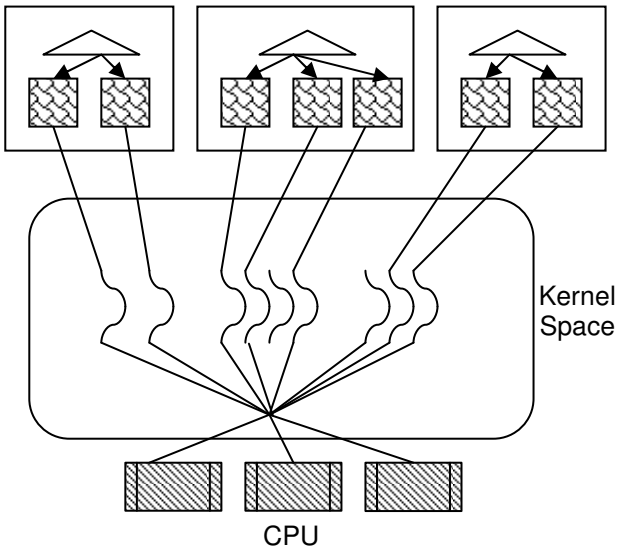


Figure 3.7 – Kernel Level threads

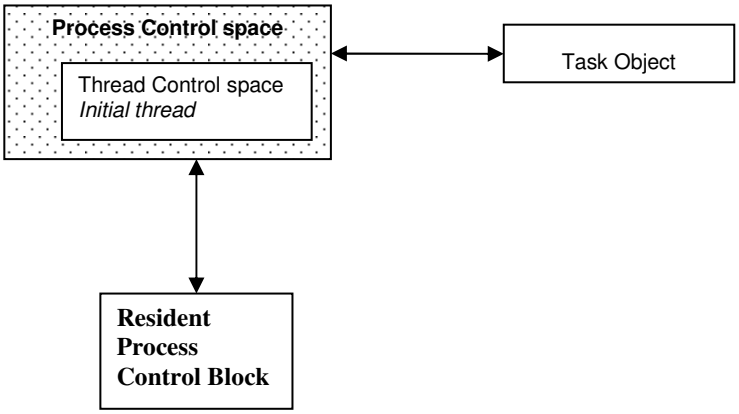
A process on AS/400 is composed of three main objects: a task object, a thread control space, and a process control space. The task object is the lowest level dispatchable entity on AS/400, commonly referred to as the task dispatching element (TDE). All dispatchable work is done within the construct of a task. It contains the hardware register state, priority, and other control information. The dispatcher controls the loading and unloading of the task object to and from the processors. Each thread contains a task object. There are four types of tasks on the AS/400: For further information refer [2.9].

Lightweight process task is used for threads. It contains a resident control block that is used to maintain status and control information that is unique to the thread.

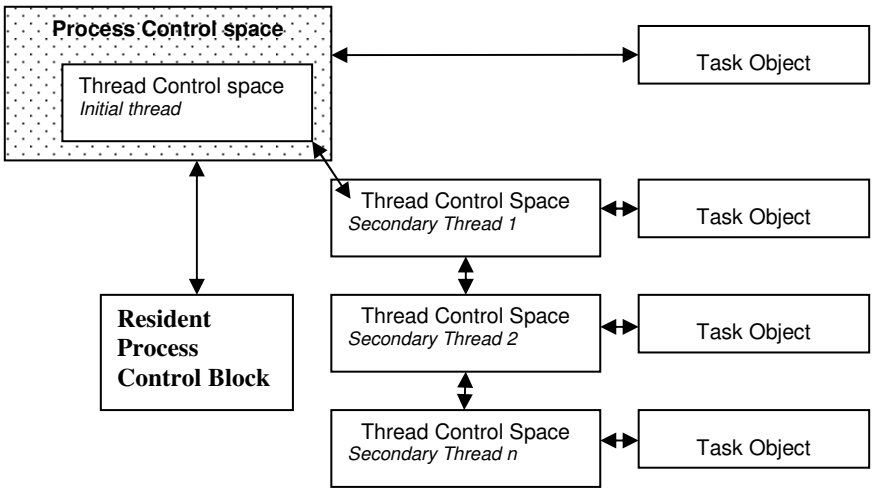
Nonresident task is used for normal SLIC functions such as communications or database functions. It can only execute code that is contained within the SLIC.

Resident task is used for SLIC functions that cannot incur a page fault while running.

Initial task is used only during Initial Program Load (IPL) of the machine



3.8 – A single threaded process



3.9 – Multithreaded process

Threads have two types of data associated with them, thread-specific data and thread-private data. Thread-specific data is defined by the application and is local to the thread. The data is shared by all functions running within the thread. Thread-private data is defined by the OS.

AS/400 threads are hierarchical. The initial thread of the process is special, in that if it is terminated by another thread all threads within the process containing the initial thread are terminated before the initial thread is allowed to complete its termination function.

Thread Management

The AS/400 support two of the leading thread management interfaces in the industry, the POSIX pthread interfaces and the Java Thread class. AS/400 supports all of the common synchronization primitives in the industry. The synchronization primitives available on AS/400 include: Compare and swap, Mutual exclusion

(mutex) locks, Semaphores, Condition variables, Threads, Space location locks, Object locks, Data queues, Message queues.

3.7.2 Deadlocks

Not like most other commercial OSs, OS/400 considers dead locks should be prevented. But in its actual implementation it does not prevent deadlocks, but try to recover from a deadlock. There is a special process, which runs with much higher priority. It checks the states of running processes if it found any program is not responding at could automatically restart the program. But this will result some sort of a data loss.

Applications develops are allowed to add customized recovery solutions or either extend the facility provided by OS. Domino exit program is such an exam which automatically restarts the Domino server when it seems server is not responding.

3.7.3 Memory Management

Memory management in AS/400 is similar to other systems other than different types of cache memories being used in the memory hierarchy. AS/400 used complex and intelligent set of algorithms to manage various cache memories [2.10.2]. Data must be in the memory in order to access and when new data need to be get in to the memory (when memory is not enough to hold new data) unused data is transferred back to storage and this storage is named as Backing Storage.

Storage is organized in to units called pages (page is 4KB) (called as segment when it is in memory) and page size is the smallest unit of data transferred from Storage to memory or other way round. This is similar to swapping.

3.7.4 Storage

OS/400 storage concepts tends to be bit different than other similar system with it own advantages.

Auxiliary Storage Pool (ASP) is a pool of storage devices, use does not see individual disks they only see and work with ASP. If user need access an objects he can not say which object is in which disk (but its some where within the pool). If you need to add a disk to the system you must add it to the disk pool. If any disk

needs to be removed user has to fist remove it from the storage pool (logically) then physically remove from the system. When a disk is removed the data in that disk is saved to other disks in the storage pool. But if some one directly removes a disk from the system data may be lost and storage pool becomes inoperable.

3.7.4.1 TeraSpace storage

All processes share a single, 64-bit address space, which is partitioned into 16 MB segments. Although the SLS (Single Level Storage) model provides many benefits to the AS/400 in terms of efficiency, scalability, and integrity, segmented storage poses a problem. There is no way to obtain contiguous storage in excess of 16 MB. The illusion of a larger contiguous storage can be created, but only with considerable expense in terms of program design and performance.

A teraspace [2.11.2] is a new temporary storage area, which provides a single process up to 1 TB of private storage. Teraspace storage overcomes the size limitation of segmented storage and thus meets the needs of memory intensive applications for large, contiguous storage. Teraspace storage also supports memory mapping. Memory mapping is used to efficiently access single-level storage objects, such as files, via memory accesses.

3.7.4.2 Hierarchical Storage

Hierarchical Storage Management (HSM) [2.11.1] provides an automatic and transparent way of managing and distributing data between different storage layers to meet the user needs for accessing data while minimizing the overall cost.

Figure 3.10 shows the most general way of data distribution in AS/400.The general theory is to place the most frequently accessed data in the higher-speed access storage components.

AS/400 single level storage (SLS) implementation manages the movement of data across the memory and disk interface. This implementation uses caching algorithms to ensure maximum performance of the disk storage layer by minimizing the number of data requests that must come directly from disk (disk paging). OS/400 provides hierarchical storage management on the AS/400 on all layers down to the disks.

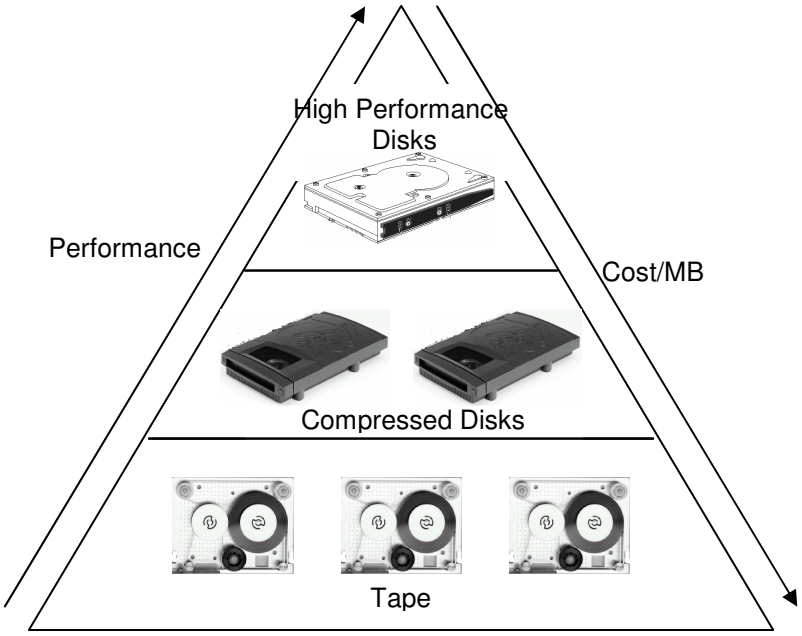


Figure 3.10 – Storage Hierarchy

HSM can be especially useful at organizations that maintain large volumes of historical information but do not require rapid access to that information. Data migration provides an automated, transparent management system that distributes data across the storage hierarchy.

Data migration

Migration (figure 3.11) is an operation in which selected data are physically moved to different ASPs. A typical use is to move data from a fast, high performance disk to a slower or compressed disk. This will allow more space on faster disks. Other way round is also possible (low speed to high speed).

When an application request for data, first it is checked at the top most storage in the hierarchy, then to the next layer like that. When data is found it is send to the top layers and application can access them. Application is not aware of the underline process what it will see is a delay in retrieving data.

Some of the benefits of this approach are;

1. Decreased total cost of storage by putting infrequently accessed objects on less costly storage devices while access to recent and historical data is maintained at the required performance level.
2. Because of HSM's potential to inexpensively expand AS/400 storage, cost justifying new applications such as data warehousing should be easier.
3. System availability can be increased by segregating historical data, which is by nature read only. Minimize the time required to backup data.

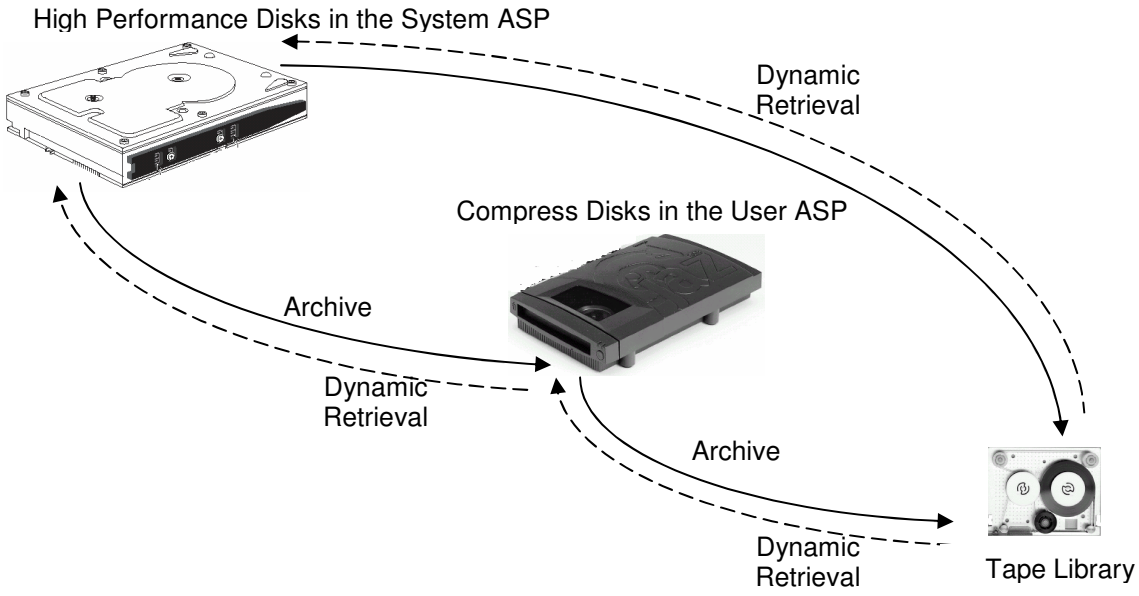


Figure 3.11 – Data migration

3.7.5 File System

A file system provides the support that allows users and applications to access specific segments of storage that are organized as logical units. These logical units are files, directories, libraries, and objects.

Each file system has a set of logical structures and rules for interacting with information in storage. These structures and rules may be different from one file system to another. In fact, from the perspective of structures and rules, the OS/400 support for accessing database files and various other object types through libraries can be thought of as a file system. Similarly, the OS/400 support for accessing documents through the folders structure may be thought of as another system.

3.7.5.1 Integrated File System

The Integrated File System (IFS) is a part of OS/400 that supports stream input/output and storage management similar to UNIX, while providing an integrating structure over all information stored in the AS/400.

AS/400 proprietary files systems were not enough to keep up with ever demanding technology changes and interoperability with other systems. The IFS enhances the already extensive data management capabilities of OS/400 with additional capabilities to better support emerging and future forms of information processing,

such as client/server, open systems, and multimedia. In simple terms IFS is a common interface to several separate file systems.

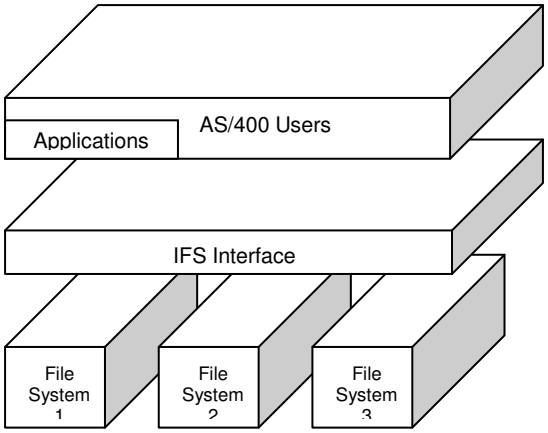


Figure 3.10 - Single interface to several file systems

The key features of the integrated file system are the following:

→ Support for storing information in stream files that can contain long continuous strings of data. These strings of data might be text of a document or the picture elements in a picture.

