Documenting a Network: The why and how

Wong Hee Kwong
Jabatan Ilmu Pendidikan

ABSTRACT

Network documentation provides a bird's eye view of a network's layout and set up. This information is important especially when new personnel are assigned to maintain or upgrade existing network. There are also various methods of documenting network ranging from complicated and detailed diagrams to simple but practical information for survival. Nonetheless, network documentation has proved many a time to be useful and constant revision needs to be made to such documentation as changes are made either to maintain or upgrade existing facilities. This article details a network documentation that follows the recommended ISO Layer Model.

INTRODUCTION

In any major IT project, documentation should be given the top priority in the list of items to be carried out. In planning and managing a network, preventing problems should be approached structurally. With the availability of network documentation this approach to solving problems on the network can be done systematically and quickly. Trouble shooting is made faster and easier with the availability of visual diagram. As employees leave the organization, loss of information is reduced making the transition less painful. Network administrators can delegate network responsibilities, as important information is made available in written form. A network diagram is a key element in any design process. It can be used for the purpose of base lining, design improvement or auditing. However, the greatest benefit of network documentation is SAVING TIME.

The purpose of this proposal is to introduce a method of documenting an existing network system in a teacher-training institute. Network documentation increases the transparency and accountability of an organization, helps to distinguish between the haves and the haves-not and helps to identify future upgrading of hardware and software.

As teacher-training institutes move towards International Standard Organisation (ISO) compliance, it is also time to look at our backrooms and do some housekeeping. With network documentation it further enhances our position in qualifying for standards such as ISO or Institution of Electronic and Electrical Institution (IEEE) in the field of information technology.

Computer network in teacher-training institutes today have grown to become more complex, spanning multiple locations and platforms. They are sophisticated and have become an important resource to the administration and imparting of knowledge, which requires proper documentation in order to control costs, plan, design, and support and manage network infrastructures. In fact network documentation should not be an option; it should be an essential part of an information management strategy.

LITERATURE REVIEW

Undocumented networks are common. This is related more to the difficulty of keeping the documentation up to date rather than to the difficulty of the documentation process itself. Perhaps the most important thing to do is to label the network cables. Usually all cables look alike, and it’s impossible to tell which cable connects to what without some extensive diagnostic work. Most network administrators are too busy to have time to fish through a big bundle of cables hoping to stumble upon the correct one every time that there’s a problem. There are other valid reasons as to why documenting a network is important.

Why documentation? The following are the reasons why:

1. The network has grown too vast, varied and complex to be understood completely without comprehensive documentation. Documentation is essential for operating, changing or analysing networks with their various components, interdependencies and capabilities. Complexity requires documentation that is sharable and available to those who are responsible maintaining the distributed system. No single individual or “brain trust”, no matter how capable one is can remember all the details of a network. Such information must be recorded, consolidated and standardized in documentation, then made available throughout the organization to all those who need it and whenever they need it. One of the most obvious reasons to document the network is the aid it provides in troubleshooting. Having information readily accessible in the event of problems about access point types and locations, Internet Protocol (IP) addresses, Wired Equivalent Privacy (WEP) settings, client configuration and channels can't be over emphasized. In the event that others need to be involved to help with the real sticky problems, the benefit of an easier transfer of knowledge applies. If permanent changes are made to the network because of the ensuing corrective action, change management and documenting the modifications must be recorded.

