Contents

Task1

Critically evaluate different internet technologies and communication protocols. [1.1, M1]

Introduction

The Internet has already become a fundamental source for finding information related to a certain field, engaging in expert dissertation, gain access to available published materials, or checking weather. Internet has become the tool that is preferred over other communication technologies such as telephone to receive news, personal massage or data graphics. According to OPENBOOKPROJECT (n.d.) a standout amongst the most well-known uses individuals have for the Internet is the World Wide Web. At whatever point you say you are "on the Internet" you are utilizing the World Wide Web. When you are surfing the Internet through diverse pages you are traveling through the World Wide Web. Then again, that is not by any means the only use for the Internet.

Email is another exceptionally well known use for the Internet. Web email may travel and be put away decoded on numerous different systems and machines out of both the sender's and the beneficiary's control. Remote access is another extremely regular use for the Internet. The Internet permits PC clients to interface with different PCs and data stores effortlessly, wherever they may be over the world. Document sharing is additionally prevalent. It permits individuals to send documents through email, FTP, distributed systems, and so on.

To function internet and different internet technologies such as World Wide Web, emails, communication and communication protocols are required to be followed. These protocols includes TCP/IP, DHCP, and SMTP etc. This paper critically evaluates these communication protocols along with their use in internet technologies.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Internet Protocol (IP) and Transmission Control Protocol (TCP) are often linked together but are two different protocols. Generally, two protocols are linked in cases where functions of both protocols are complementary to each other. Together they help to achieve particular task but alone they are not much helpful. This process of combining two or more protocol is termed as stack. Term TCP/IP is utilized to refer the whole suite of protocols that regulates the functions of web, though it is also utilized in LAN (Local Area Network) system.

According to Rouse (n.d.) TCP/IP is two layer application. First layer (higher layer) is TCP (Transmission control protocol) which creates packets and put them together again in correct order

at the other end. Packets are broken pieces of information. TCP assembles files or massage into packets to enable fast communication as different packets are transmitted using different routes at same time and all packets are received and reassembled together by receiver. TCP also ensures minimal information loss by checking the packets received while reassembling. Lost data packet are requested in order to put received file/massage correctly. On the other hand, IP (Internet protocol), the other layer of TCP/IP is protocol that is utilized to route data to correct address. Each resources in network has their own unique identity which allows network to recognize them. This identity address is known as IP address. In data communication, packets created utilizing TCP contains IP address that provides location for destination. Network checks these IP addresses in packets to deliver packet to right destination computer. By this way, TCP and IP forms TCP/IP and utilized in communication. Implementation of TCP/IP suite includes protocols UDP and ICMP. User Datagram Protocol (UDP) is protocol similar to TCP but it does not check packets and does not guarantees receipt of data. Whereas Internet Control Message Protocol (ICMP) is utilized to send error messages.

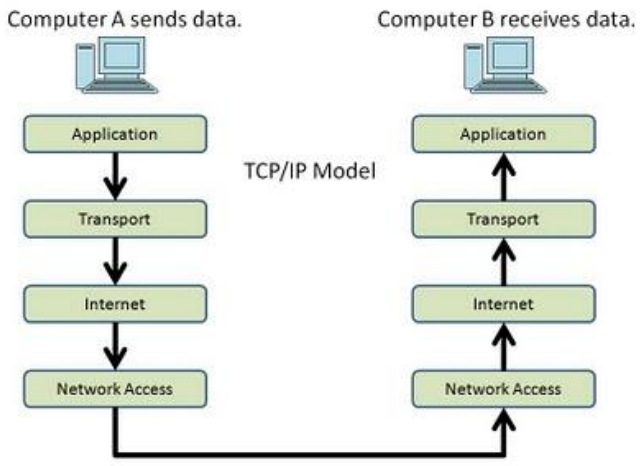


Figure 1 Data communication in TCP/IP (Source: http://www.samos.aegean.gr)

TCP/IP itself functions in 4 layers to enable information communication (WHATISNETWORKING, n.d.). First layer is Network access which is basically physical components while second layer enables to connect host with other resources of network. Third layer is known as transport which enables data transportation. And finely application layer provides interface to communication. This layer utilizes transport layer to send or receive information. Internet technologies depends on TCP/IP to communicate and following are some of the key benefits and weaknesses of TCP/IP communication protocol. Major benefits and limitations of TCP/IP technology is listed below.

Benefits

- It enables communication between computers/ allows to form network environment
- It is platform independent which means it does not depends on operating system
- Ensures minimal packet loss by rechecking package number
- Givers suitable error message based on the fault
- It automatically assemble information into small packets for past data transmission before sending and reassemble them into one piece after receiving.

Weaknesses

- A protocol owned by Xerox, **Internetwork Packet Exchange** is faster protocol
- TCP has higher overheads
- TCP/IP has inborn security disadvantages

Open System Interconnection (OSI)

OSI model is a reasonable and legitimate format that characterizes system correspondence utilized by system open to interconnection and communication with different systems. In the event that system communication needs to happen with no inconvenience, numerous issues must fathomed. Organizing every one of these issues are so mind boggling and difficult to oversee. To make these assignments smooth, in 1978 the International Standards Organization (ISO) proposed the Open Systems Interconnection (OSI) system model (Technopedia, n.d.). The Open Systems Interconnection (OSI) model separates the issues included in moving information starting with one PC then onto the next PC. Open Systems Interconnection (OSI) model arranges these many issues to Seven Layers as shown in figure 3.