→ A hierarchical directory structure that allows objects to be organized like fruit on the branches of a tree.

→ A common interface that allows users and applications to access not only the stream files but also database files, documents, and other objects that are stored in the AS/400.

→ A common view of stream files that is stored locally on the AS/400. Stream files can also be stored remotely on a LAN server, a Novell NetWare server, another remote AS/400, or a Network File System (NFS) server.

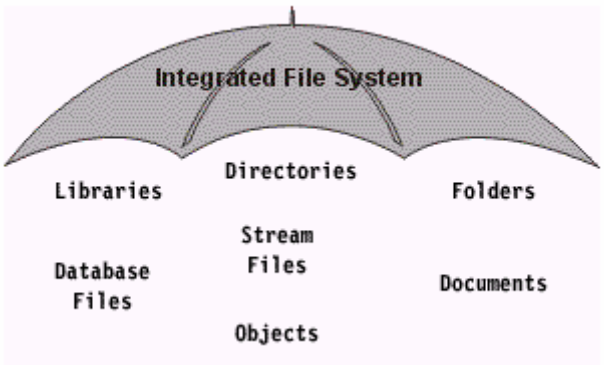


Figure 3.13 – All information stored in AS/400 under IFS

Before the IFS was added to OS/400 (prior to V3-R1), the QSYS.LIB (library file system) and QDLS (document library services file system) file systems existed simultaneously, but separately. Each file system had its own set of interfaces to

access its data. The IFS created a common set of interfaces and brought all file systems together.

Today IFS support large numbers file systems such as root (/), QOpenSys QSYS.LIB, QDLS, QLANSrv, QOPT, UDFS (User defined file system), NFS, QNTC (Windows NT Server file system), etc. Refer documents in biography [2.11.1] for more detailed explanations.

3.7.6 Logical Partitioning

Logical partitioning is a way of running multiple servers in a single server at the same time. It's much more cost effective than having several physical servers and it allows easy of management as well. But with the draw back of loosing every thing if the single serves stops working.

Users need to have separate systems when they need; multiple versions of the OS for different applications, different servers for different departments, same OS with different languages and time zones, different OSs (running Linux & Windows on AS/400), separate server for testing, firewall servers. Due to its higher availability some customers like to run Linux and Windows on AS/400 rather than PC servers (user can install and run those OS on top of OS/400 or use IBM e-Server x-Series).

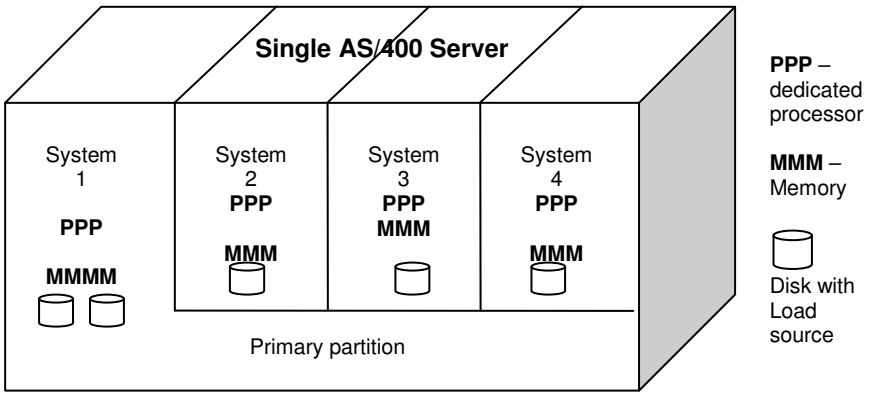


Figure 3.14 – Logical partitioning

Latest e-Server i-Series serves could support up to 32 logical partitions. But this depends on the number of multiprocessors in the system. Each logical partition runs separate copy of SLIC and OS/400 on its own processor (dedicated) and its main storage. So number of logical partitions is limited to the number of multiprocessors.

Logical partitions are divided in to two sections, primary partition and secondary partitions. Primary partitioning is the control body of all the other partitioning and

it defined polices for each partition. You need only to license to the primary partition. If something goes wrong with the primary partition, all other secondary partitions will be inaccessible.

Primary partition needs a minimum of 256 MB of memory and each secondary partition must have at least 64MB. Each partition must have a single disk to keep its load source (similar to boot information and system files in PC environment).

3.7.7 Clustering

V4R4 of OS/400 introduces clustering technology to support continuous availability (24x365). In a continuous availability environment, two or more AS/400s are joined together (clustered) to help ensure against system failures including planned shutdowns (e.g., maintenance, backups) and unplanned outages (e.g., power blackouts, operator errors). The group of connected systems is known as a cluster. The systems in a cluster can be physically connected via a LAN or a high-speed OptiConnect bus, or they can reside in different locations and communicate over telephone lines.

By taking advantage of clustering, application developers can improve availability (i.e. reduce downtime) and reduce user disruption for unplanned outages and planned maintenance. For example, without clustering, a disk drive failure might require the user to sign on to the backup system, restore data from backup files, restart the application, and reenter one or more transactions. At the other end of the spectrum, clustering support will ultimately make possible a planned switchover for scheduled backups with only a slight delay at the user's workstation.

A cluster resource group (CRG) specifies a recovery domain that defines a group of nodes and the role of each node in the group. A node can act as a primary node, a backup node, or a replicate node. They can work either active-active or active-passive. A recovery domain designates only one primary node, and that AS/400 is used to access resilient resources. A CRG can have one or more backup nodes identified in the recovery domain, each of which can take over for the primary node (active-passive). The recovery domain also defines the order in which backup nodes are activated.

In addition to the recovery domain, a CRG also specifies an **exit program** that is called for any event (node failure) that affects the recovery domain. By calling the

designated exit program for a CRG, OS/400 transfers control to a program so that appropriate actions such as application restart can be initiated. There is only one exit program per CRG.

Application level clustering is also possible based on the program. Each application has its own CRG and exit program. Giving each application its own CRG affords users the flexibility to transfer a specific application to a different server without impacting any other application. For example, you could use this strategy to balance workloads or to perform backups that only impact a specific application's resources (e.g. Blue Chip have a backup mail server when enabled which can work active-active by sharing the load).

Other clustering system services, while less visible, are still important because some functions can be implemented much more effectively at the OS level than they could be with any third-party product. IP address takeover (or IP takeover) makes it possible for multiple nodes in the recovery domain to have the same IP address at different times. (2 nodes can never have the same IP address at the same time.) IP takeover facilitates transparent switchover in a TCP/IP environment.

Above is just an abstraction, AS/400 clustering technology is much more complex and offers all sorts of options to make sure you have the best QOS (quality of service). Refer [2.13] for more information.

3.8 AS/400 Advanced Technologies

Over time AS/400 had evolved from a system with several dumb terminals to a system that meets today's e-business infrastructure with all sorts of new features. Some of the new capabilities include Java, Web serving and Web Sphere, Lotus Domino, integration with windows NT/2000, databases (DB2) and business intelligence solutions. AS/400 also continues to be a strong performer in growing areas such as data warehousing and Internet (already grown).

3.8.1 Java support

Today Java is the key application development environment for AS/400. AS/400 system takes the advantage of new functions and feature of this environment. The Java Virtual Machine (JVM) which resides below the TIMI (Technology Independent Machine Interface) layer enables fast interpretation and execution of

Java code on AS/400. A type of static compiler called class Transformer, which generates RISC machine codes from Java byte codes. Java transformer enables direct execution of Java on the AS/400 without the over head of interpretation.

Higher performance Garbage collection is provided by OS/400 to improve the performance and the scalability of Java. An advanced garbage collection algorithm allows Java to scale to the large number of objects expected when running enterprise applications on the server.

Over time, Java will become even more integrated with and tuned for OS/400 to meet the requirement of performance and scalability on the server without compromising the cross-platform portability of the rich language.

AS/400 developer kit for Java allows GUI applications to run on the AS/400 without modification. This is called Remote AWT (Abstract Windowing Toolkit). This interprets GUI requests coming from java program and re-route the request to an attached workstation running its own JVM. The workstation then interprets and displays the java.awt graphical components. This allows server programs which have GUIs for configuration or tuning to run on the AS/400 without any modification.

IBM strongly recommends all developers (for AS/400 environment) to be familiar with Java since they may not support certain application development environments in near future. For further details refer [2.14].

3.8.2 Web Serving

The IBM HTTP Server for AS/400 makes participating in the world of Internet and Intranets easy. This product combines the basic functions of a web server with expanded functionality that allows for grater flexibility in establishing a web presence. HTTP server support most common functions such as responding to browser requests, SSL security protocol, CGI, various user level access, integrating AS/400 security to the web, enhanced log reporting, etc.

IBM Web Sphere Application Server provides a framework for consistent, architected linkage between HTTP requests and business data and logic. It is for organizations that want to take advantage of the productivity, performance advantage and portability that Java provides for dynamic Web sites. It supports

Java Servlets, ORB (Object Request Broker), connection to backend databases and application services for session and management.

3.8.3 Lotus Domino

Lotus Domino is worlds leading workflow, messaging, groupware and web software. Blue Chip uses Domino 5.0.5 for their mail and web server. I had the opportunity of installing and configuring Domino 6.0 Enterprise Edition.

Domino allows;

- Powerful, flexible communications within and beyond any organization.
- World class collaboration and coordination with e-mail and groupware.
- Rapid Application development that meet any business requirements with an IDE (Integrated Development Environment) (similar to Visual Basic).
- Portability and interpretability (can run on verity of platforms)

Although Domino runs on Varity of platforms it is specifically designed for AS/400. So if any user needs to have optimum results he/she must run Domino on an AS/400. There are special AS/400 Domino servers which are specially optimized to run Domino. Running Domino on dedicated server is more cost effective and efficient than running on an ordinary AS/400. Domino server could be identified by its yellow stripe at the front.

3.8.4 Integration with Microsoft NT/2000

You could run Windows NT/2000 on an AS/400 if you are concerned on higher availability, high speed backups, improved data protection with RAID-V, etc. This feature provides the device driver to enable Windows NT/2000 Server to run on the AS/400 Integrated Infinity Server and to share AS/400 Disk, tape and CD-ROM drives. Similarly you could support Linux on latest servers as well.

3.9 Commercial Processing workloads

In PCs people to tend to measure system performance based on the clock speed of the processor. But it has become a bad yardstick because various other factors like level of piping, floating point and multimedia performance. So various rating like iCOMP index, Cyrix P-Rating and AMD P-Rating has evolved.

Evaluating the performance in a server environment is much more difficult. When AS/400 was announced in 1988 Relative Performance Rating (RPR) and Relative System Performance (RPS) of different models were measured a RAMP-C workload. This is a representative of genetic commercial processing. The AS/400 product line continues to grow in power with the PowerPC RISC processors and 12 way processors. With the increased processing power and as more and more applications utilizing vital technologies such as Web serving, Client Server, object Oriented and multimedia RAMP-C became obsolete.

RAMP-C was replaced by workload called Commercial Processing Workload (CPW) in mid 1996. CPW considers inclusion of batch components, various transaction types, increased path length, more complex file & terminal I/O. CPW is subdivided to client/server environment (batch) and interactive environment (interactive systems).

As an example consider 150 and 170 servers that Blue Chip uses. 2269 is the processor type of 150 server and 2291 is for the 170 (table 2.2).

Processor type	CPW – client/server	CPW – interactive
2269	20.2	13.8
2291	115	25

Many I/O interrupts in an interactive environment reduce the system performance considerably. Above values proves that as well.

3.10 Control Language Commands

As any other OS with a CLI (Command Line Interface) AS/400 also has rich set of command that allows manipulation of file, objects, directories, hardware resources, system utilities, etc. Control language commands are used every where, whether you use a menu, high level language, program product or system utility internally you are using those commands. System understands only those commands not a option number in a menu.

AS/400 command set is huge that it is impractical to remember all the commands, but when ever you want to do something you will remember the command. With my experience with other Operating Systems like MS-DOS, Linux and Sun Solaris; AS/400 command set is the most simplest and easily remembered command set I have ever used.

AS/400 control language command consists of two parts; verb and the subject. But there are few exceptions that do not fallow this rule.

Command = <verb abbreviation> + <subject abbreviation>

When ever you want to do something, write it on a piece of paper in simple English (or do this in the mind) then find the verb and the subject. Get the abbreviation of the verb and add it to the abbreviation of the subject.

Example: If I need to check messages to me, my request would be "Display Message" so the command would be DSPMSG

Description	Verb	Subject	Command
Display disk status	Display	Disk status	`DSPDSKSTS`
Work with problem	Work	Problem	`WRKPRB`
Start TCP/IP service	Start	TCP/IP service	`STRTCP`

Commands like DLTF (delete file) and DSPJOBB (Display job description) does not fallow the exact rules; either because it's considered to be an overhead typing several character(DELF) or either there may be another similar rule (display job DSPJOB and DSPJOBB) conflicting with it.

If you are still not being able to find the exact command context sensitive help is always available. You could either type part of the command with wild cards or could search the list of all the available commands.

Each menu has a unique name. If user needs to go to a specific menu use GO keyword before the menu name. As an example to use the menu "work with licensed programs menu" use the command "`GO LICPGM`"

3.11 How to install OS/400

Installing OS/400 does not drastically differ from installing any other CLI based OS. You could either load files from a tape driver (old fashion way) or use CD/DVD ROM. OS/400 could only be installed using CLI (green screen) through a consol attached to the system.

It is impractical to present every single step in the installing process in this report mainly because it would need 8-10 pages. So my effort is to present only the important points and decisions during the installation process.

OS/400 installation could be done in several steps depending on the requirement. At minimum user has to install Licensed Internal Code (LIC) and the OS. Figure 3.15 indicate all the possible installation steps.