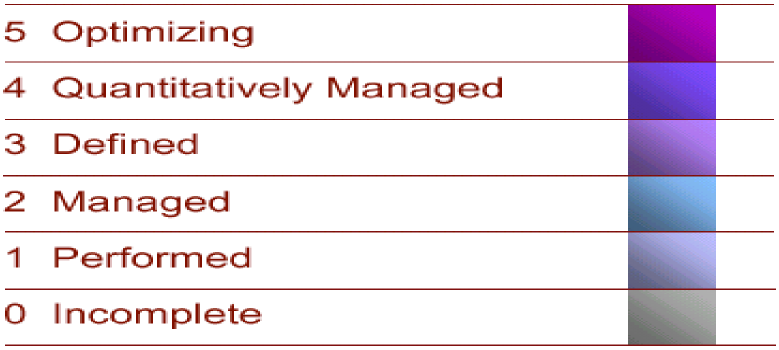
2. Institutions or organizations are becoming increasingly dependent on the network infrastructure for core business processes. Networks have become the vehicle for many mission critical applications. As reliance on the network increases so does the cost of system failures and network down time. The longer the interruption, the greater will be the loss and the more detrimental to clients and employees relationship. To fix problems quickly, information needs to be available for analysis, diagnosis and then repair. Typically, 80% of the time is spent on determining the cause of the problem and 20% is spent solving the problem. As organizations seek to improve efficiency and competitiveness, a new network paradigm is emerging. Networks are being used to achieve radical new levels of organizational integration. This integration obliterates traditional organizational boundaries and transforms local operations into components of comprehensive, network-resident processes. For example, in teacher training institutes, the various departments are integrating operations with other units and clients through the intranet and internet and networks that enhance communication and services. These networks combine fragmented operations into coherent processes open to many organizational participants. This new move represents a change from “closed” networks with central control to “open” networks. “Open” networks are characterized by distributed administrative control without central authority, limited visibility beyond the boundaries of local administration, and lack of complete information about the network. At the same time, organizational dependencies on networks are increasing and risks and consequences of intrusions and compromises are amplified. Detailed documentation therefore is absolutely required to ensure prompt repairs, sustain high system availability and reduce support costs.

3. Network costs are difficult to quantify and audit. The infrastructure of a network typically consists of a wide variety of geographically distributed assets, namely circuits, equipment, connections and other components that have been purchased from different suppliers. Lacking a centralised knowledge base of network assets, the management does not know what is “out there” and therefore cannot effectively understand and streamline costs such as replacing older assets with better and cheaper alternatives, reallocating existing assets to increase utilization and performance and eliminating cost redundancy. When an audit is made on an existing local area network – connected workstations, hardware and software, it allows the management to identify opportunities for improvement and also allows transparency to be practised in the allocation of assets to departments or sections.

4. Top technical talents are increasingly hard to find and to keep. Fast and accelerated changes in system technology and a growing diversity of network products add to the woes of network specialists. Network

specialists need to recoup and enhance their knowledge through training and attending workshop sessions. Intimate knowledge about network infrastructure must be documented before it disappears.

5. Organisational changes and regulatory compliance demand improved asset reporting system. Documenting network assets is not an option as financing needs to be made and those responsible should be made accountable. Close accounting of mission critical network resources require institutions or organizations to maintain current accurate and complete documentation of their network infrastructure. With the amount allocated and spent each year on these assets it is high time to stop and ponder, “Where are we?” Most institutions in their quest for excellence acquire a standard in their process. If institutions or organizations are to claim that they are of certain standard compliance, then their network certainly needs another look – whether they actually adhere to the standard or not? Capability Maturity Model Integrated (CMMI) levels – a recognition widely seek by organizations and institutions alike for information technology clearly indicates that when an organization or institution do not have any documentation they are at Level 0. Motorola Malaysia, for example, is an organization that has been appraised to be a CMMI Level 5 organization.



5	Optimizing
4	Quantitatively Managed
3	Defined
2	Managed
1	Performed
0	Incomplete

CMMI Maturity Level

CMMI Maturity Level

Webster defines professionalism as "the standing, practice, or methods of a professional, as distinguished from those of an amateur." By following the practice of documenting network, we are showing that we are indeed an IT Professional.

Methods of Documenting a Network

Microsoft TechNet introduces a network mapping and diagramming solution through one of its software called Microsoft Visio 2000. Visio tools provide a common graphics technology for network diagramming providing a standard platform across departments and disciplines. The software helps IT professionals to transform data into visual understanding. However, Microsoft TechNet does not provide a guideline on what to be included in the documentation of network.

IEEE is a standards organization that oversees the quality and inter-operability of today's computing applications and hardware. The various subcommittees of IEEE 802 set the various standards and guidelines starting with Local Area Network or Metropolitan Area Network overview and architecture. These guidelines provide the backbone to the documenting of a network.