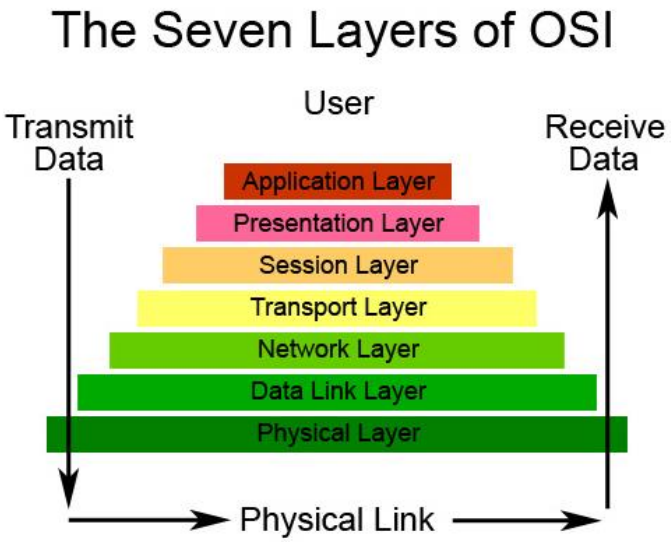


Figure 2 Layers of OSI (Source: https://networksmania.files.wordpress.com)

Open Systems Interconnection (OSI) Seven Layered reference model is just barely a reference model. Every one of the issues which are identified with the correspondences are replied by particular protocol working at diverse layers. Each layers of OSI model is evaluated below here.

Layer 1. Physical Layer

First layer of OSI model is referred as physical Layer. This layer consists of physical circuits to enable communication. It portrays the optical or electrical signal utilized in network for communication. According to OMNISECU (n.d.) this layer only concerns with electrical attributes such as physical state of connector, synchronization, voltage of electrical current used in communication, media type such (optical, twisted pair, coaxial cable etc.). This layer is responsible for providing hardware mean for communication.

Layer 2. Data link Layer

The Data Link layer dwells over the Physical layer and underneath the Network layer. Data link layer is in charge of giving end-to-end legitimacy of the information being transmitted. The Data Link Layer is coherently partitioned into two sub layers, The Media Access Control (MAC) Sub layer and the Logical Link Control (LLC) Sub layer.

Physical address of host is determined by MAC (Media Access Control). The MAC sub-layer keeps up MAC addresses (physical device addresses) for speaking with different gadgets on the system. MAC locations are blazed into the system cards and constitute the low-level location used to decide the source and destination of system movement. MAC Addresses are otherwise called Physical locations, Layer 2 addresses, or Hardware addresses. The Logical Link Control sub layer is in charge of synchronizing edges, blunder checking, and stream control.

Layer 3. Network Layer

The Network layer of the OSI model which is third layer is in charge of overseeing coherent tending to data in the parcels (packets) and the transmission of those bundles to the right destination. The network layer is in charge of working with logical locations. To uniquely identify computer and identity of network, logical address is utilized. This logical addressing system is known as IP address. This layer gives switching and routing advances, making sensible ways, known as virtual circuits, for transmitting information from node to node. Routing and Forwarding are elements of this layer. This layer also function error handling, packet sequencing, congestion control etc.

Layer 4. Transport Layer

The fourth layer of OSI model which is also called transport layer is enables transparent communication of information between systems. This layer gives end to end transport benefits and builds up the coherent association between two PCs. Two transport conventions, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) sits at this layer. Primary difference between these two protocols are speed and reliability. TCP sets up associations between two hosts on the system through "sockets" which are controlled by the IP address and port number. TCP monitors the packet delivery. This makes TCP reliable protocol. UDP then again gives a low overhead transmission service, yet with less mistake checking and higher speed.

Layer 5. Session Layer

The session layer is in charge of building up, overseeing, and ending communication between applications at every end of the correspondence. In the association foundation stage, the service and the rules (who transmits and when, the amount of information can be sent at once and so on.) for correspondence between the two device are proposed. Data transfer phase begins once rules are established. Association end happens when the session is finished, and connection closes effortlessly.

Layer 6. Presentation Layer

The presentation layer gets data from the application layer and deciphers in the format that all PCs can get it. The presentation layer is not worried with the importance of information. This layer is likewise intended to handle issues identified with compression and encryption. Presentation level consists of External Data Representation (XDR. It changes representation of information to its accepted structure and the other way around. At the point when the presentation layer gets information from the application layer, to be sent over the system, it ensures that the information is in the correct configuration. On the off chance that it is not, the presentation layer changes over the information to the best possible arrangement. On the opposite side of correspondence, when the presentation layer gets system information from the session layer, it ensures that the information is in the best possible organization and by and by believers it in the event that it is definitely not.

Layer 7. Application Layer

According to SIMPLILEARN (n.d.) the application layer works closer to the client and gives system administrations to the end-clients. This layer does exclude the genuine applications but rather the conventions that backing the applications. Mail, ftp, telnet, DNS, NIS, NFS are samples

of system applications. Application Layer is the top-most layer of the seven layered Open Systems Interconnection (OSI) system model. Genuine movement information will be regularly produced from the Application Layer. This may be a web demand created from HTTP convention, a command from telnet convention, a record download demand from FTP convention and so forth. Some of the key benefits and limitations of OSI model is listed below.

Benefits

- OSI model breaks complex problem into smaller pieces
- It does not rely on particular computer system
- It provides compression and encryption facility to enhance security purpose
- Provides Standardizes interfaces to allows multiple vendor support
- It facilitates modular engineering allowing hardware model and software model communicate together

Weaknesses

- OSI model provides data integrity which many application does not required. This unnecessarily consumes resources.
- This model is yet to adapt to all telecommunication applications.
- It is complex model as it is associated with variety of layer protocol. Working together with large number of protocols are complex.

Dynamic Host Configuration Protocol (DHCP)

It is one of the imperative correspondence conventions that helps the administrator to manage the PC in the system centrally and allot the Internet Protocol (IP) address consequently in networking environment. According to Indiana University (n.d.) Dynamic Host Configuration Protocol (DHCP) is a system convention that empowers a server to automatically relegate an IP location to a PC from a characterized scope of numbers (i.e., a scope) arranged for a given system. Administrators are required to allocate IP address to each resources in network in order to make the recognizable by other resources in network. Manual IP addressing can still be useful for very small network but when it comes to large networking environment, manual distributing of IP can be time consuming and stressful. With DHCP it allows to distribute IP to client computers automatically based on the IP scope defined by administrator.