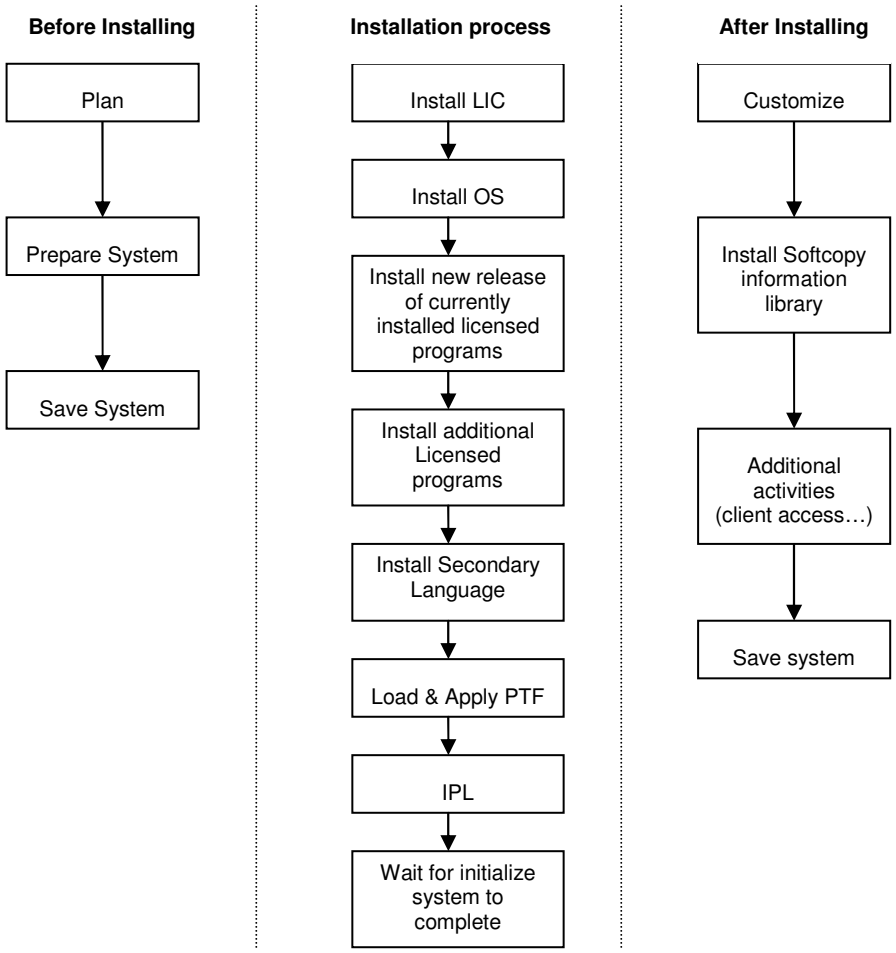


Figure 3.15 – OS and Licensed Programs Installation Process

You could install the OS when LIC (Licensed Internal Code) is already installed. But if the LIC version and the OS version that you are planning to install is different you have to install or upgrade the LIC first.

3.11.1 How to install LIC

Step 1 : Do a manual IPL from external load source

`Select` **`D M`** `from System control panel and press Enter Button`

D – Load from external source (used when doing a IPL for the fist time using external media such as tape, CD or DVD ROM)

M – Do a manual IPL (Initial Program Load is similar to booting a PC)

Step 2 : Insert the tape or CD-ROM (DVD) to the drive

If your are using CD/DVD ROMs insert the CD/DVD labeled Base Pack - SLIC

Stpe 3 : Now system is on IPL stage

`Keep an eye on the display area of the System control panel to see any attention message is there. If system is showing attention check the error code on the manual and do necessary corrections`

Step 4 : Select Language group

Select the language to be used
Default is English and it is denoted by number 2924
Press Enter key

```
                    Select Language Group

Language feature ……2924
```

Step 5 : Adding disks to ASP

User must add all the disks to the ASP

Select Option 2 to work with DST (Dedicated Service Tools)

```
              Install Licensed Internal Code

Type Choice, Press Enter

1.     Install Licensed Internal Code
2.     Work With DST
3.     Define Alternative Installation Drive

Selection …2…
```

You need to sign on in order to access DST
Factory default username & password is 22222222
After typing the password press enter (you can change the password later, password before V5-R1 are not case sensitive)

```
          Dedicated Service Tools (DST) Sign On

Type Choice, Press Enter

DST User…… _________
DST Password…… _________
```

```
            Use Dedicated Service Tools (DST)

Select one of the following:

1.     Install Licensed Internal Code
2.     Work with disk units
3.     Work with DST Environment
4.     Start a service tool
5.     Work with remote service tool

Selection   _2_____________________________________

            F3 - Exit           F12 - Cancel
```

Select option 2 to work with disk units
A disk needs to be initialized and format before use. Formatting will remove all the data in the disk.
If disks are using parity for better protection before formatting you have to stop the parity protection.

Select option 5 and press enter key

```
                    Work With Disk Units

Select one of the following:

1.     Save load source disk unit data
2.     Copy load source disk unit data
3.     Display/Change page data
4.     Analyze disk unit surface
5.     Initialize and format disk unit
6.     Reclaim IOP Cache storage
7.     Stop device parity protection

Selection   5

       F3 - Exit           F12 - Cancel
```

Step 6 : Installing LIC

```
Disk selected to write the Licensed Internal Code to:
Serial No     Type   Model  I/O Bus  Controller Device
68-572f3      6607   074     0           1         0

Select one of the following:

1.     Restore LIC
2.     Install LIC and Initialize the System
3.     Install LIC and Recover configuration
4.     Install LIC and Restore disk unit data
5.     Install LIC and upgrade load source use for
       upgrade

Selection   2
```

Based on the requirement select applicable option
If you need to install the LIC and then initialize the system select option 2 and press Enter key.
You have to install LIC if OS and LIC versions are different you must install LIC

3.11.2 When LIC is already installed

Step 1 : Do a manual IPL from load source

Select **B M** from System control panel and press Enter Button

Step 2 : Wait sometime until “IPL or Install OS menu” appears

```
IPL or Install The System

Select one of the following:

1.     Perform an IPL
2.     Install the Operating System
3.     Use Dedicated Service Tools (DST)
4.     Perform automatic installation of the Operating
       System
5.     Save Licensed Internal Code

Selection   5

       F3 - Exit           F12 - Cancel
```

If you want do a LIC update select option 5

```
If you want to use dedicated services tools to add or format disks
select option 3
If you need to install OS select option 2
```

Step 3 : When you do an IPL from load source you get more options on DST than earlier

```
User could add to ASP, initialize or format disks
After adding disks, to install the OS select option 2
```

```
Use Dedicated Service Tools (DST)

Select one of the following:

1.     Perform an IPL
2.     Install the Operating System
3.     Work with Licensed Internal Code
4.     Work with Disk Units
5.     Work with DST Environment
6.     Select DST Console mode
7.     Start a service tool
8.     Perform automatic installation of the OS
9.     Work with save storage and restore storage
10.    Work with remote service support

Selection   2

       F3 - Exit           F12 - Cancel
```

Step 4 : Confirm the which language to use

```
Language feature ……..     2924
Confirm Language by Enter of F12
```

Step 5 : Select whether you like to have more options while installing or to use default installation

```
Install the Operating System

       Install Option 1
              1 - Take default
              2 - Change install options
```

Step 6 : Set data and other environmental variables

```
Date:
              Year…… 03        00-99
              Month…… 08       01-12
              Date…… 12        01-31

Time:
              Hour…… 13        00-23
              Minute…… 16      00-59
              Second…… 49      00-59
```

```
OS/400 Installation System

Stage 2:
       +---------------------------------------------+
       | |||||||||||||||| 32%                        |
       +---------------------------------------------+
Installation stage

1.     Creating needed profiles and Libraries  : X
2.     Restoring programs to library QSYS      :
3.     Restoring Language objects to library QSYS :
4.     Updating Program table                  :
5.     Installing database files               :

Completing the OS/400 Installation
```

Step 7 : After successfully installing the OS you would get the sign on menu

```
Sign On
                                System        S4412F22A
                                Sub System    QSYSSBSD
                                Display       DSP01

       User ..........._______________
       Passowrd ..... ......_______________
       Program/Procedure ..........._______________
       Menu..........._______________
       Current Library..........._______________
```

When you login for the fist time, use "qsecofr" for the username and password. System will prompt the user to change the password after sign in.

qsecofr has the highest authority and it is similar to Administrator (Windows) or root (UNIX) user accounts.

Step 8 : After sign in user gets the AS/400 main menu.

Options available in the main menu may vary depending on the user privileges.

```
AS/400 Main Menu

Select one of the following:

1.     User Tasks
2.     Office Tasks
3.     General System Tasks
4.     Files, Libraries and Folders
5.     Programming
6.     Communications
7.     Define or change system
8.     Problem handling
9.     Display a menu
10.    Information assistance options
11.    Client Access options

90.    Sign off

Select or command
➔ _____________________________________________
_____________________________________________

F3 - Exit     F4 - Prompt   F9 - Retrieve F12 - Cancel
C Copyright IBM Corp 1980-2000
```

Step 9 : Licensed programs could be installed after sign in to the system.

```
Use work with licensed programs (GO LICPGM) command to go to the
appropriate menu.
```

3.12 Other features

AS/400 has lot more concepts and feature than what I have discussed here. Above is just an abstraction of some of the concepts that I fell that should be presented. For more information refer references given in [2]

Some of the other concepts include;

- AS/400 shared memory concepts
- Extended adaptive cache
- Server consolidation
- High availability
- Wireless on i-Series
- Backup and recovery support
- TCP/IP Services

And feature such as;

- Enhanced business intelligence
- OS/400 directory services
- Web Sphere
- DB2 support
- Java Beans

.

4

Network Security

"The whole is greater than the sum of its parts"

During my industrial training I worked with range of network security products from WatchGuard and Trend Micro. This chapter introduces some of the theoretical concepts, technologies, network security threats and need for devices such as Firewalls, ID systems, server protection mechanisms and enterprise level anti-virus solutions. I was able pass the WatchGuard certification exam conducted by WatchGuard training center and obtained the "WatchGuard Certified Professional" certificate.

4.1 Introduction

Originally computers were stand alone units; it was not a really big issue protecting what ever on those machines. Soon large scale users begin interconnecting those computers for the ease of exchange of information. Although advantages of interconnecting those machines are immense, the potential threats are higher as well. With the introduction of Internet and almost every organization having some sort of connectivity to Internet these threats are becoming much more series, organizations or home users will not survive unless they use adaptive, preventive and corrective mechanisms. Security is not one a step process, it should be monitored, evaluated and adapted according to varying security threats.

Organizations demand for better, flexible and secure service, but prevent outsiders and those with malicious intent from damaging systems and critical data. No single product can perform all of the necessary tasks. It is not either protecting at the desktop level (or server) or protecting at the entry point (internet gateway) to the network. A **defense-in-depth** approach to security is needed to protect any investment. Businesses of all sizes are advised to combine the fallowing in to holistic security solution that meets their type of business.

- Awareness and Commitment
- Firewall
- Network and System Monitoring
- Access Control & Authentication
- Auditing
- Anti-Virus
- Encryption
- VPN
- Server Integrity

4.2 Security Policy

Many people understand that they need to protect thing but they do not understand the need of a policy. A security policy is a compromise that an organization decides to adopt between absolute security and absolute access. A fully formed security policy spells out who can get in, where they can go, and who can get out. And it should also consider controlling of physical access to rooms, devices (routers, firewalls), Servers and how to protect data cartridges (tapes). There is no point spending millions of rupees on Firewall(s), antiviral solutions, ID (Intruder Detection) systems while you keep your Server Room door open [3.3].

For example, a security policy might specify that certain IP addresses on the Internet may not contact anyone or anything within an organization. It might also state that certain computers within the organization are accessible only by accounting, top-level management, or marketing team. It might further establish that other computers on the Internet cannot directly access any computer within your organization; instead, all outside traffic may only contact your Firewall.

Benefits of a policy

Publishing a security policy and the reasoning behind it, to the entire organization provides at least three benefits;

i. Users gain a sense that the organization is looking out to protect their files and their livelihood.
ii. Users often find that they have access freedoms they were not previously aware of.
iii. Users gain an understanding that access limitations are implemented to protect the organization from disaster.

4.3 Vulnerability Window

Is the time gap between the first attack and until you get ready to face it (before it hits you). In order to be protective against immerging threats Larger Vulnerability Window means your are more vulnerable to attack so it should be minimized. This should be the whole purpose of your security solution partner.

As an example consider at 6.30 am (time is in GMT) some where in USA first attack happens (attack could be virus, worm or any thing destructive), and attack continues spreading. At 8.00 am your security solution provides got to know such an attack is there and start working to fight against it. During that time attack is still

spreading all around the world. At 12.25 pm India also gets infected hope fully still you are safe. Your security solution partner comes up with a solution at 2.45 pm. And you are able to apply the patch at 3.35 pm and hopefully ready to face the challenge (unless you are not already attacked). The time gap between 6.30 am and 3.35 pm is the size of your Vulnerability Window (09:05). Size of the window could be several hours or sometimes several days. Task would be to minimize it

4.4 Firewalls

Lot of techniques such as Proxies and Intrusion Detection (ID), were implemented to prevent and detect attacks, but these solutions were unable to guard against new treats that are immerging, they only support protection against already know threats. To protect against the Internet's inherent security threat, the Firewall was created as a new class of network device. Three historical trends led to the development of Firewalls as a class of network protective device.

- The increasing reliance on the Internet for commerce, research, and collaboration
- Rise of the Internet as an avenue of unauthorized access into corporate networks
- The costs associated with that unauthorized access

4.4.1 What is a Firewall?

A Firewall is a device that protects the resources of a private network from intrusion from outside the network. Basically, a Firewall examines each network packet to determine whether to forward it to its destination or to discard the packet.

4.4.2 Need of a Firewall?

Banks employ armed guards to ensure that customers don't get behind the counter, and to be on the alert for potentially threatening situations. Similarly Firewall prevents unauthorized people from getting into networks and will also prevent passage of unauthorized traffic. The Firewall has become corporate security's most common tool and a crucial first step to solid defense-in-depth.

A Firewall management policy is a subset of the organizations security policy. It specifically addresses how an organization's network Firewall(s) are configured to contribute to the overall security policy. A Firewall management policy determines:

- Which hosts send and receive which kinds of traffic
- What communication protocols and content types are allowed
- Which communication links require authentication and/or encryption
- Which users are authorized to use various services through the Firewall
- What times of day organization members are able to browse the Web
- What types of Web sites organization members can visit

Firewalls are the current industrial standards to prevent most of the attacks (not limited to specific type of attack, it is an instigation of several services) coused by hackers through Internet. Fallowing section discus Firewalls in detail.

4.4.3 Stance of a Firewall

The stance dictates what the Firewall does with any given data packet, in the absence of explicit instructions. The default stance of a Firewall is not to allow anything in (as accepted by the Internet security community) which is not specifically allowed. Firewall administrator can define what sort of services to allow, if any service is not allowed it will (should) be discarded.

This protects against attacks based on new, unfamiliar, or obscure IP services. It also provides a safety net regarding unknown services and configuration errors that could otherwise threaten network security.

4.4.4 Technology

In simple terms Firewall filters packets. All Internet traffic travels in the form of packets. Packet has two parts which is the header (properties such as source & destination address, type of protocol, error correction, etc.) and the data (what user really want to send).

In packet filtering; header (protocol and address information) of each packet is examined and its contents are ignored. Then header information is checked against the rules (also called policies) assigned by the administrator. If that packet is according to the rules, it is accepted to transmit (either incoming or outgoing) other

wise it will be denied. Incoming packets and outgoing packets are considered separately and administrator can assign different rules based on the direction they travel. Packet filtering works on the Network and Transport (TCP/IP) Layers of TCP/IP.

Packet filtering alone is very effective as far as it goes but it is not foolproof security. Firewalls allow another method called Circuit Relay. Circuit Relay assigns several rules based on nonheader information, such as who wants to communicate, at what time of the day it is allowed, which user is allowed to use the service, etc. Circuit Level filtering takes control a step further than a Packet Filtering. The third approach to Firewall is Application Gateway it also called as Security Proxy.