The International Standard Organization (ISO) developed the OSI Seven Layer Model to provide a standard for the complex relationships in computer networks. It divides the different functions and services provided by network hardware and software into seven compartmentalized layers. This approach facilitates modular engineering, simplifies network technologies and helps to isolate problems when troubleshooting. The seven layers provide a reference and guide when documenting a network.

Layer 1: Physical Layer

The bulk of documentation needs to be done at Layer 1. A full description of each device on the network is essential for inventory control, future upgrade planning, and physical security. Device refers to computer hardware, peripherals, routers, and switches. The network cabling and patch panels must also be documented. Using a tool such as Microsoft Visio can draw the topology and architecture of the network and this diagram should be kept up-to-date as the network changes. This diagram can help in doing pre-emptive planning and answer important questions about the network. Are hubs close to being maxed out? This is valuable information for the managers of organization, and the documentation could be the hard proof needed to get new purchases approved during planning meetings with management.

Layer 2: Data Link Layer

The Data Link Layer is responsible for the communication between the network and the physical layers. One of the primary network specifications handled at the Data Link Layer is the hardware address (also called the MAC address) of network adapter cards. Every network adapter in the world has a unique hardware address, based on the vendor of the adapter. You should have a list of MAC addresses for each network adapter on your network. You should know what speed they are and what protocols they support. Plus, you should have statistics from a network monitoring application that shows baseline information about activity on your network.

Layer 3: Network Layer

The Network Layer defines the standards of how data is communicated across your network and between your network and other networks, including the Internet. Network Layer documentation should include information about WAN links, Internet connections, and Virtual Private Network (VPN) and Remote Access Servers (RAS). This is the layer that is responsible for converting a logical name into an IP address. So the documentation of your subnet should include a map of NetBIOS/Host names and IP addresses, Dynamic Host Configuration Protocol (DHCP) scopes, gateway/router addresses, proxy server addresses, Windows Internet Name Service (WINS) and Domain Name System (DNS) server addresses, and IP addresses and information on any other network servers. Network Layer documentation should also include policies on the naming conventions of computers and users, domain controllers, and routers/switches.

Layer 4: Transport Layer

The Transport Layer is responsible for the packets getting to their destination in the proper sequence and without errors. This is a critical layer for security, especially firewalls and screening routers. The two primary protocols that operate at this layer are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), and one of the main methods that firewalls use to block or allow traffic is based upon TCP and UDP port numbers. Your documentation should include a list of which port numbers your firewall(s) allows.

Layer 5: Session Layer

The Session Layer makes sure that a system can open a communications connection with a remote system and that data can flow back and forth between the systems. Examples of protocols that work at the Session Layer include Telnet, Secure Shell (SSH), Simple Network Management Protocol (SNMP), and Secure Socket Layer (SSL). In terms of documentation, you should include SSL-enabled sites in security documentation, and you should have a policy about having SNMP enabled for network monitoring and management. Telnet and SSH will probably be documented as part of your remote access plan for administrators.

Layer 6: Presentation Layer

The Presentation Layer transforms data into a form that is understandable to the recipient. If encryption is required, it takes place here, as does decryption. The Presentation Layer also participates in encapsulation and decapsulation and encoding and decoding, such as in multimedia applications like Moving Pictures Expert Group (MPEG). There really aren't any documentation activities that relate specifically to the Presentation Layer.

Layer 7: Application Layer

The Application Layer is the interface that controls applications such as e-mail and other applications used to send or receive information. It is about application in the more traditional sense—the ones that are installed on operating systems. The network administrator must have policies in writing from the powers-that-be that spell out what applications should be available on the network and to whom. Without this document, administrators are in a precarious position. If a user wants an application, and it is withhold with no written policy, you face appeal. If you give a user an application, and someone higher up doesn't think you should have done so, you face reprimand. If you have policies in hand that make the decisions for you, you will have the needed consistency.

Proposed Documentation

The proposed network documentation follows the recommended ISO Layer Model. This is to provide an insight and an example of how network documentation can be done. However, other methods can also be employed depending on how complex and detailed documentation is needed. Very often the requirements of an organization need to be considered and balanced with simplicity and ease of keeping an up-to-date documentation enough for the understanding and maintaining a network. An example of such documentation is shown in Appendix A. The first step in managing a network is to know what is in a network, what are the components connected to, and where about are the components. Ideally network documentation should contain Layer 1 – the topology of the network, Layer 2 – switching, Layer 3 – router implementation and scalable LAN (Local Area Network), Layer 4 – protocols, Layers 5, 6 and 7 – the software installed so as to provide how computers connected through a network interact, communicate or perform tasks. The software installed will provide a clearer picture of how computers will work in a network environment.