Working Functionality

Arora (n.d.) explains the working functionality of DHCP as a client-server model based protocol. Figure 3. Demonstrates functionality of DHCP technology. When a client is connected to network consisting DHCP server, DHCPDISCOVER massage is sent to server from that client to find DHCP mechanism consist in connected network environment. DHCPDISCOVER massage is then received by DHCP server and replies with DHCPOFFER. This massage contains IP configuration as well as DNS and default gateway can also be included in this massage (optionally). Once client receives DHCPOFFER massage it replies server with DHCPREQUEST massage to inform server that it is ready to accept configuration. And finally, DHCPREQUEST massage is received by server and replies with DHCPACK massage to indicate client can use the IP configuration. These configuration are lease based. Once lease is expired DHCP server may use same IP address for another client.

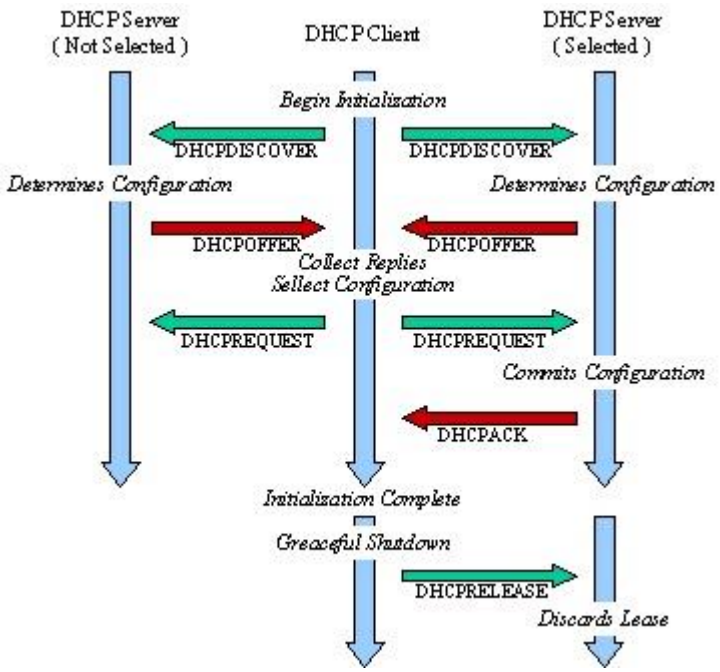


Figure 3DHCP functionality

Benefits

Static IP addressing is utilized to manually configure IP address of clients. This methodology has multiple issues that can be address via DHCP IP addressing. One problem of static IP addressing is it can be prone to error or misconfiguration resulting loss of service. With DHCP all computers receives IP address based on pre-defined IP range (scope) which makes it less prone to misconfiguration. Another benefit of DHCP is it allocates IP address automatically and which is far less time consuming. DHCP IP are temporary which expires in certain defined timeframe, this

is ideal for a network where client are temporary and IPs are required freed regularly. DHCP is capable of distributing gateway address, DNS address, subnet mask which helps to centrally manage network.

Weaknesses

DHCP is popular due to its large number of benefits to network configuration, but it has its limitations. One of the key drawback of DHCP is network becomes reliant on DHCP server, failure in DHCP can jeopardize whole network environment. Misconfiguration in defining IP scope results whole network failure. Another limitation of DHCP is it is not suitable of resources that requires permanent IP address such as servers, printers etc.

Simple Network Management Protocol (SNMP)

According to MANAGEENGINE (n.d.) SNMP (Simple Network Management Protocol) is a part of TCP/IP protocol suite. It is an application–layer convention characterized by the Internet Architecture Board (IAB) in RFC1157 for trading administration data between system gadgets. SNMP is one of the generally acknowledged conventions to oversee and screen system components. The majority of the professional–grade system components accompany packaged SNMP agent. It is a standard method for observing equipment and configuration from almost any producer, from Juniper, to Cisco, to Microsoft, UNIX, and everything in the middle. SNMP requires just two or three fundamental segments to work: an administration station, and an agent.

Straightforward Network Management Protocol (SNMP) is a prominent convention for system administration. It is utilized for gathering data from, and designing, system gadgets, for example, servers, printers, center points, routers, and switches on an Internet Protocol (IP) system. Microsoft Windows Server 2008 gives SNMP agents that works with third party SNMP software tools to screen the status of oversaw gadgets and applications. Generally it is utilized as a part of administration of system framework with a specific end goal to screen system appended gadgets and advice to network head in regards to conceivable strings. Various feature of SNMP is listed here below:

Features

SNMP is powerful yet simple and has the ability to provide assistance in managing network through:

- Provides ability to remotely reconfigure IP address or remotely reset passwords

- Collect bandwidth consumption information
- College information about errors and report them into log
- Monitor and Alert administrator when disk, CPU, memory us thresholds are exceeded as shown in figure 2 below.

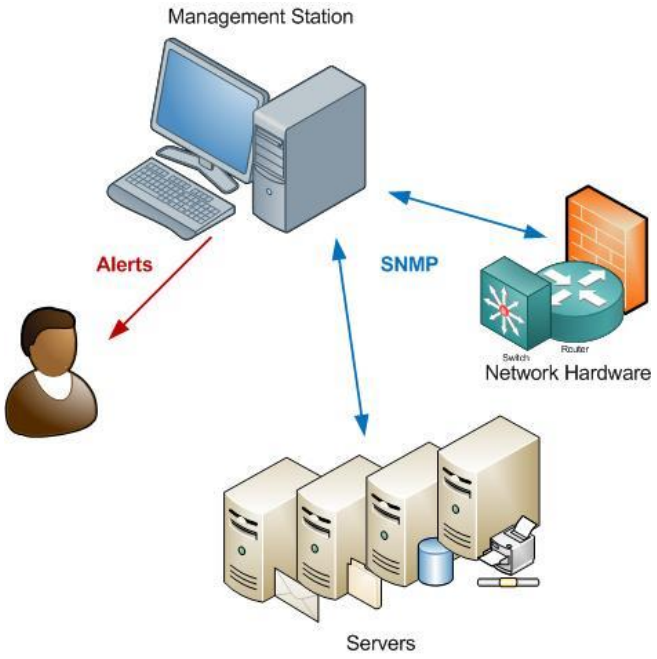


Figure 4Basic SNMP Functionality (Source: http://www.networkmanagementsoftware.com)

Benefits

SNMP compliant network provides various benefits to the management of the networking environment. Implementing such application allows administrators to manage system efficiently. Key benefits of SNMP is discussed below.