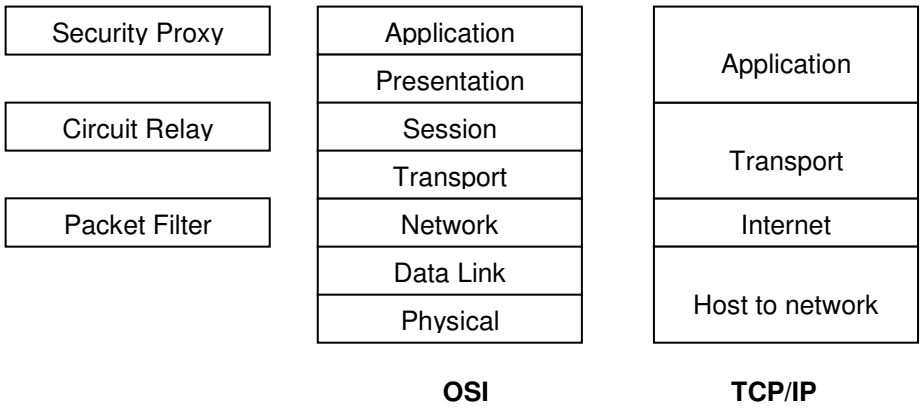


Figure 4.1 – Packet filleting at different OSI and TCP/IP layers

Proxy

In the word of network security the word proxy can be used to refer to many different things. In generally proxy is a software program that intercepts Internet data packets, examine the content and take some action to protect the system in which the traffic is intended (a server). In terms of security terms such as "Security Proxy", "Transparent Proxy", "Application Layer Proxy," refers to the same thing.

In this approach Firewall goes beyond both packet filtering and Circuit Level filtering. Security Proxies work on the Application level (OSI layer 7) and examine its content for validity. In doing so, the proxy determines if there is a forbidden content type hidden or embedded in an allowed packet (by filtering rules). Each packet received by a proxy is stripped of its wrapping, analyzed, processed, re-wrapped, and forwarded to its intended destination. It takes some time to unwrap, analyze and rewrap a packet as a result throughput decreases slightly.

Figure 4.2 show the logical sequence of a Firewall with Security Proxies. If administrator decides he only needs packet filtering he/she could forward packet to the destination just after packet validation (packet filter rules) without forwarding to the next level (Circuit Relay).

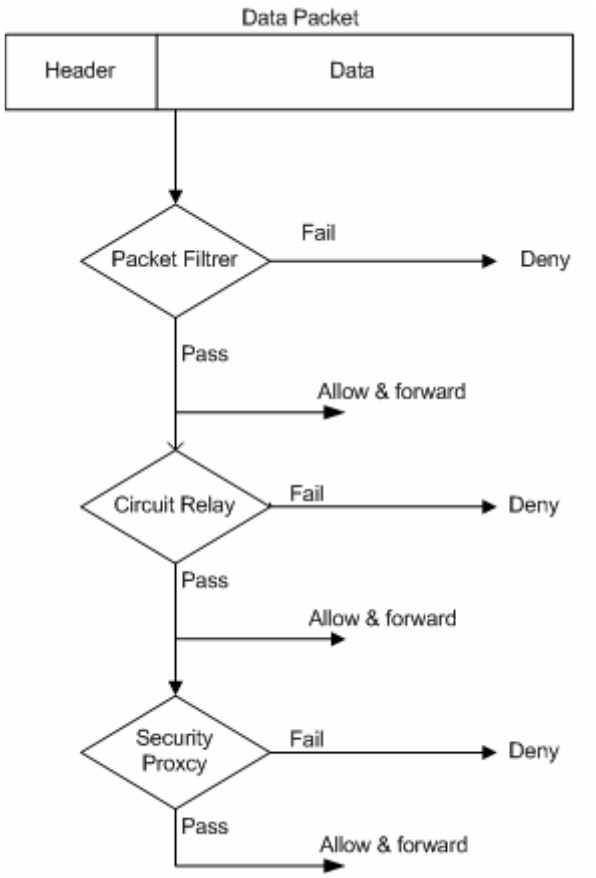


Figure 4.2 - Logical Sequence of a Firewall with Security Proxies

Proxies offer fallowing advantages;

→ Proxies make networks harder to hack by blocking entire categories of commonly used attackss

→ Proxies make networks harder to hack by concealing details about internal network servers from the public Internet

→ Proxies help to use network bandwidth more effectively by preventing unwanted or inappropriate traffic entering to the network

→ Proxies reduce corporate liability by preventing a hacker from using networks as a launch point for further attacks

→ Can simplify the management of networks by providing administrator with tools and defaults that can be applied broadly, rather than desktop by desktop

4.4.5 Where does it fit in?

Since Firewall is supposed to control both incoming as well as outgoing traffic it should stay at the entry point (gateway) to any network. It should physically stay (in terms of wiring) between the Router and the network (see Figure 4.3).

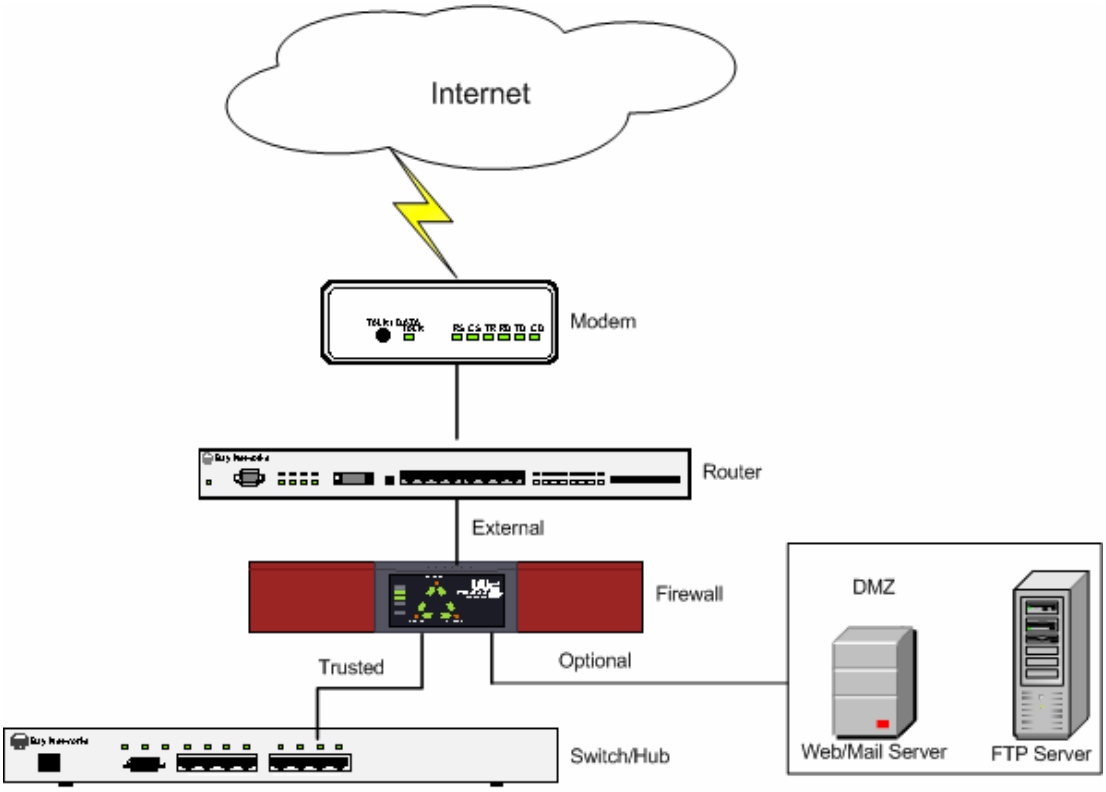


Figure 4.3 – Physical location of a Firewall

Medium and large scale Firewall normally has three interfaces but optional interface may not be available on small scale ones (used for SOHO) but could have several trusted interfaces (act as a hub/switch).

External Interface - connection to external interface (typically Internet)

Trusted Interface - connection to internal interface which needs maximum protection

Optional Interface - connection to DMZ or free areas. Public Web, e-mail FTP, DNS servers could be connected here

4.4.6 Terminology

Before proceeding further it would be better to introduce some of the keyword and abbreviations that is used in next few sections.

4.4.6.1 DMZ

Demilitarized Zone is the place where you keep your publicly available services such as Web, mail and FTP services. Servers in the DMZ are physically separated (not in the same physical wire) from internal network for better security. See figure 4.3.

4.4.6.2 Network Configurations

Firewall protects a wide array of private networks and/or hosts by representing them as a single IP address (its external IP address). Whether you have a single network behind the Firewall, a few networks, or a group of disjointed networks and random addresses assigned to specific hosts, they are grouped into a Firewall compatible network configuration. Three types of configurations have being identified; Simple network (Drop-in), multiple (Routed) network and Secondary network configuration.

Drop-in network

As the word drop-in implies; something dropped in to already existing network. No IP address change behind the Firewall is necessary (same host IP addresses). Firewall, router and private network uses the same IP address range. See figure 4.4.

Routed network

In here at least two of its 3 interfaces have different network address ranges (figure 4.4). It requires user to change internal IP addresses unless network is build from a scratch. But this configuration is more suitable in terms of security and management.

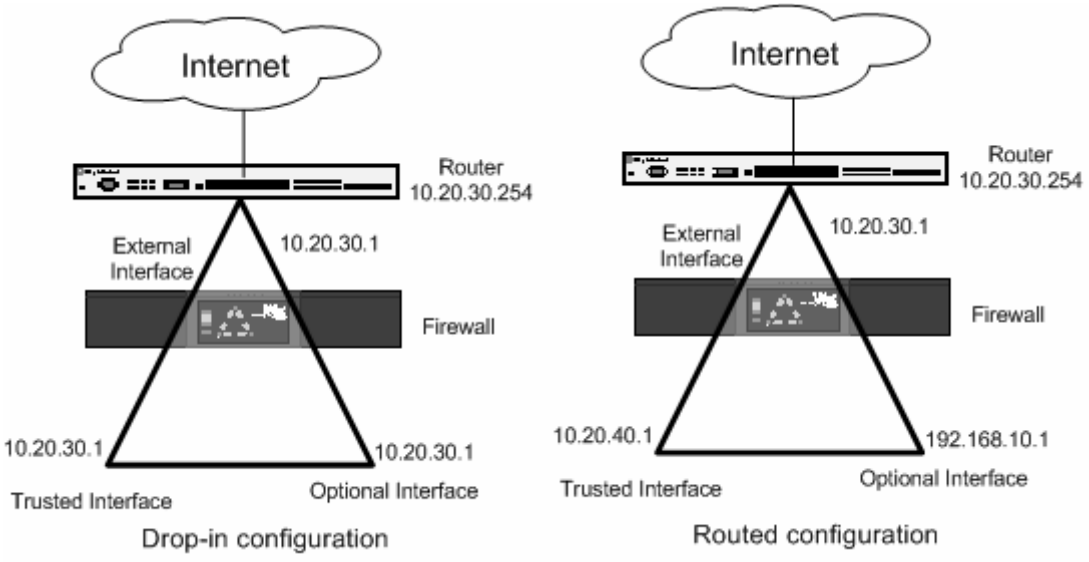


Figure 4.4 – Drop-in and Routed configurations

Secondary network

Secondary Networks are networks on the same physical wire as the Firewall's interfaces which having IP addresses that belong to an entirely different network (figure 4.5) When adding a Secondary Network to one of the Firewalls interfaces, user map an IP address from the Secondary Network to the IP address of the interface. This is known as creating or adding an IP alias to the network interface for the Secondary Network. This IP alias becomes the default gateway for all the machines on the Secondary Network

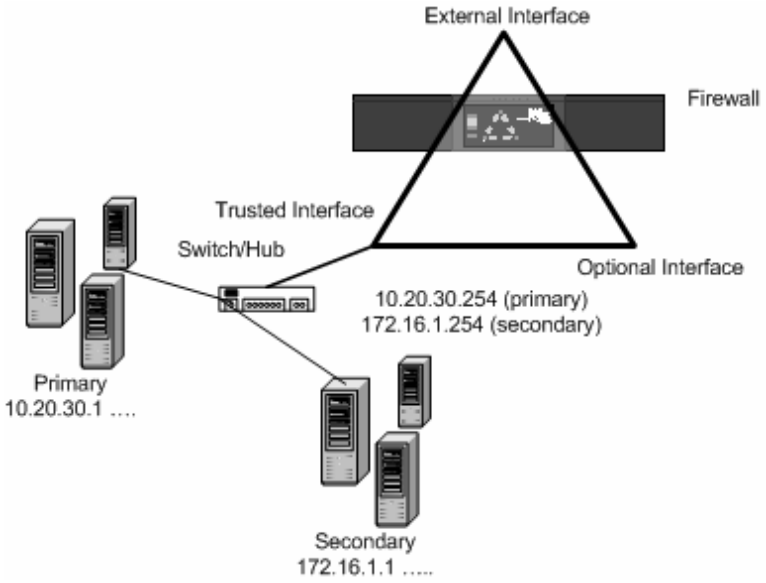


Figure 4.5 – Secondary network on the same physical wire

4.4.6.3 Network Address Translation (NAT)

Also referred as "IP masquerading" or "port forwarding". NAT takes IP addresses on one network and translates them into IP addresses used within another network. NAT hides network addresses from hosts on another network. Hosts elsewhere see all the outgoing packets as coming from the NAT supported device (either Firewall or PC which NAT software runs).

This improves security by mapping private addresses to public address(es). NAT conserves the number of public IP addresses an organization requires. More importantly, NAT allows use of a single public IP address for all outgoing and incoming communication, which keeps trusted addresses secure. Several types of NAT configurations are exist;

Dynamic NAT

Outgoing source IP addresses are translated into the IP address of the external interface. Incoming packets are translated from the external interface's IP address into the appropriate private IP address. Communication should always initiated from inside therefore public Web or mail sever cannot work with Dynamic NAT you need either 1 to 1 NAT or static NAT.

1 to 1 NAT

Incoming public IP addresses are translated into specific private IP addresses.

Static NAT

Assigns a specific port to a given service to another port internally, so that originators of incoming traffic never know what host is actually receiving the packets. Used for public servers behind the firewall.

4.4.6.4 User Authentication

User Authentication is used to confirm users who they say they are. Authentication is done based on the username and passphrase (password). When used by firewalls (or any other authenticating server like RADIUS, SecureID, NT Domain controller), authentication allows network administrators to define security policy rules based on users and user groups, instead of simply IP, network addresses or host name.

4.4.6.5 Virtual Private Network (VPN)

VPN is a technology which allows a logical private path (channel/tunnel) in a public path. It creates an end to end (between two VPN gateway devices or PC and a VPN gateway device) secure, encrypted channel through Internet or even on LAN. Which make sure mobiles users, home workers, branch offices and Extranets can communicate with each other or with the head office without the risks of some one intercepting their traffic. VPN uses IPSec or PPTP protocols.