CONCLUSION

The capability of a system to fulfill its mission in a timely manner, in the presence of attacks, failures, or accidents is known as its survivability. The term system is defined in the broadest possible sense, including networks and large-scale systems of systems. The term mission refers to a set of very high-level (abstract) requirements or goals. Missions are not limited to military settings since any successful organization or project must have a vision of its objectives whether expressed implicitly or as a formal mission statement. Judgments as to whether or not a mission has been successfully fulfilled are typically made in the context of external conditions that may affect the achievement of that mission. For example, assume that a network shuts down for 12 hours during a period of widespread power outages caused by a thunderstorm. If the system preserves the integrity and confidentiality of its data and resumes its essential services after the period of environmental stress is over, the system can reasonably be judged to have fulfilled its mission. However, if the same system shuts down unexpectedly for 12 hours under normal conditions (or under relatively minor environmental stress) and deprives its users of essential network services, the system can reasonably be judged to have failed its mission, even if data integrity and confidentiality are preserved. Therefore when a network fails, it is critical that some sort documentation be made available so as to assess and measure the survivability of that network. With documentation, assessment can be made to its foundation services, scalability, traffic analysis, utilization analysis, network monitoring and security tuning which are all important for the survivability of a network.

BIBLIOGRAPHY

Mark, A. Miller, P. E. (1996). *Troubleshooting TCP/IP*, pp. 65 – 256.

Mark Beaulieu (2001). *Wireless Internet: Applications and Architecture*. Addison Wesley, Boston, MA.

Rod Trent (2001). *IIS 5.0, A Beginner's Guide,* McGraw Hill, Berkeley, California.

Ed Bott, Carl Siechert (2006). *Microsoft Windows XP: Networking and Security* Microsoft Press, Redmond, Washington.

James F. Kurose, Keith W. Ross (2001). *Computer Networking: A Top-Down Approach Featuring the Internet* Addison Wesley.

Roberta Bragg (2004). MCSE Self-Paced Training Kit (Exam 70-298): Designing Security For A Microsoft Windows Server 2003 Network, Microsoft Press, Redmond, Washington.

Brien M. Posey. (2002) Documenting your network. http://www.brienposey.com/kb/documenting_your_network.asp. Date accessed: January 2008.

Appendix A

LOCAL AREA NETWORK
Technical Documentation

DOCUMENT CONTROL INFORMATION

Revision	Revision History	Date	Signatory
	Initial Release (Baseline)	15/08/06	
1	1st Revision	11/01/07	