- **Control:** SNMP is anything but difficult to-utilize and permits administrators the control they require to keep up a solid system. The advantages of running a SNMP- application incorporate the capacities to forestall, distinguish, and adjust system related issues. It enables administrator with a system administration component that proficiently screens system performance.
- **Popularity:** Practically all network equipment manufacturer today supports SNMP. Which enables to extremely effective and wide spread solution to system management in centralized manner. Since, TCP/IP has become so popular, importance of SNMP has been more significant.

- **Productivity**: SNMP enables to monitor bandwidth usage, resource usage which allows to prevent unwanted network related issues. This increases productivity of the system.

Weaknesses

Though SNMP has significant benefits, it has its own limitations as well. One of the biggest concern of SNMP is security issues. It fails to provide adequate security features such as encryption and massage authentication. With these security incompetence, it fails to prevent unauthorized users to execute network management functions. But fortunately latest version which is SNMPv3 address these issues and provide enhancement is security.

File Transfer Protocol (FTP)

The File Transfer Protocol (FTP) was one of the first endeavors to make a standard method for trading documents over a TCP/IP system, so the FTP has been around since the 1970's, NCFTP (n.d.). The FTP was composed with however much adaptability as could reasonably be expected, so it could be utilized over systems other than TCP/IP, and being built to have the capacity with trading documents with a wide assortment of machines. FTP convention characterizes the route in which information must be exchanged over a TCP/IP system. The core roles of FTP protocol is to enable file sharing among remote devices using web browser (shown in figure 4) and allow efficient information transfer.

In a securely configured environment, FTP requires two PCs, one running a FTP server, the other running a FTP client. The trade is started by the client which sign in under an acknowledged client name and secret key (username and password). Once this happens, a session is opened and stays open until shut by either the customer or the server, or until it times out. While the session is open, the customer may execute various FTP commands on the server. These incorporate commands to change folders, list files, get documents and put records.

Now Question arises if FTP is better than HTTP for downloading files, and the answer is yes, as a self-evident truth it seems to be. HTTP is intended to bring site pages. It is enhanced for various rehashed brings of little things. FTP is intended for exchanging records, and offers speedier general throughput and better mistake checking. It is not exceptional for a client to fail more than once to download a substantial record by means of HTTP via web browser, just to succeed on their first attempt while utilizing a devoted FTP client.

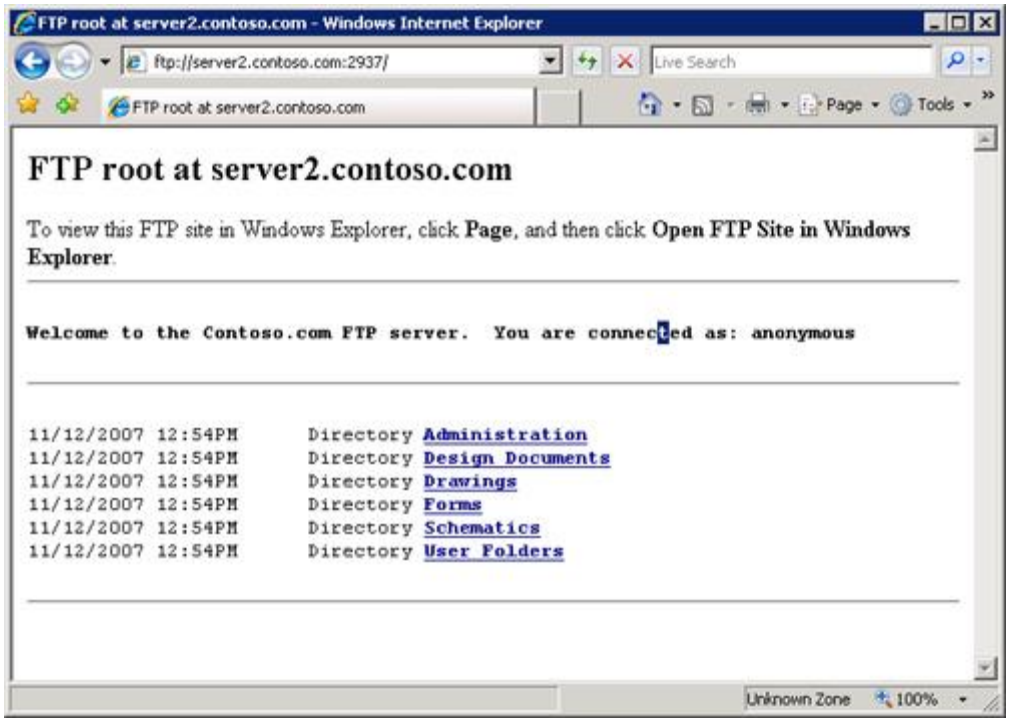


Figure 5 FTP file sharing (source: http://mscerts.wmlcloud.com)

FTP has enabled various benefits to the information technologies while it still possess few significant drawbacks. But advancement of technologies allows to mitigate limitations of FTP technology while utilizing its benefits. Some of the key benefits and limitations of FTP protocol is provided below.