4.4.6.7 URL Filtering

URL filtering let the administrator to control web site access privileges. Web surfing can be restricted based on the user, group, time of day, web site or content of the page. Filtering checks the request of a site with the filtering database, if a certain URL is in that database access to particular site (or page) is prohibited. For optimal performance the database should be updated from time to time.

4.4.6.8 ASIC Architecture

ASIC stand for Application Specific Integrated Circuit; the application is hardcode to the chip. It eliminates some of the bottlenecks in 1st and 2nd generation (section 4.4.7) Firewalls. The PC system bus carries traffic between network cards (NIC) and

the CPU. When used as a Firewall with an encryption accelerator, the system bus must also support the traffic between the CPU and the accelerator device. To visualize this arrangement, see the figure 4.6, which shows how all of the devices must communicate using the same system bus. This conventional configuration allows only one signal at a time (if multiple processes need to use the bus, all but one must wait for their turn). So the system bus becomes the bottleneck by reducing the throughput

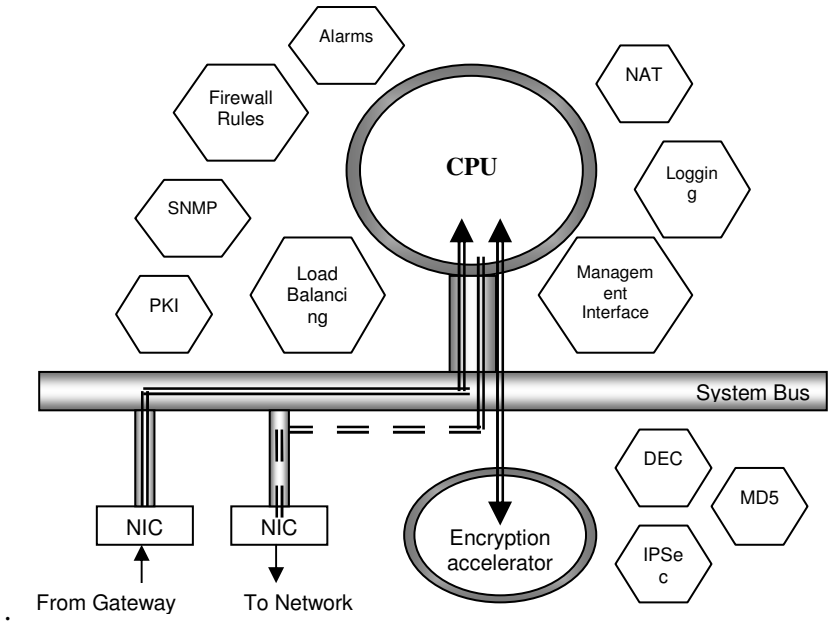


Figure 4.6 – Data communication in ordinary Firewall

The traditional ASIC appliance combines a host processor and bus architecture with a special chip that handles common tasks. In this architecture, many of the steps are compressed onto the ASIC, improving processing efficiency since the system bus is no longer required since those chips can carry out there own tasks. In ASIC architecture, pure network operations such as packet handling and IPSec acceleration are done directly in the ASIC, while Firewall policy enforcement, NAT, load balancing, and packet classification are done on the host CPU through system bus.

Early ASIC designs were limited, because once programmed, they could never be updated to run new software or to add functionality. Intelligent ASIC was introduced to overcome some of the problems. The Intelligent ASIC combines the speed of the traditional ASIC with the flexibility and scalability of a general purpose CPU. An Intelligent ASIC has several general purpose CPUs built in, allowing it to adapt to new technologies. With flexible computing power on board,

the intelligent ASIC no longer has to query the host CPU for every packet. Instead, when it receives a new packet, it queries for the active security policy for that type of traffic, stores it in cache and uses it to process all other packets in that data stream. This design eliminates the all packets to require a call to the host CPU, and prevents the system bus from becoming the performance bottleneck. Because the intelligent ASIC makes fewer calls to the system bus, it is inherently capable of higher throughputs.

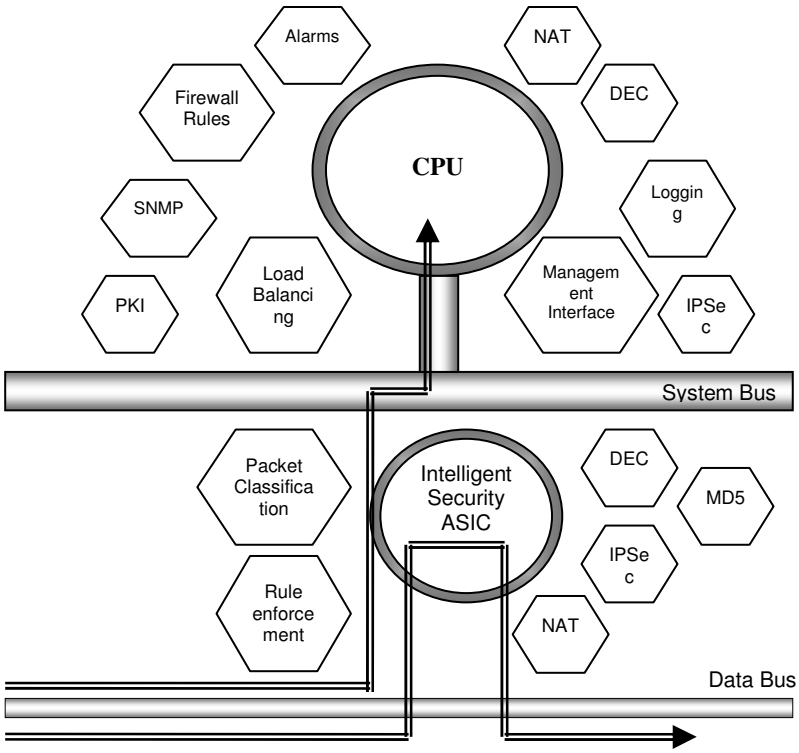


Figure 4.7 – Intelligent ASIC architecture

4.4.6.9 Attacks

There are several kinds of attacks that cannot defend against by basic packet filtering and proxies. Fallowing are some of the well known attacks;

Spoofing attacks

Where hackers alter packets to create a false identity (IP address that Firewall allows in) for the purpose of gaining access to the network

Port space and Address space probes

Where hackers attack ports (or IP addresses) sequentially in search for security holes they can exploit. If the firewall is able to keep track of pass transactions (stateful packet filtering) it can guard against both port and address space attacks.

Use of IP options

Optional header of TCP/IP packets are normally used for debugging and special applications on LANs. Attackers can use it to specify a route for a packet to fallow in order to fool the Firewall.

SYN flood attacks

Where hackers try to deny service to legitimate users by overloading networks with illegitimate TCP connection attempts.

When an attempt is made to initiate a connection between a client and server using TCP, a three-way handshake occurs before the connection is successfully established. As part of the handshake, the server attempts to verify that the connection attempt is originating from a valid client address. Once the server verifies the client address is valid, the connection is completed.

A SYN flood attack overloads the server (target) with connection requests that have bad source IP addresses. Because the requests have bad addresses, the server cannot verify that the addresses are valid and cannot complete the connection. A flood of unverified requests causes the server to begin ignoring legitimate incoming requests thus denying users service.

4.4.7 Generations of Firewalls

There is bit of confusion in defining Firewall generations. Over time Firewalls had several significant improvements, based on those improvements people have defined of three generations. Definition of Firewall generations are bases on whether it's purely a software based Firewall or hardware based Firewall.

The term software based Firewalls refer to the software programs which stay below the application layer (either OSI or TCP/IP) and check IPs, ports as well as protocol. They run either on a PC (e.g. Norton Personal Firewall, Sygate Personal Firewall) or a Server (Linux Firewall, Microsoft ISA).

Hardware based Firewall refers to a standalone or rack mounted device with special hardware, hardened OS and limited set of software for Security Proxies and management (e.g. CISCO Pix, WatchGuard).

Software Based Firewalls

1st generation - Packet filtering bases on IP address, Port number and Protocol

2nd generation - Stateful (dynamic) packet filtering by keeping track of packet state. Able to detect SYN flood attacks, address/port space probes, address sniffing and address spoofing.

3rd generation - Application Proxy. Checking the data section of packet to catch the forbidden content types.

Hardware based Firewalls

1st generation - A dedicated PC in a box. CPU has the control over all the functions and almost everything is carried out by respective software program.

2nd generation - A dedicated device with more electronics than 1st generation. Services like encryption and IPSec is done using a dedicated IC. Still the processor has full control of all the services.

3rd generation - Use ASIC architecture (section 4.4.6). Certain services are given to specific ICs, and it carries out service without processor intervention. Considerable increase in the throughput.

4.5 WATCHGUARD®

Figure 4.8 – WatchGuard® Firebox III™ (Firebox & SOHO) and V-Class models

During my training at Blue Chip I was able to learn, install, configure and troubleshoot WatchGuard FireBox III and ServerLock.

4.5.1 Introduction

WatchGuard is a leading provider of dynamic, defense-in-depth Internet security solutions. WatchGuard's award-winning Firewall appliances and server security software, combined with the innovative LiveSecurity Service™, deliver up to date Firewall and VPN technology, and Server/Application security to protect any size network from the perimeter to the core. Unlike traditional Firewall solutions that are difficult to deploy and keep up to date, the WatchGuard Firebox System III and V-Class is easy to install and manage from a central location, and comes with a unique service that delivers timely updates directly to user desktop.

Blue Chip is the only authorized resellers of WatchGuard products in Sri Lanka. WatchGuard Firebox™ is becoming highly popular because of its easy of

configuration and management as well we as its low cost compared to other Firewall products in the market. WatchGuard Fireboxes™ III comes in 5 different flavors, Firebox 4500, Firebox 2500, Firebox 1000 Firebox 700 and Firebox 500. Firebox III is specially designed for small to medium scale organizations. Capacity (throughput, number of concurrent connections, VPN users, etc.) of each Fireboxes various according to its number, (i.e. Firebox 4500 has the highest capacity and 500 has much lesser capacity).

Firebox SOHO6 (Small Office Home Office) is designed for small business with up to 10 users (upgradeable to 25). Recently WatchGuard introduced the wireless version of Firebox for businesses with WLANs (SOHO wireless)

WatchGuard VClass™ is designed for medium to large scale business (enterprise class) which having large number of concurrent uses and with high speed connections; such as Data centers and ISPs (as a value added service). It can support 10/100 Mbps and Gigabit Ethernet connections as well. VClass™ uses intelligent ASIC architecture and it has passed lot of benchmarks tests and it's considered to be the beset, compared to other competitive products in the market.

4.5.2 Configuration

Service	Incoming		Outgoing		Properties
	From	***To***	***From***	***To***	
HTTP	Any	Web server	Any	Any	Port 80
FTP	HQ only	170 & Dinky	Any	Any	Port 21
SMTP	Any	Mail server	Any	Any	Port 25
DNS	Any	170	Any	Any	Multi protocol on ports using client ports
Telnet	HQ only	170 & Dinky	Any	Any	Port 23
Ping	Dinky	Any	Any	Any	Do
Lotus Notes	HQ only	170	Any	Any	TCP on port 1352
WatchGuard	None	None	Trusted	Any	Multi protocol on port 4103
Virus Scan	None	None	Any	64.75.31.197	TCP on port 80
Authority	Admin PC	Firewall	Any	Any	TCP on port 113

HQ Only - Public IPs of Head office in UK

170 - AS/400 170 Server which contains Mail, Web, DNS server

Dinky - AS/400 150 Server

Admin PC - PC where Management station program is installed

Table 4.1 – Rules assigned in the Firewall

Table 4.1 presents a summery of rules assigned by the system administrator. Although I manage to check and change configurations rules assigned in organizations Firewall is it not good to present it to public (as it is) because it could harm the integrity of internal security policy. Therefore table 4.1 indicates only selective set of rules, host names (no public IPs) with few modifications as well. In here my idea is to show what sort of rules could be configured depending on the requirement.

4.5.3 User Interface

Because of Fireboxes easy to use graphical user interface (GUI) configuring WatchGuard Firewalls are simple compared to other Firewalls with CLI. Drag and drop Windows style interface creates a configuration file and that file is send to the firewall using a secure channel. It also keeps an encrypted copy in the management station for disaster recovery purposes. Users could save different configurations with different file names and upload it to the Firewall when ever necessary.

For the initial configuration user has to use a serial cable to upload the configuration to the Firewall because WatchGuard consider consol as a security risk and they have removed the OS (customized Linux kernel) components relating to consol. When Firewalls is assigned an IP addresses, management station (PC with the management program) can connect to the Firewall using secure channel and do changes or monitor activities. Management station can manage Firewalls even located in branch offices through a central location in the head office.Firebox manager is a collection of set of components, it includes;

Control Center

Is the main interface which use to connect to Firewall(s) and it indicates basic stats and status of the connected Firewall. Figure 4.9 shows a screenshot of the control centre.

Policy Manager

Used to manage Firewall policies (rules), add/modify rules, configure NAT, change network settings, etc. Figure 4.10 shows a screenshot of the policy manager.

Firebox Monitor

Is used to monitor Firebox interface for the real-time bandwidth utilization, authenticated users, blocked sites, etc.