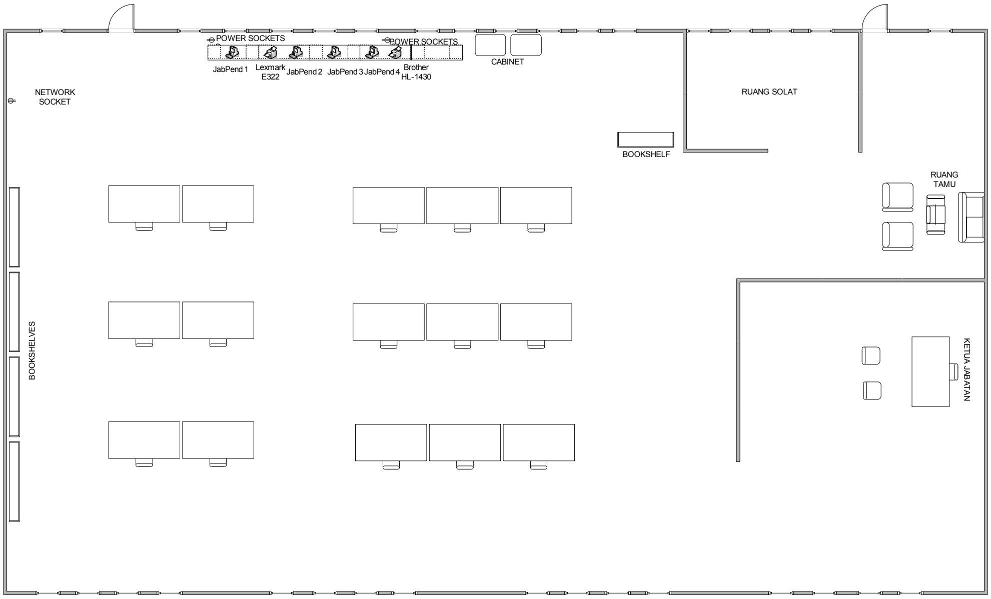
TECHNICAL DOCUMENTATION

OVERVIEW

The Department of Educational Studies has sixteen staff. It currently has 4 computers that are networked to a server running Windows NT. The network topography is of the extended star type. They are sharing a lease line (2MB) internet connection, and have a website at http://www.ipbl.edu.my

Overall, the department has computers ranging from five year old Pentiums to PIV computers, though most computers are 2-3 years old. The network is also showing its age, the wiring is all CAT5 but is not organized in any way, and connected to the hub. The print server is having a few problems, crashing occasionally and losing print jobs, but overall has been functioning well for the last couple of months. The hub (8 port) capacity is 10Mbps, and has 1 slot free.

NETWORK DIAGRAM



Network Floor Layout Plan

PHYSICAL NETWORK

Wiring

Item	Description
Wired By	Wong H K
Cable Type	UTP CAT5
Central Wiring Location	N/A
Wiring Diagram Stored Where	N/A

Hubs/switches

Make and Model	SSID	Protocol	IP Address	Encryption settings	Channel	Connected To
D-Link DE-600TC	N/A	IP	auto	none	8	Server

Wireless

Make and Model	Speed	Location	Ports		IP Address	User/ Password	Connected To
			Total	Free			
N/A							

PRINTERS

Printer Type	Share	Location	IP Address	Security
Lexmark E322	No	JabPend2	N/A	N/A
Brother HL-1430	Yes JabPend1 JabPend3 JabPend4	JabPend4	N/A	N/A

PRINTING – PRINT SERVER

Brother HL-1430	On/Off	Problem	Solution
Power Hub	On [no alarm] On	Scenario 1 Cannot print	Check parent [JabPend4] JabPend4 - operational
Power Hub	On [no alarm] On	Scenario 2 Cannot print	Check for virus
Power Hub	On [no alarm] On	Scenario 3 Cannot print	Restart printer
Power Hub	On [no alarm] On	Scenario 4 Cannot print	Restart JabPend4

WORKSTATIONS

User	OS/LICENSE	RAM	Processor	Processor Speed	Hard Drive		Office	Antivirus
					Total	Free		
JabPend1	Win ME JWQ73-CBGX8-YXCXF-KWK3Q-W32YM	128MB	P III	500Mhz	C -40GB	32GB	MS 2003	Panda Titanium
JabPend2	Win XP DYJMH-6YJRX-64BGD-CR372-6T8WO	256MB	P IV	2.4GHz	C -10GB D – 30GB	4GB 12GB	MS 2003	Panda Titanium
JabPend3	Win ME R386P-QW6BB-82RGJ-HXYR2-MTPGW	256MB	P IV	2.8GHz	C -40GB D – 40GB	34GB 37GB	MS 2003	Panda Titanium
JabPend4	Win XP DDJ47-4WR7F-VYYWC-4K9JB-8KQQT	256MB	P IV	1.5GHz	40GB	30GB	MS 2003	Panda Titanium

OPERATING ENVIRONMENT & USERS

Logging On

Computer ID	Protocol	Password	Class	Connected To
JabPend1	end-user	N/A	Administrator	Printer Brother HL-1430
JabPend2	Registered IPBL ID & password	Registered password	Ordinary user [ADMIN]	Printer Lexmark E322
	administrator	N/A	Administrator [JABILMUPEND]	Printer Lexmark E322
JabPend3	administrator	N/A	Administrator	Printer Brother HL-1430
JabPend4	administrator	N/A	Administrator	Printer Brother HL-1430