Benefits

- Allows single transfer with no size limitation
- Enables to transfer multiple directories or files
- It offers much better transfer speed that HTTP
- Allows to secure connectivity via authentication

Weaknesses

- One of the key weaknesses of FTP technology is username and password submitted while authenticating and files are not encrypted and are sent in clear text which fails to improve security
- Security is not highlight of FTP server as it is not designed to be a secured protocol

Internet Control Message Protocol (ICMP)

According to TECHTERMs (n.d.) when data is exchanged over the Internet, PC frameworks send and get information utilizing the TCP/IP convention. On the off chance that there is an issue with

the association, blunder and status messages in regards to the association are sent utilizing ICMP, which is a piece of the Internet convention. In situations where there is an issue with the association (figure 5), ICMP can send back codes to your framework clarifying why an association fizzled. These may be messages, for example, "network unreachable" for a framework that is down, or "access denied" for a safe, secret word secured framework. ICMP might likewise give directing recommendations to sidestep inert frameworks. While ICMP can send an assortment of distinctive messages, most are never seen by the client. Regardless of the possibility that you do get a mistake message, the product you are utilizing, for example, a Web program, has in all likelihood as of now made an interpretation of the message into straightforward (and ideally less specialized) dialect you can get it.

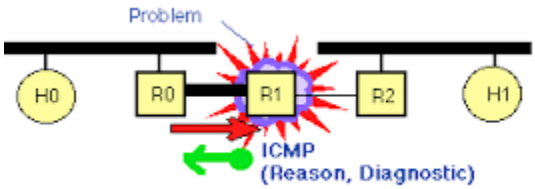


Figure 6 ICMP demonstration

NETWORKSORCERY (n.d.) suggest ICMP messages are sent in a different circumstances: for instance, when a datagram cannot achieve its destination or when the gateway not have the buffering ability to forward a datagram, and when the gateway can guide the host to send activity on a shorter course. The Internet Protocol is not intended to be totally solid. The motivation behind these control messages is to give criticism about issues in the correspondence environment, not to make IP dependable. There are still no sureties that a datagram will be conveyed or a control message will be returned. Some datagrams might in any case be undelivered with no report of their loss. If dependable communication is required, higher level protocols that utilizes IP must enforce their won reliability practice. The ICMP messages normally report blunders in the handling of datagrams. To maintain a strategic distance from the unending relapse of messages about messages and so forth, no ICMP messages are sent about ICMP messages.

Williams (n.d.) writes ICMP convention systems assists administrators by helping them in diagnosing system issues. Most issues that emerge, similar to server blackouts or PC failure, are resolved with two supportive commands. These commands are PING and TRACERT. An administrator utilizes PING to send a request from the PC he uses to another PC or server. This request traversed the system and, once it achieves the other machine, an answer gets sent back to

the first PC telling the overseer that the correspondence was gotten. TRACERT performs the same capacity as PING. This enables administrator to view the request path and analyze the issue. Another benefits of ICMP is it enables administrator with diagnosing network speed by sending timed request across the network. Which allows to identify blockage that is causing network slow down.

Simple Mail Transfer Protocol (SMTP)

Today, email is distributed utilizing a client/server structural design. An email message is created using a mail client platform. This application then directs the message to a server. The server then forwards the message to the receiver's email server, where the message is then delivered to the receiver's email client. SMTP is one of the commonly utilized protocol in email technology. Microsoft (n.d.) notes according to RFC 821 "*The objective of the Simple Mail Transfer Protocol (SMTP) is to transfer mail reliably and efficiently".* SMTP is protocol utilized to send and receive e-mails. But its ability is limited to queue messages at receiving end and does not have ability to save mails it requires other protocols as complement. However, for it is still highly preferred technology for LAN environment.

SMTP typically is applied to function over Internet port 25. A substitute to SMTP that is extensively used in Europe is X.400. Extended Simple Mail Transfer Protocol (ESMTP) is now supported by several mail servers, which allows multimedia records to be transported as e-mail. This feature is not support in SMTP as name suggest it can only send simple mails. At whatever point you send a bit of email, your email client application communicates with the SMTP server to handle the sending. The SMTP server on your host might have discussions with other SMTP servers to convey the email as shown in figure 5 below. According to Brain and Crosby (n.d.) when an email is sent to an address let's say Atut@kathhospital.com, SMTP takes this address and breakdowns it into two parts. Before @ "Atut" is recipient name whereas kathhospital.com is domain name. Sending client connects with local server using SMTP and local server connects with destination server again using SMTP. Receiving end may utilize POP3 to receive emails as it provides ability to save.

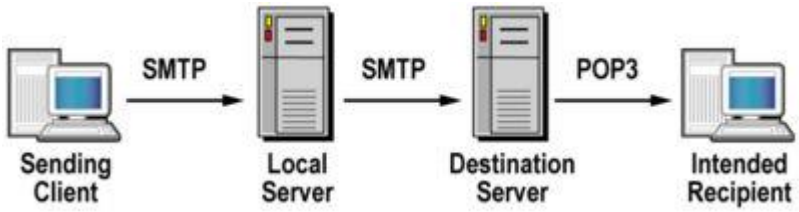


Figure 7 SMTP Email Transfer (Source: http://www.hill2dot0.com)

SMTP is very popular protocol being practiced for email delivery due to its benefits though it has some limitations as well. Some of the key benefits and drawbacks of the SMTP protocol is evaluated below.

Benefits

With effective and simple features, SMTP continues to be most extensively applied email conventions as most of the emails are still text based. Simplicity is one of the key benefit of SMTP as it provides simples mean of email delivery. End users does not have any annoyance as they only requires to provide address and content of the message. SMTP also provides quick email delivery as multimedia files are not supported as part of email and delivery process is simple. BENEFITOF (n.d.) writes, SMTP offers reliability. By reliability it means outgoing mails are sent repeatedly until it is not successfully sent.

Weaknesses

While SMTP has significant benefits, it has limitations as well. One of the key limitation being inability to provide email storage feature. To address this issue POP3 (Post Office Protocol V3) is utilized. This makes SMTP ineffective for internet based email system. Another drawback of SMTP is inability to send multimedia data. This issue is solved via use of Extended SMTP.

Conclusion

This paper has critically evaluated several protocols related to internet technologies and communication. Internet technologies and communication protocols are set of rules that enables to establish proper network environment. Each protocol has their own role to play, TCP/IP helps to establish communication while DHCP allows to distribute IP address. Similarly, SNMP enables administrator to manage networking environment. Other protocols are FTP and SMTP which enables files transfer, mail transfer. These protocols enables to standardize the network and allow to provide internet services. These protocols helps organization to achieve business requirement by establishing required network.

