NETWORK INFRASTRUCTURE FOR E-COMMERCE COMPRISING OF HARDWARE AND SOFTWARE REQUIREMENTS

We need to understand our existing network infrastructure to determine how well it can meet the needs of our deployment goals. By examining our existing infrastructure, we identify if we need to upgrade existing network components or purchase new network components. We should build up a complete map of the existing network by covering these areas:

1. Physical communication links, such as cable length, grade, and so forth
2. Communication links, such as analog, ISDN, VPN, T3, and so forth, and available bandwidth and latency between sites
3. Server information, including:
    - Host names
    - IP addresses
    - Domain Name System (DNS) server for domain membership
4. Locations of devices on your network, including:
    - Hubs
    - Switches
    - Modems
    - Routers and bridges
    - Proxy servers
5. Number of users at each site, including mobile users

After completing this inventory, you need to review that information in conjunction with your project goals to determine what changes are required so that you can successfully deliver the deployment.

Routers and Switches

Routers connect networks of your infrastructure, enabling systems to communicate.

You need to ensure that the routers have spare capacity after the deployment to cope with projected growth and usage.

In a similar vein, switches connect systems within a network. Routers or switches running at capacity tend to induce escalating bottlenecks, which result in significantly longer times for clients to submit messages to servers on different networks. In such cases, the lack of foresight or expenditure to upgrade the router or switch could have a personnel productivity impact far greater than the cost.

Firewalls

Firewalls sit between a router and application servers to provide access control.

Firewalls were originally used to protect a trusted network (yours) from the untrusted network (the Internet). These days, it is becoming more common to protect application servers on their own (trusted, isolated) network from the untrusted networks (your network and the Internet).

Router configurations add to the collective firewall capability by screening the data presented to the firewall. Router configurations can potentially block undesired services (such as NFS, NIS, and so forth) and use packet-level filtering to block traffic from untrusted hosts or networks.

In addition, when installing a Sun server in an environment that is exposed to the Internet, or any untrusted network, reduce the Solaris software installation to the minimum number of packages necessary to support the applications to be hosted. Achieving minimization in services, libraries, and applications helps increase security by reducing the number of subsystems that must be maintained. The Solaris™ Security Toolkit provides a flexible and extensible mechanism to minimize, harden, and secure Solaris systems.

Web Servers:

Web servers are electrical devices known as computers that open pages on the web. Each web server has an IP address and also on some occasions a domain name. An example of this is when you type in a URL in your browser it sends a request to the web server whose domain name it is. Computers can be turned into a web server by installing server software and connecting it to the internet.

The most common use of web servers is to host websites but there are other uses such as data storage or running enterprise applications.

Browsers:

Browsers are software applications that are used to locate and access web pages. Browsers also translate HTMLs which allows us to view images, videos and listen to audios on the website as well as hyperlinks in which allows us to travel from page to page. Browsers request information from the web servers and then the web servers display the information required.

Examples of some web browsers are Mozilla Firefox, Google Chrome and Internet Explorer.

Server Software:

Server Software is used by web developers mainly. It is software that allows web developers to add more web pages to their websites easily. Without the software it would be a pain trying to add another web page to an already made website. The software works through a process known as FTP (file transfer protocol) this process uploads web pages directly onto a website without any problems.

Examples of some server softwares are FreeNas, Ubuntu server edition, Apache, etc.

Web Authoring Tools:

Web authoring enables a user to develop a website in publishing format. It will first generate the required HTML for the layout of the web page based on the desired design. Any software program that can be used to create content that can be uploaded and viewed on the Internet or intranet network systems is considered a web authoring tool.

Database Systems:

Database systems are a bunch of programs that allow you to store modify and extract information from the database. Database systems are not just of one size; depending on how big the systems are. It can contain many things that will be changed by the users of the website. The database will store passwords, names, addresses, store items and other business information.

For example: You will have a small database for a personal computer but large one in businesses.

Domain Name:

A domain name is your website name. A domain name is the address where Internet users can access your website. A domain name is used for finding and identifying computers on the Internet. Computers use IP addresses, which are a series of number. However, it is difficult for humans to remember strings of numbers. Because of this, domain names were developed and used to identify entities on the Internet rather than using IP addresses.

A domain name can be any combination of letters and numbers, and it can be used in combination of the various domain name extensions, such as .com, .net and more.

The domain name must be registered before you can use it. Every domain name is unique. No two websites can have the same domain name. If someone types in www.yourdomain.com, it will go to your website and no one else's.

TCP/IP Address:

TCP/IP includes an Internet addressing scheme that allows users and applications to identify a specific network or host to communicate with. An Internet address works like a postal address, allowing data to be routed to the chosen destination. TCP/IP provides standards for assigning addresses to networks, sub networks, hosts, and sockets, and for using special addresses for broadcasts and local loopback.

Each computer must have a unique IP address. An IP address is a 32-bit number that uniquely identifies a host (computer or other device, such as a printer or router) on a TCP/IP network. TCP/IP uses four numbers to address a computer. The number is always between 0 and 255.

IP addresses are normally written as four numbers separated by a period, like this: 192.168.1.50.

TCP/IP is used when transferring data across a network. If computers do not use the same protocol, it becomes impossible for the data to be understood.

Ports and Protocol:

As per its word definition, a protocol is a set of rules. In computer networking, a protocol defines a standard way for computers to exchange information. Most common protocols used in computer networks and the internet are TCP (Transmission Control Protocol), UDP (User Datagram Protocol), and IP (Internet Protocol).

A port in computer networking is a logical access channel for communication between two devices. Bi-directional communications and more complex connections may use multiple ports simultaneously.

Data on the Internet is organized into standard TCP or UDP packets. Network clients use different ports (or channels) to transfer this data. Generally one port is used to send data and another to receive it, so packets don't collide. The port number (and the destination IP address) is included as part of the header each packet is given. Ports range from 1 to 65535 for the TCP and UDP protocols.