Log Viewer

Is used to view and manage log entries. See figure 4.11

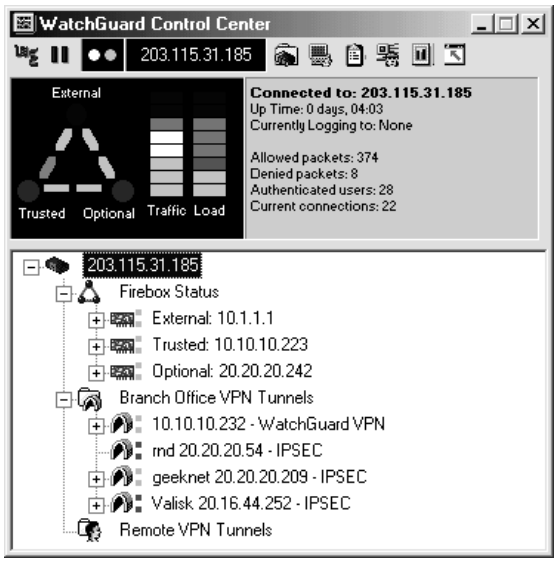


Figure 4.9 – Screenshot of the Control Center

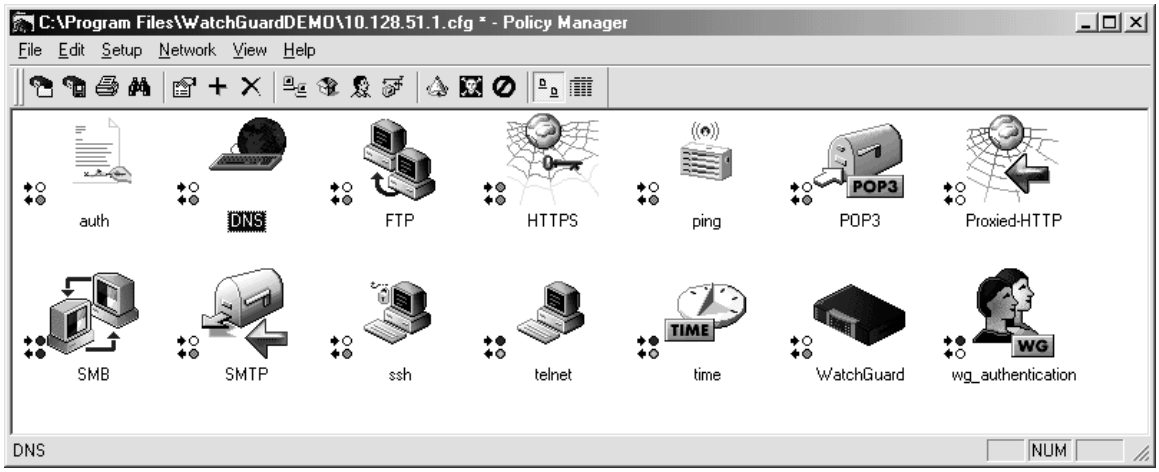


Figure 4.10 – Screenshot of the Policy manager

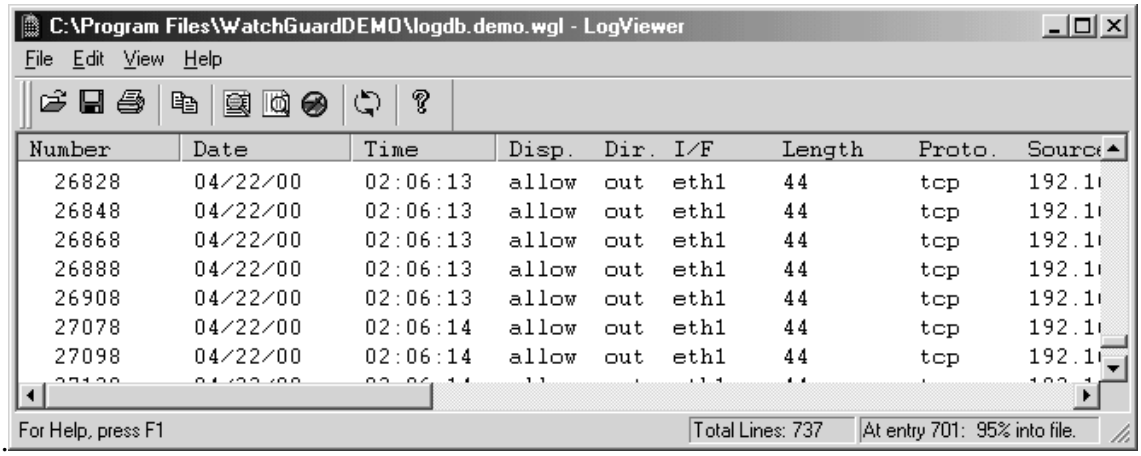


Figure 4.11 – Screenshot of Log viewer

Host Watch

Allows real-time monitoring of host activities (web sites users are connected, services are being used). Saved log files can be run to identify certain activities that took place when assessing security vulnerabilities. Figure 4.12.show a snapshot of activities in a specific time instant.

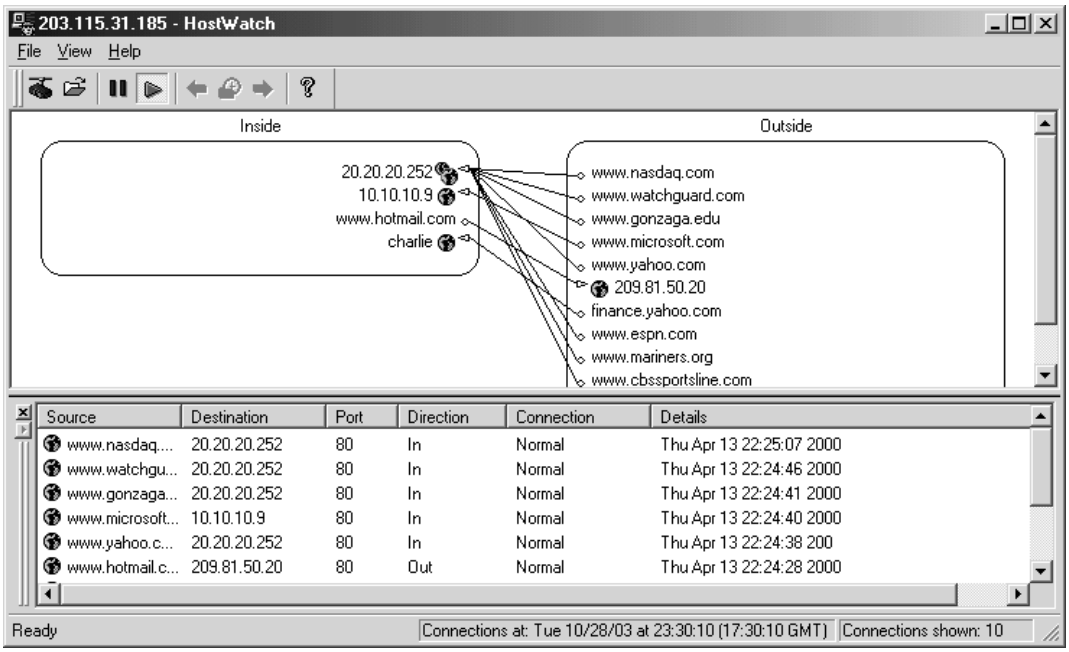


Figure 4.12 – Screenshot of Host Watch

4.6 Server Protection

Many administrator consider threats come only from outside (through Internet) and they tend to think internal users would not cause any harm. But researches have shown that possibility of an internal threat is also significant and it should not be neglected. These threats are caused by misuse, personals gain or by accidents.

None of the commercial Operating Systems are designed with security in mind. Security is not an integrated part of the system it is a different layer which stays at the user mode. It is acceptable because Secure OS would need immense planning, time, effort and more importantly more processing power due to extra overhead.

With all the current security mechanisms, still it is possible for an hacker to access a web or mail sever with legitimate power (as the super user) and change the content of a web page to divert credit card information to a different location, create a user account as a backdoor and even delete all the log entries that could indicate a system hack happened.

WatchGuard had introduced a new concept, a product called ServerLock, which will lock it self (from altering), critical OS files, registry entries and user defined file and folders.

4.6.1 ServerLock

Operating under the belief that protecting user data from unauthorized change is more effective than detecting attacks, WatchGuard created ServerLock: that "locks down" important OS files and valuable business information to create a secure foundation for the critical information systems in organizations.

ServerLock protects against Web site defacement and unauthorized changes, data and information tampering, accidental damage, hostile attacks, and unauthorized system reconfiguration. In this way, ServerLock ensures the integrity of data and the viability of the system.

ServerLock denies write and delete access not on the user permission but on the resource the user is trying to access. So if some resource is locked even the system administrator cannot tamper with that resource. If something protected by ServerLock need to be removed or modified first user must unlock the particular resource with ServerLock.

ServerLock work at the kernel (just above kernel as a filter device driver in Windows and as a loadable module in Sun Solaris) intercepting all the system calls. It check whether the request is a write or delete request if so it checks against the rules (protected or not). Figure 4.13 indicates the logical sequence of steps.

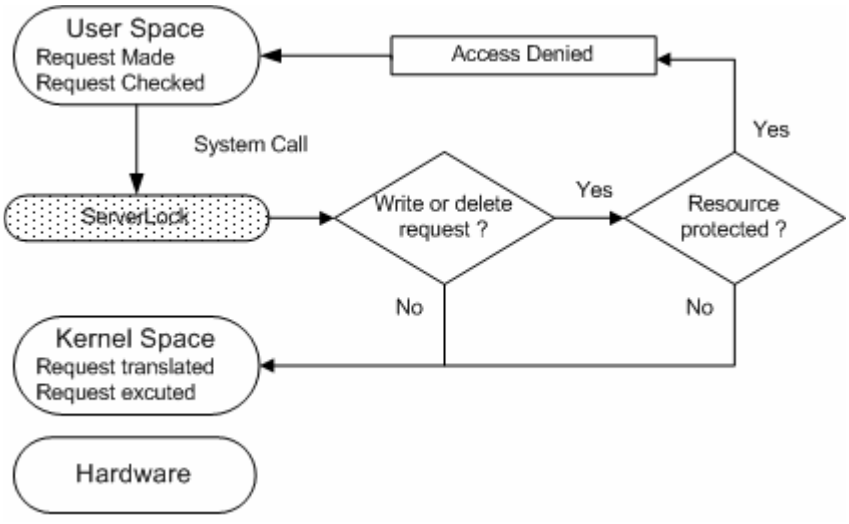


Figure 4.13 – ServerLock logical sequence

ServerLock protects itself from being altered, disabled or removed by unauthorized individuals by securing hardware profiles (to make sure ServerLock is loaded just after kernel), ServerLock files (executables, .dll, configuration files, etc.) and important registry entries. Everything depends on how secure ServerLock is. It

even uses encrypted channel between itself and kernel (first encrypted using PKI and then by 239-bit ECC (Elliptical Curve Cryptosystem)) for communication.

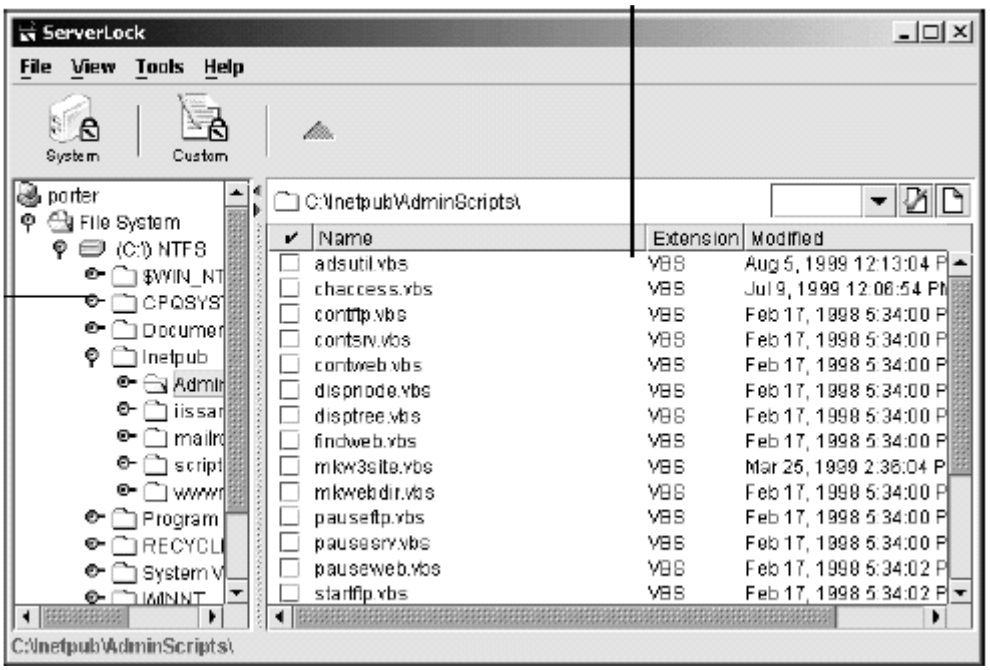


Figure 4.14 – Screenshot of ServerLock Advanced View

ServerLock is designed and proven to be low-overhead. It has a click of- the mouse user interface for ease of setup and maintenance. ServerLock adds less than 2% of CPU utilization on a fully loaded computer and added almost no time to the average response. ServerLock is a new concept and it is still in its evolving stage.

4.7 Enterprise level anti-virus solutions

Virus is hell of a trouble for system administrators and any one who is concerned in security. It has being found that new destructive threat originates in every 11 hours around the world. Guarding against viruses is a dynamic process which requires frequently updating of virus definitions and virus engines.

According to defense-in-dept approach virus protection should also be from Internet gateway (entry point) to the desktop. There is no point removing viruses just after the firewall while user can insert an infected floppy/CD-ROM to their PCs. As figure 4.15 indicates virus protection should be every where. And all those products should be capable of integrated with each other and work as a single unit.

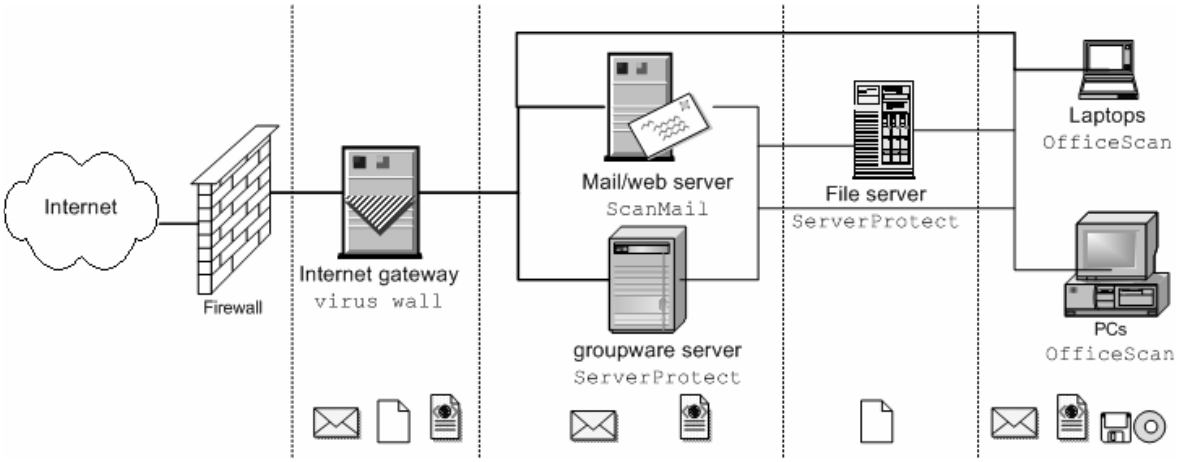


Figure 4.15 – In-depth anti-virus solutions for total security

4.7.1 Trend Micro Products

Trend Micro is a global leader and provider of comprehensive anti-virus and Internet content security. Trend Micro Products and services deliver a framework for coordinated enterprise protection throughout the virus outbreak lifecycle. Trend Micro specializes in high-performance virus protection and content security products and services, with advanced centralized management capabilities that are scalable for any enterprise or desktop.

I had to opportunity of installing, configuring, managing and troubleshooting some of the products by Trend Micro mainly for testing purposes. Products were tested for there ability to detect viruses (real-time scan) as they come in to the system and ability to remove worms like Nimda. Fallowing is a brief description of products that included in the Trend Micro NeatSuite package.

VirusWall

Located at the Internet gateway just after the Firewall (figure 4.17), in order to protect all traffic (SMTP. HTTP, FTP, etc.) must passes through the Viruswall. It stops viruses, worms and spam at the entry point.