References

- Arora, H. (n.d.) [Online] Available: what is DHCP and How DHCP Works? (DHCP Fundamentals Explained) http://www.thegeekstuff.com/2013/03/dhcp-basics/ Accessed [10/11/2015]
- BENEFITOF (n.d.) benefits-of-SMTP [Online] Available: http://benefitof.net/benefits-of-smtp/ Accessed [10/11/2015]
- Brain, M. and Crosby, B. (n.d.) How E-mail Works [Online] Available: http://computer.howstuffworks.com/e-mail-messaging/email3.htm Accessed [10/11/2015]
- Indiana University (n.d.) what is DHCP? [Online] Available: https://kb.iu.edu/d/adov Accessed [10/11/2015]
- MANAGEENGINE (n.d.) SNMP tutorial [Online] Available: https://www.manageengine.com/network-monitoring/what-is-snmp.html Accessed [10/11/2015]
- Microsoft (n.d.) Simple Mail Transfer Protocol [Online] Available: https://msdn.microsoft.com/en-us/library/aa480435.aspx Accessed [10/11/2015]
- NCFTP (n.d.) an Overview of the File Transfer Protocol [Online] Available: http://www.ncftp.com/libncftp/doc/ftp_overview.html Accessed [10/10/2015]
- NETWORKSORCERY (n.d.) ICMP, Internet Control Message Protocol [Online] Available: http://www.networksorcery.com/enp/protocol/icmp.htm Accessed [10/11/2015]
- OMNISECU (n.d.) Seven Layers of OSI Model and functions of seven layers of OSI model [Online] Available: http://www.omnisecu.com/tcpip/osi-model.php Accessed [10/11/2015]
- OPENBOOKPROJECT (n.d.) History of the Internet [Online] Available: http://openbookproject.net/courses/intro2ict/internet/history.html Accessed [10/10/2015]
- Rouse, M. (n.d.) TCP/IP (Transmission Control Protocol/Internet Protocol) definition http://searchnetworking.techtarget.com/definition/TCP-IP Accessed [10/10/2015]
- SIMPLILEARN (n.d.) Understanding Open Systems Interconnection Reference Model (OSI) [Online] Available: http://www.simplilearn.com/understanding-open-systems-interconnection-reference-model-osi-article Accessed [10/11/2015]

- Technopedia (n.d.) Open Systems Interconnection Model (OSI Model) [Online] Available: https://www.techopedia.com/definition/24205/open-systems-interconnection-model-osi-model Accessed [10/10/2015]
- TECHTERMS (n.d.) ICMP [Online] Available: http://techterms.com/definition/icmp Accessed [10/11/2015]
- WHATISNETWORKING (n.d.) Advantages and Disadvantages of TCP/IP Model [Online] Available: http://www.whatisnetworking.net/tag/advantages-and-disadvantages-of-tcpip-model/
- Williams, J. (n.d.) What Are the Benefits of Internet Control Message Protocol? [Online] Available: http://www.ehow.com/list_6742787_benefits-internet-control-message-protocol_.html

Task2

Critically compare different internet services and internetworking servers. [1.2, M2]

Introduction

The Internet is a worldwide arrangement of interconnected PC organizes that utilizes the standard Internet Protocol suite (TCP/IP) to serve a few billion clients around the world. It is a system of systems that comprises of a large number of private, open, scholarly, business, and government systems, of neighborhood to worldwide extension, that are connected by a wide cluster of electronic, remote and optical systems administration advances (Afriyie, 2012). The Internet conveys a broad scope of data assets and administrations, for example, the inter-linked hypertext archives of the World Wide Web (WWW), the base to support email, and distributed systems.

The most crucial capacity of the Internet is to pass electronic data starting with one PC then onto the next. Each PC on the system is recognized by a 32 bit Internet Address or IP-address. This number is normally spoken to as four numbers joined by periods. The Internet utilizes these numbers to guide data through the system ("routing"). For human clients, on the other hand, such numbers are typically hard to remember. In this manner, PCs are additionally recognized by Domain Names, which are to some degree like street numbers. Unique projects, called "Name Servers", make an interpretation of Domain Names into IP-Addresses. Individuals everywhere throughout the world uses internet based services for different purposes, for example, correspondence, data gathering, downloading media and so forth. This paper critically compare various internet services while also comparing inter-networking servers which supports these internet services such as database servers, email servers, media servers directory servers etc.

Internet services

TUTORIALSPOINT (n.d.) writes Internet services enables clients to access to large amount of information resources such as graphics, texts, software and sound over the Internet. Internet services includes four major categories as shown in figure 1. Exchange of data between individual clients are enabled by communication services such as email, chat, and internet telephony etc. Other service category consists information retrieval which offers easy access to resources via internet such as File transfer protocol. Another internet service is web services which enables give-and-take of information between web applications. This allows web applications to interact with each other. And final and one of the most popular internet service is WWW which is also referred as W3.

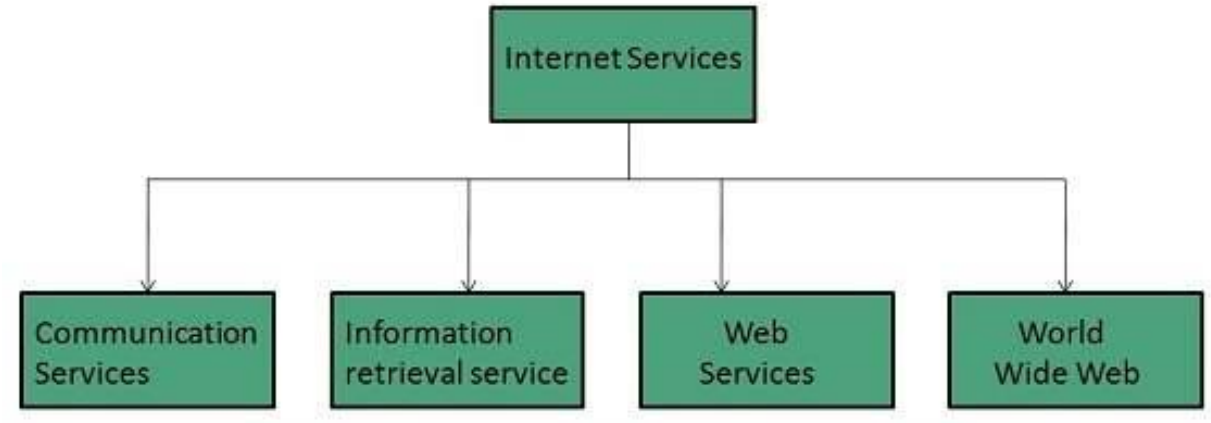


Figure 8Varios Internet services types (Source: Tutorialspoint.com)

WWW allows clients to access documents (web pages) and view them in application called browser. Web pages includes contents such as audio, hyperlinks, videos, texts, images etc. This document critically compare different internet services such as intranets, directory services, DHCP, DNS etc.

Intranet

Intranet is a "Private system" with a limited number of PCs interconnected and controlled in a characterized way. Intranet part of internet and is setup and controlled by an administrators to guarantee secure and continuous association between individuals to trade data all the more productively. Association necessities might incorporate sharing most recent news overhauls, administration data, association changes, new arrangements and methods and so on. According to Dellpe (2014) Intranet is much like the Internet, yet it is disengaged from the outer world. Firewalls are utilized to associate Intranet to the outside world when it must be joined with Internet. It utilizes same conventions like TCP/IP. Size of the Intranet relies on upon the association necessities.

It might compass more than one building, one zone, or one nation. Moreover, there are numerous multinational associations keep up Intranets between nations utilizing committed fiber optic associations. Correspondence effectiveness between system gadgets is high since the transfer speed is completely doled out to a settled number of clients. There are no continuous activity spikes, channel breakdowns or server disconnected from the net circumstances in the Intranet. Intranet may be available through the Internet. There are strategies like VPN association with give secure associations in such circumstances. Intranet is basically running internet services inside a corporate LAN as shown in figure 1, entire LAN is behind firewall. Intranet is capable of running internet

services like HTTP services, FTP services or Email services but within defined network boundaries.

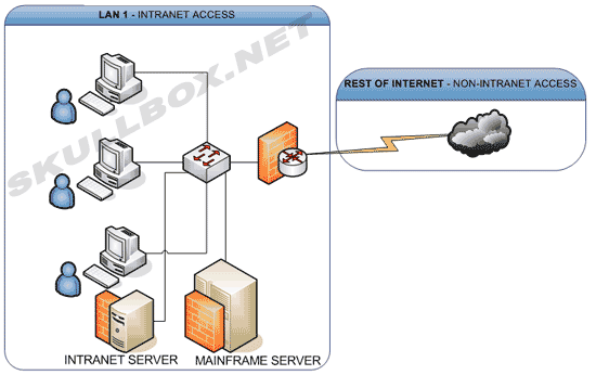


Figure 9 Simple Intranet Diagram (Source: http://www.skullbox.net/intranet1.gif)

To provide secure access to an Intranet from outside, Extranet is utilized which is piece of Intranet itself. According to an article in Webopedia (n.d.) Extranet popular expression that alludes to an intranet that is in part available to approved outcasts. While an intranet lives behind a firewall and is open just to individuals who are individuals from the same organization or association, an extranet gives different levels of availability to untouchables. You can get to an extranet just on the off chance that you have a substantial username and secret word, and your character figures out which parts of the extranet you can see.

Many business companies requires to allow their partners or clients to connect to securely connect to intranet to achieve business needs as shown in figure 3. As Intranet supports internal member to access the system, extranet enables external members to join and use intranet resources. In most cases these external clients are given limited authorization. Extranets are turning into an extremely famous means for business accomplices to trade data.

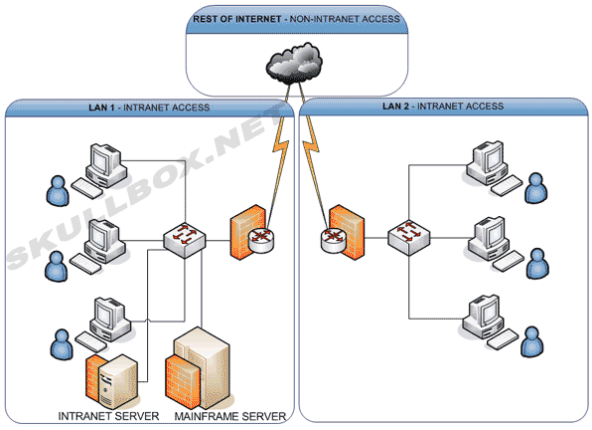


Figure 10 Extranet layout

Intranet and Extranet Comparison

Component	Intranet	Extranet
Central repository	Allows central repository	Allows central repository
Collaboration Tool	Enable improved collaboration	Enable improved collaboration
Web Accessibility	Only locally accessible	Utilizes secure web technology
Technical Structure	Administrator assign and control access and only internal members are allows	External members are allowed to access extranet through VPN

In table above critical comparison between intranet technologies is done. An article in Hyperoffice (n.d.) analyzes key similarity and differences between intranet and extranet. Corporate networks are allowed to store and share projects, group calendars and documents centrally both in intranet and extranet. Similarly, both allows improved association among distributed employees, partners etc. One of the key difference between intranet and extranet is their web accessibility. Generally intranet is accessible from within corporate network whereas extranet utilizes secured web technologies to connect intranets. Other difference being ability to server internal members and external members. Due to similarities and differences both technologies are utilized to achieve business requirements.

Email

Email is short for electronic mail, email or email is data put away on a PC that is traded between two clients over information transfers. All the more evidently, email is a message that may contain content, documents, pictures, or different connections sent through a system to a predefined individual or gathering of people. COMPUTERHOPE (n.d.) notes, the principal email was sent by Ray Tomlinson in 1971. By 1996, more electronic mail was being sent than postal mail.