ScanMail

Scans e-mails before they are send to the clients, if virus found it is striped off and rest of the mail is delivered to the client. Works with Lotus Notes, Microsoft Exchange, and Hewlett-Packard OpenMail servers.

ServerProtect

Is a standalone (or distributed) server based anti-virus solution designed to protect application and file servers. Works on verity of platforms like Windows, Linux and Novel Netware. Allows centralized management of servers and reporting.

OfficeScan

Protection for desktop and mobile users. Centralized management of all the hosts and applying of policies for the entire organization. Extensive graphical report facilities of infected clients, level of infection and type of viruses.

4.8 Conclusion

Protecting a network is a highly dynamic process which needs lot of vigilance and maintenance. Attacks are evolving all the time, unless you and your solution partner constantly work against those evolving threats and stay one step ahead you will be hacked. It is an interconnected layers of tools working to together to provide the deepest and most robust level of protection to your network and resources.

According my experience with customers (site visits and at the exhibitions) it really sorry to say that; most of them do not have any idea of security risks other than destruction caused by viruses. Every one is searching for a cheap anti-virus solution that could protect everything. Since they have heavily invested on IT infrastructure they hesitate spending more on security solutions (until they loose everything).

Most of organizations who understand such threats are moving towards various solutions that would minimize the risk making it harder to hack. But countries like us still keep our door open, when those hackers can not find a site to hack (at least when it gets hard) they would surely focus on organizations in third world countries. Therefore we must make people aware of evolving threats.

If you spend more on Coffee (Tea) than security you are deserved to hack!
By advice for defense for US president

5

Wireless Computing

"freedom of mobility"

Blue Chip is a reseller for range of wireless products from I-O wireless. During my training I had the opportunity of installing and configuring those products. I also did some planning for small scale wireless networks.

"By eliminating restrictive network cables, wireless networks offer you the freedom of mobility. Move to the conference room. Sit by the pool, kick back in the family room. Take your PC to your presentation down the hall. Hard-earned money is saved by eliminating the cost of reconstruction and pricey cable installation. And, with wireless network you never need to punch holes in your walls to string cables and there is no need for expensive hubs or switches". This paragraph is extracted from the newsletter that I wrote about I-O Wireless products.

5.1 Introduction

WLAN stands for Wireless Local Area Network. Is the next generation data communication system that can either; fully replace or extend traditional wired LANs. As most other wireless device (mobile phones, PDAs) WLAN make use of the radio waves (RF) to transmit and receive data. Binary data is superimposed onto conventional radio waves by the process called modulation and at the receiving end it is converted back to original binary data (demodulation).

5.2 Why Wireless?

Capabilities of WLAN go beyond just the absence of wires. Today's competitive market businesses needs to be ahead of its competitors, with the ability to move quickly in order to meet the varying needs of the customer and gain more market share. Wireless LAN could be the best fit for any organization because of;

Flexibility

- Staff can work any where any time within the work place (higher mobility)
- Cable free access to network. e-Mail, applications and Internet

- Onsite work teams can collaborate and share documents with higher mobility

Fast response

- Higher availability of critical data leads to faster and accurate decision making
- On fly information increase sales efficiency
- Higher employee satisfaction (proven by research)

Simple

- Easy to setup
- Significantly lesser Installation time
- Minimum planning compared to wired LAN

Speed

- It is fast! With up to 11 Mbps (faster than 10BaseT) and extensions with much higher speeds are immerging

Robust

- No wires which could get damaged
- Isolation from power surges or lightning that comes through network cables

Scalable

- Need not to stick with mounted network (wall or desk) outlets
- Several PCs can communicate with just wireless cards without an access point (depend on the manufacture)
- If needed access points can allow connection to the wired LAN
- When business grow WLAN can also grow with the business
- Could support roaming

Cost effective

- Easy of installation and flexibility reduces total cost of ownership
- Significantly lower maintenance and reconfiguration cost compared to wired LANs
- Very low incremental cost

5.3 Applications

Any organization can have its own Wireless LAN. There are applications which essentially require Wireless LANs. It has proven that what ever the type of business WLAN, will significantly improve any organizations performance and more importantly staff satisfaction.

WLANs are specifically suitable for fallowing environments;

- Mobile offices
- Offices with large number of mobile staff
- Health care centers
- Warehouses
- Construction sites
- Cyber cafes
- Trade shows or exhibitions

- SOHO users
- Historic or Old buildings
- Lecture or Conference rooms
- Banks
- Hotels
- Airports
- Universities

5.4 Technology

Manufactures of WLAN devices have several of technologies to choose from depending on the task of the device. Each technology comes with its own advantages and limitations.

5.4.1 Narrowband technology

A narrow band radio system transmits and receives information on a specific radio frequency, while trying to keep the frequency range as narrow as possible. Undesirable cross talk between communication channels is avoided by carefully coordinating different users (hosts) on different frequency channels.

End users must obtain FCC license (in Sri Lanka user must get it from SLTS) for each site and this is considered to be one of the significant drawback.

5.4.2 Spread spectrum technology

Is designed to trade off bandwidth efficiency for reliability, integrity and security. Spread spectrum consumers more bandwidth than narrowband, but it allows louder (amplitude) easily detectable signal. There are two types of spread spectrum radio;

5.4.2.1 Frequency Hopping Spread spectrum technology

Uses a narrow band carrier that changes frequency in a pattern known to both transmitter and receiver. When properly synchronized it maintenance a single logical channel all the time. Frequency of the signal can change from time to time but connection is not lost. Allows better utilization of available frequencies.

5.4.2.2 Direct Sequence Spread Spectrum technology (DSSS)

Generates a redundant bit pattern (called as chip) for each bit to be transmitted. The longer the chip, grater the possibility that the original signal data can be recovered.

Statistical techniques can be used to correct errors that occur during the transmission.

5.5 Standards

Institute of Electrical and Electronics Engineers (IEEE)

The WLAN standards were started with the 802.11 standard, developed in 1997 by the IEEE. This base standard allowed data transmission of up to 2 Mbps. Over time, this standard has been enhanced. These extensions are recognized by the addition of a letter to the original 802.11 standard, including 802.11a and 802.11b. The table 5.1 below details the various standards related to 802.11.

Standard	Description
802.11	The original WLAN Standard. Supports 1 Mbps to 2 Mbps.
802.11a	High speed WLAN standard for 5 Ghz band. Supports 54 Mbps.
802.11b	WLAN standard for 2.4 GHz band. Supports 11 Mbps.
802.11e	Address quality of service requirements for all IEEE WLAN radio interfaces.
802.11f	Defines inter-access point communications to facilitate multiple vendor-distributed WLAN networks.
802.11g	Establishes an additional modulation technique for 2.4 GHz band. Intended to provide speeds up to 54 Mbps.
802.11h	Defines the spectrum management of the 5 GHz band for use in Europe and in Asia Pacific
802.11i	Address the current security weaknesses for both authentication and encryption protocols. The standard encompasses 802.1X, TKIP, and AES protocols.

Table 5.1 – IEEE standards for WLAN

The 802.11b specification was ratified by the IEEE in July 1999 and operates at radio frequencies in the 2.4 to 2.497 GHz bandwidth of the radio spectrum. The modulation method selected for 802.11b is direct sequence spread spectrum (DSSS) using complementary code keying (CCK) making data speeds as high as 11 Mbps.

IEEE sets the standard, but does not ensure compliance to the standard nor does it ensure interoperability between different manufacturers' products.

Wi-Fi Alliance

The Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of WLAN products based on IEEE 802.11 specification.

The goal of the Wi-Fi Alliance's members is to enhance the user experience through product interoperability.

The **Wi-Fi CERTIFIED*** logo comes from the Wi-Fi Alliance. The Wi-Fi CERTIFIED logo indicates that the product has met rigorous interoperability testing requirements to ensure products from different vendors will work together. The Wi-Fi Alliance is also active in creating new and stronger security standards, like Wi-Fi Protected Access* (WPA), as well as promoting the proliferation of hotspots (public areas like coffee shops and airports where WLAN access is available, usually for a fee).

5.6 Security

Because wireless technology it heavily used in military applications security issues has long being design criteria for wireless devices. Security provisions are typically built in to the wireless devices therefore it is extremely difficult for an unintended receiver to listen to the traffic. IEEE 802.11i addresses these security weaknesses. Complex encryption techniques such as 64 or 128-bit WEP (Wired Equivalent Privacy) facilitate such requirements. Individual nodes must be security enabled before they are allowed to participate in the network traffic. Administrator need to make user the passphrase used to generate the WEP key is kept as secrete.

5.7 Terminology

Before proceeding to next section it would be better to get familiar with some of the keywords related to WLANs and WLAN concepts.

Wireless card

Or wireless adapter card (figure 5.1) is the device which is used to connect a PC or a Laptop to the wireless network. It is same as a network interface card (NIC) other than being wireless. Typical wireless card can send signals up to about 100 m (300ft) in normal room conditions; on open air it could go bit longer (depend on the manufacture and card type). Card could be either PCI, PCMCIA or USB ones.

Access point

Access point (figure 5.1) is similar to a hub or switch where several wireless cards connect each other through this. Access point can accommodate many clients (e.g. I-O wireless access point theoretically supports up to 256 clients but in practice they prefer not to connect more than 50 users due to bandwidth limitations). Access point also has a finite range (about 500ft to 1000ft open air) and certain access

points also support roaming. Access point could also be used as a point which interconnects wired and wireless LANs.

Wireless bridge

Used to interconnect two or multiple building (with wired LANs) through a wireless connection. Suitable for places like campus and head offices with near by branch offices. These bridges combined with antennas could cover up to several miles. See figure 5.1

Antenna

As normal radio antenna (figure 5.1) this is used to either send on receive RF signals. It could also extend the distance between two access points. A Wireless (I-O Wireless products) bridge with an antenna would cover 11 miles (line of sight).

Wireless Cards Access Point Wireless bridge Antenna

Figure 5.1 – Wireless devices

5.8 Wireless LAN configurations

WLANs can be configured in a variety of ways; it can expand from a very basic point-to-point network (with just 2 PCs or Laptops) to a large network through a Wireless access points.

Ad Hoc Network

An ad hoc (peer-to-peer) network is an independent LAN which is isolated from a wired network and where all stations are connected directly to one another (figure 5.2).

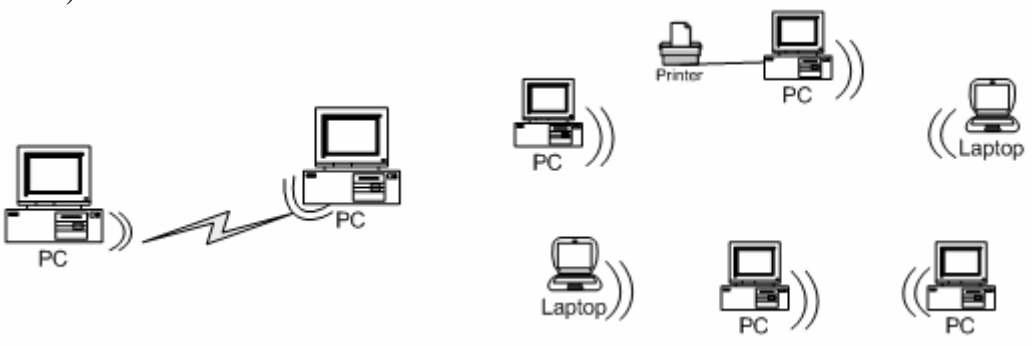


Figure 5.2 – Ad Hoc Networks

Infrastructure Network

WLAN clients connect to the corporate network through a wireless access point and operate like a client in the wired network (figure 5.3).

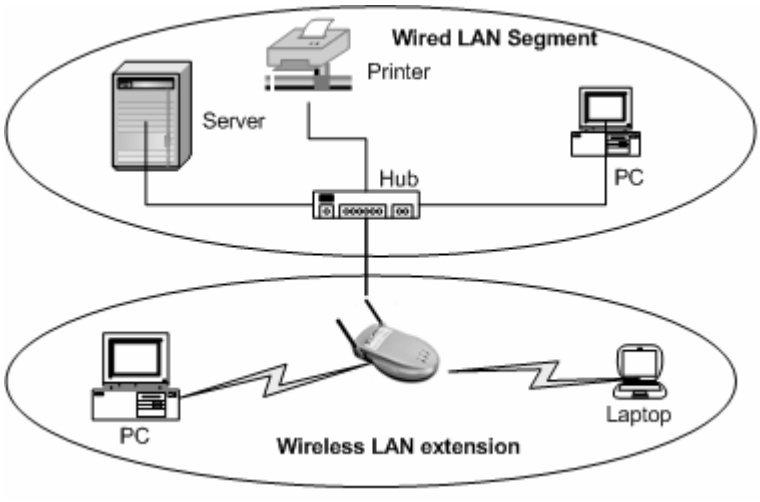


Figure 5.3 – Infrastructure Network

Roaming

Is an extension of infrastructure configuration where clients can have roaming facilities. Also call as Hotspots. Access points are located in such a way that their ranges are overlapping each other. So clients could move from one location to the other (i.e. one access point to another) ensuring unbroken connection (figure 5.4)

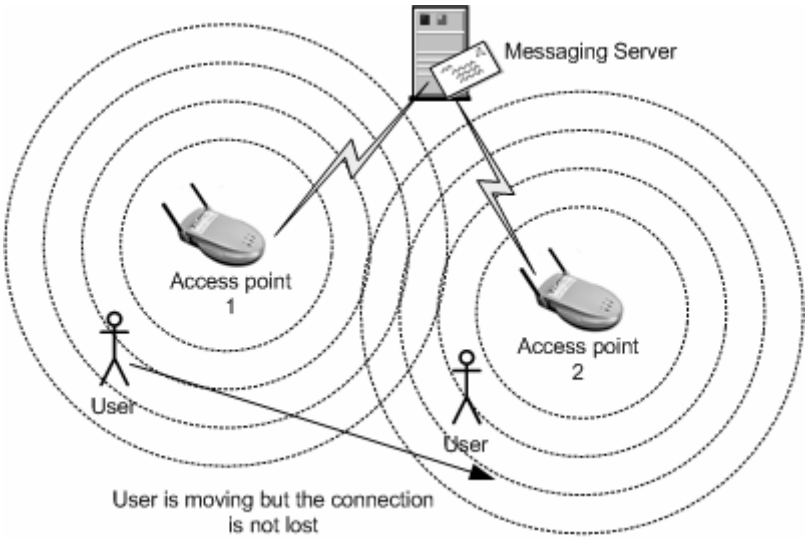


Figure 5.4 – Roaming, although user is moving and within the range of different access point he/she is still connected to the messaging server

Point-to-Point Bridge

A bridge is used to connect two isolated networks within separate buildings through wireless connectivity (figure 5.5)

Point-to-Multipoint Bridge

When it is necessary to connect 3 or more isolated networks point-to-multipoint bridge configuration is used. This is an extension of Point-to-point Bridge

Wireless Bridge with Wireless End Nodes

A specific bridge called the Bridge Master which is capable of servicing the clients. The wireless client device can contact with the Bridge Master and have access to all local and remote LANs, workstation, and network resources.

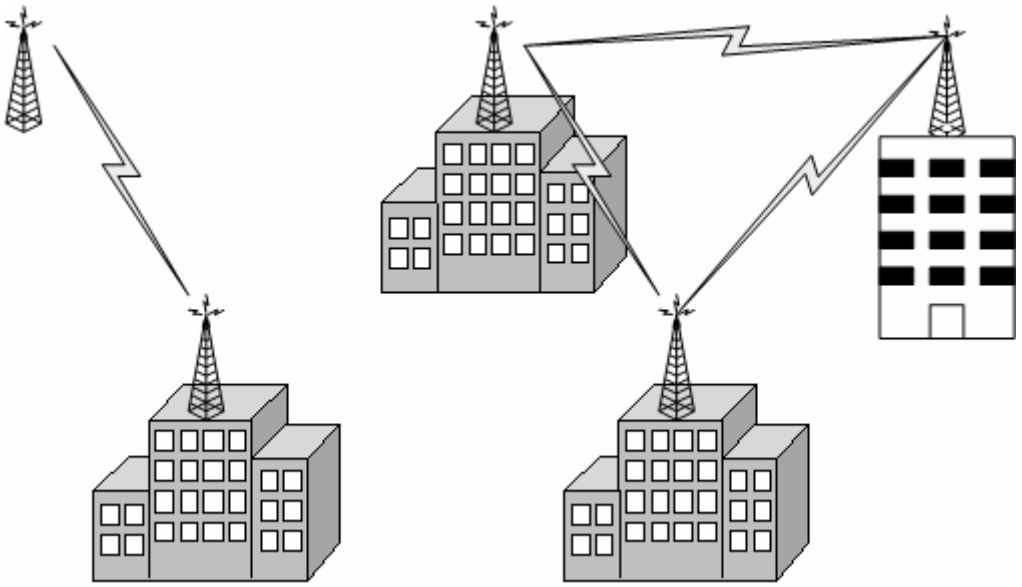


Figure 5.5 – Point-to-Point and Point-to-Multipoint Bridges

5.9 I-O Wireless

I-O Wireless is a brand name for range Wireless Products from I-O Corporation (USA). By eliminating restrictive network cables, I-O wireless solutions offer the freedom of mobility within offices, factories, schools, universities, etc. Simple, easy to install, configure and upgrade solutions give customers fast 11Mbps transmission, which utilize 802.11b technology. These devices use Direct Sequence Spread Spectrum technology (DSSS) technology. I-O Wireless products could support all the network configurations discussed in section 5.8. Blue Chip is the local partner for I-O Wireless and other I-O products in Sri Lanka.

5.10 Conclusion

In closing, the price of installing wireless LANs are more expensive than using cabling. Mobility is the number one reason for choosing wireless LANs. The initial cost of purchasing and setting up a wireless LANs are higher, but in the long run Total Cost of Ownership (with constant relocation) is much les than a wired solution.

In general, as large corporations and businesses move toward a mobile work force, we will see a higher demand for wireless applications. In the years to come, such a demand will, hopefully, bring down the existing cost of going wireless, thereby making it more affordable to a larger audience.

6

Conclusion

The primary objective of industrial training program is to allow student to get sound appreciation and understanding of the theoretical knowledge they gained at the university. In university we learnt about lot of equipments and devices that is being used in the industry. But most were only seen either through a window or picture, industrial training expose us to the real device were we get the hand on experience (installing, configuring, maintaining and troubleshooting of such devices) while being an undergraduate.

At Blue Chip I was given all the freedom to work with all sorts of equipments (or devices) regardless off there higher cost (single mid-range sever cost several million rupees). They were never hesitating to give such resources to me. They gave me enough freedom to work with devices and machine (I make sure nothing bad happens to those devices or machines)

But finding the right person at the right time for some advice was a big case. Since it's a small company single person had to cover several areas of work as a result most of them were busy and not in the office. So it was hard to find person when ever I want, as a result I decide to give up my initial work plan. Instead of a specific plan, I identified what are the key technologies that I must cover, and got people to help me when ever they are available.

It is quite natural to have such problems especially in a small company where few people have to do who lot of things. In a way it gives me lot of freedom because it allows me more time to work independently (because they are not in a position to tell every thing, I have to search for it and do it in my own way).

As a result I was covering several subjects a week; I think that approach is much better than doing the same thing (referring the same manual or user guide) during the entire week and making life boring. It allows me to grasp the opportunities such as attending to customer site visits product presentations.

They never hesitate to put me in front of the customer and it was a grate experience. At the latter stage of my training I was in a position to meet customers alone and interact with them on various issues (requirements analysis, proposals).

Blue Chip have qualified people, but if you really want to lean bit more you must go to them and ask what ever you want to know and do. Although Blue Chips idea is to be professional in specific set of products, still they use all most all the products in the market (Server and Network related stuff) other products internally or for testing purposes. So you are not stuck in to a frame you could go beyond the frame as well. So as a training establishment Blue Chip could provide really good training.

I got to know about Blue Chip from NAITA and no one around me had any idea on what sort of business Blue Chip is engaged in. It was a risk that paid wonderfully well in the end. But there were few other places where my friends had bad training experiences (as me they were not having any initial idea about the organization). So it would be nice if NAITA, Training Department and other Departments could get-together and arrange student awareness program regarding each organization. Or organize group of presentations where companies come to the university and tell (presentation) what sort of thing they do.

As a Computer Science and Engineering undergraduate I was keen on Computer Hardware and Networking only. Had some idea to become a System administrator or so, but today my idea has changed and I have understood that as an engineer it would be much better to work with a solution provider rather than maintaining a system designed and developed by some one else. It is a quite a challenge, where you have to design solutions, keep updating with technology changes and being aware of competitive products, etc.

Training is not only oriented towards technical stuff, it is every thing; interpersonal relationships, managing and resolving conflict, communication, competition and organizational and human resource management are part of it. We should observer such problem carefully and should be able to overcome them.

I am really happy about the exposure I had to industry as an undergraduate and I would recommend Blue Chip to any one who is keen on areas like Computer Hardware and Networking.

Abbreviations

24x7	24 hours and all 7 days of the week
ADSL	Asymmetric Digital Subscriber Line
API	Application Programming Interface
AS/400	Application System 400
ASCII	American standard Code for Information Interchange
ASIC	Application Specific Integrated Circuit
ATM	Asynchronous Transfer Mode
AWT	Abstract Windowing Toolkit
CCK	Complementary Code Keying
CGI	Common Gateway Interface
CISC	Complex Instruction Set Computing
CLI	Command Line Interface
CPU	Central Processing Unit
CPW	Commercial Processing Workload
CRG	Cluster Resource Group
CSU/DSU	Channel Service Unit/Digital Service Unit
DES	Data Encryption standard
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name Service
DSSS	Direct Sequence Spread Spectrum
ECC	Error Correction Code
ECC	Elliptical Curve Cryptosystem
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
GUI	Graphics User Interface
HSM	Hierarchical Storage Management
HTTP	Hyper Text Transfer Protocol
I/O	Input/Output
IC	Integrated Circuit
iCOMP index	inter Comparative Microprocessor Comparative Index
ID	Intrusion Detection
IDE	Integrated Development Environment
IEEE	Institute of Electrical and Electronics Engineers
IFS	Integrated File System
IP	Internet Protocol
IPL	Initial Program Load
IPSec	Iinternet Protocol Security
ISDN	Integrated Services Digital Network
JVM	Java Virtual Machine
LAN	Local Area Network
LIC	Licensed Internal Code
MIME	Multipurpose Internet Mail Extension
MS-DOS	Microsoft Disk Operating System
NAT	Network Address Translation
NFS	Network File System
NIC	Network Interface Card
ORB	Object Request Broker

OS	Operating System
OS/400	Operating System 400
OSI	Open Systems Interconnection
PBX	Private Branch eXchange
PC	Personal Computer
PCI	Peripheral Component Interconnect
PCMCIA	PC Card - Personal Computer Memory Card International Association
PKI	Public Key Infrastructure
PM	Preventive Maintenance
PPTP	Point to Point Tunneling Protocol
PTF	Program Temporal Fixes
QOS	Quality Of Service
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Independent Disks or Redundant Array of Inexpensive Disks
RF	Radio Frequency
RIO	Remote I/O
RISC	Reduced Instruction Set Computing
RPR	Relative Performance Rating
RSP	Relative System Performance
SCS	Structured Cabling Systems
SLIC	System Licensed Internal Code
SLS	Single Level Storage
SLTS	Sri Lanka Telecommunication Services
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture
SOHO	Small Office Home Office
SOI	Silicon on Insulator
SSL	Secure Socket Layer
STP	Shielded Twisted Pair
TCP	Transport Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDE	Task Dispatching Element
TIMI	Technology Independent Machine Interface
TOC	Total Cost of Ownership
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTP	Shielded Twisted Pair
VM	Virtual Machine
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
xDSL	any DSL (Digital Subscriber Line) techonology
XOR	Exclusive OR

References

1. Blue Chip Customer Engineering Lanka (Pvt) Ltd
   - 1.1 Official company web site
     `http://www.bluechip.lk`
     Provides information about history, products, partners, new events, etc.
   - 1.2 Internal documents
     Not released to the public. Various documents such as; summery of events, profitability, performance analysis.

2. Mid-Ranger Servers
   - 2.1 Official web site for IBM e-Server i-Series machines
     `http://www.as400.ibm.com`
     Have all sorts of links to product information, technical support, white papers, special offers, latest new, etc.
   - 2.2 Hardware and Operating System Basics
     AS/400 System Hand Book, February 1999 V4-R3 & V4-R4
     Contains basic information about Advanced Application Architecture, hierarchy of microprocessors, CPW, OS/400 new enhancements, etc.
   - 2.3 AS/400e Technical Overview 2000
     A multimedia CD-Rom which presents large collection of documents and presentations relating to hardware, OS, networking, database supports, client server, etc for V4-R1 to V4-R5.
   - 2.4 White Papers for i-Series and AS/400
     `http://www-1.ibm.com/servers/eserver/iseries/whpapr/`
   - 2.5 64-Bit Computing Made Simple – White paper
     by Michael P. Flannery Advisory Engineer AS/400 Division Rochester
   - 2.6 RAID
     - 2.6.1 Understanding IBM i-Series 400 and AS/400 Disk (DASD)
       By Brian Podrow, i-Series Hardware Product Manager
     - 2.6.2 Strategic and Innovative RAID Solutions
       `http://www.acnc.com`
       This site contains simple explanations with clear diagrams
   - 2.7 I/O Technology
     White paper by Bruce Walk
   - 2.8 OS 400 - The Operating System Handbook
     By Bob DuCharme
   - 2.9 AS/400 Thread technology
     White Paper by John Attinella and John Orbeck

2.10 Memory Management

2.10.1 AS/400 Shared Memory concepts
White paper by Ed Prosser

2.10.2 iSeries Extended Adaptive Cache
White paper by Carl Forhan, Bob Galbraith, and Jessica Gisi, IBM Development Engineers

2.11 Storage

2.11.1 Hierarchical Storage Management
White paper by Luz Rink

2.11.2 Teraspace Storage
White paper by Scott Plaetzer

2.11.3 File System

2.11.3.1 AS/400e Series Integrated File System an Introduction – Version 4
By IBM

2.11.13.2 Introduction to the integrated File System
A presentation by Dave Boutcher

2.12 Logical Partitioning
White paper by Bill Armstrong, Troy Armstrong, Naresh Nayar, Ron Peterson, Tom Sand, Jeff Scheel

2.13 Clustering

2.13.1 AS/400 Clustering Technology
White paper by Sharon L. Hoffman

2.13.2 Clustering
By Mike Snyder

2.14 Java on AS/400

2.14.1 AS/400 Java Application Models
White paper by Pual Rerntema

2.14.2 AS/400ToolBox for Java
`http://www-1.ibm.com/servers/eserver/iseries/whpapr/toobox_java.html`

2.14.3 Enterprise JavaBeans and the AS/400
`http://www-1.ibm.com/servers/eserver/iseries/whpapr/enterprice_java_beans.html`

2.15 IBM WebSphere for AS/400
`http://www-1.ibm.com/servers/eserver/iseries/whpapr/websphere.htm`

2.16 Lotus Domino

2.16.1 Domino for AS/400

2.16.2 Domino for AS/400: Frequently Asked Questions
2.16.3 Domino for AS/400: The IBM Rochester Experience
2.16.4 AS/400 Domino: Leveraging an integrated architecture
2.16.5 Domino for AS/400 and Total Cost of Ownership
2.16.6 Lotus domino –Server Consolidation
`http://www-1.ibm.com/servers/eserver/iseries/whpapr/`

3 Network Security

3.1 Official Web site for WatchGuard Products
`http://www.watchguard.com`
Contains product information, product pricing, product comparisons, white papers, user guides, user training information, etc.

3.2 What is a Firewall
`http://www.pc-help.org/www.nwinternet.com/pchelp/security/firewalls.htm`

3.3 An Examination of Firewall Architecture
A white paper by Paul Henry

3.4 Defense-in-Depth, Firewalling Basics Student Guide and Network Security Hand book
by WatchGuard Technologies

3.5 WatchGuard Partner CD
A CD-ROM with all the product information, pricing, comparisons, user guides, training materials, demo versions that is given only to WatchGuard registered partners

3.6 NAT or No Nat
A web page introducing how NAT work
`http://www.nkdsl.co.uk/ethernat.htm`

3.7 Intelligent ASICs – The future of Security
White paper by WatchGuard Technologies

3.8 Trend Micro official Web site for products
`http://www.trendmicro.com/en/products/global/enterprise.htm`

4 Wireless Computing

4.1 I-O wireless Official Web site
`http://www.iowireless.com`
Contain information about products, pricing, whitepapers, connectivity, etc.

4.2 Exploring WLAN Solutions
`http://www.intel.com/ebusiness/strategies/wireless/wlan/index.htm`

4.3 What is a Wireless LAN?
A white paper by Proxim

4.4 Modern Wireless Applications
by ICI Networks

5 Patton Products

5.1 Patton electronics Official web site
http://www.patton.com

6 Thin client

6.1 I-O Corporation official web site
http://iocorp.com

7 ADSL/xDSL/ATM

7.1 Asymmetric Digital Subscriber Line
A presentation by Priyanka Undugodage – Head of IT & Broadband Service Section, SLT

7.2 SLT Web site for ADSL
http://www.slt.lk/inpages/atbusiness_pages/adsl.htm

7.3 Asynchronous Transfer Mode (ATM) Switching
From Internetworking Technology Overview

8 FingerTec

7.4 FingerTec Official web site
http://www.fingertec.net

9 CISCO Products

9.1 Official Cisco Web site
http://www.cisco.com