Types of Email

There are basically three major types of email based on its contents. Marketing emails, Notification emails and Transaction emails.

Marketing email

Advertising (or Bulk) messages invigorate your customers and leads. They contain educational/motivation messages. The beneficiary must consent to get such messages: opt-in is mandatory.

Notification email

Notification email are otherwise called trigger, caution or automated assistant. They permit the client to be told every time a specific occasion happens (or has happened). All the for the most part, the notification email may utilized as a part of request to celebrate and/or mark an occasion.

Transaction email

This is a normal message and its substance is data that the customer wishes to check or affirm, and not "find". This kind of email is not proposed to improve the client relationship but rather to characterize it and mark it out.

Comparison of Email types

	Marketing *= Bulk*	**Notification** *= Trigger / Auto-responder / Alerts*	**Transactional**
Trigger	Sender	Sender or Recipient *Event scenario / System*	Recipient
Relation	One-to-many	One-to-one	One-to-one
Unsubscribe link	Yes	Yes	No

Figure 11 Comparison between email types (source: https://www.mailjet.com/docs/email_types)

Table above (figure 4) critically compare different types of emails. Marketing emails are triggered by sender where are transactional emails are triggered by receiver. Notification email are either triggered by sender of recipient. Similarly, marketing emails provides one-many relationship in which sender sends mail to many clients in bulk form whereas notification and transactional emails provides one-one relationship (MAILJET, n.d.). In such relationship sender sends particular email to one receiver only. Finally, marketing and notification emails are subscription based emails hence it consists of unsubscribe link allowing receiver to unsubscribe from receiving such emails whereas transactional emails does not have such links. All three types of mails are utilized for different purposes.

E-Commerce

Electronic trade or ecommerce is a term for a business, or business **exchange that** includes the exchange of data over the Internet. It covers a scope of diverse sorts of organizations, from shopper

based retail destinations, through closeout or music locales, to business trades exchanging products and administrations between companies. It is presently a standout amongst the most essential parts of the Internet to rise**,** writes NETWORKSOLUTIONS (n.d.). Ecommerce permits buyers to electronically trade merchandise and benefits without any hindrances of time or separate. Electronic trade has extended quickly in the course of recent years and is anticipated to proceed in light of current circumstances, or even quicken. Soon the limits in the middle of "ordinary" and "electronic" trade will turn out to be progressively obscured as more organizations move areas of their operations onto the Internet. According to export dot GOV (n.d.) there are basically three types of ecommerce sites available. Similarities and differences between these ecommerce services is compared below.

Transactional Site

Individuals who shop online are most acquainted with this kind of site. A value-based site may be an electronic storefront for a block and-mortar retailer or a list business, (e.g., Lands' End), or a maker showroom for those wishing to offer specifically to people in general (e.g., Dell Computer). Value-based destinations direct full "end-to-end" exchanges through the site, permitting clients to look for, request, and pay for items online and additionally permitting them to contact the organization for after-deals administration.

Information Delivery Site

This website creates deals by advancing corporate mindfulness as opposed to encouraging online exchanges. Its capacity is like a leaflet, giving data about the item or benefit and contact data on the best way to continue with a buy. Since this webpage is frequently static and doesn't require the product frameworks vital for online exchanges, it is less costly to plan and keep up than the value-based website.

E-marketplaces

These websites are business sector producers: they unite purchasers and dealers to encourage exchanges. Support in a business frequently gives an effective method for discovering a client without the cost of building an exclusive value-based site.

Comparison of ecommerce site types

All three types of sites provide ecommerce benefits. Major difference between these sites are transaction ability and structure. Information delivery site does not have transaction ability whereas other two ecommerce site types have such ability. All three types are utilized for different purposes.

Most of the information delivery sites are static whereas transactional and e-markets places are dynamic. Key differences and similarities are demonstrated in table below.

Component	Transactional	Information Delivery	E-marketplaces
Website type	Dynamic websites	Static/dynamic	Dynamic
Transaction	Yes	No	Yes
Information delivery	Yes	Yes	Yes

Certificate Services

Associations use certificates to improve security by tying the character of a man, gadget, or administration to a relating private key (Technet, n.d.). Be that as it may, with a specific end goal to understand the improved security made conceivable by endorsements, associations require a practical, proficient, secure approach to deal with the dispersion and utilization of testaments. Certificate Authority (CA) is an association that is trusted to sign computerized authentications. CA checks personality and authenticity of organization or person that asked for an endorsement and if the confirmation is effective, CA issues marked authentication, NAMECHEAP (n.d.). Contingent upon the usefulness that you require, the capacities of your IT foundation and IT managers, and the expenses that your association can bolster, you may construct your accreditation power base with respect to inside CAs, outsider CAs, or a mix of inner and outsider CAs. Internal CA and Third party (Outsider) CA is compared below.

Comparison of Internal and Third party CA

Internal CA enables corporate network to preserve control over security policies where are in third party CA less flexibility in management and configuration ability is provided.. Internal CA allows direct integration with active directory infrastructure. However, internal CA has to be organized and managed by organization themselves whereas third party CA are managed by professional experts. Deployment of Internal CAs can take longer than that of Third party CA, Microsoft (n.d.). On the other hand, Third party CA provides greater deal of confidence to clients due to their global popularity. However Third party CA are more expensive than internal CA.

Inter-Networking Servers

DHCP Server

DHCP stands for Dynamic Host configuration protocol and is utilized to assign IP address to resources/hosts on the network, COMPTECHDOC (n.d.). DHCP enables automatic IP distribution

based on predefined configuration to avoid complications. The fundamental target of DHCP is to give the programmed designation of IP customer setups for a sure timeframe and to abrogate the work important to control a vast IP system. This paper compares several DHCP provider such as Microsoft DHCP and ISC DHCP daemon.

DHCP Comparison

Comparison	ISC DHCP daemon (Linux)	Microsoft DHCP
Platform	Linux Based	This server is Microsoft platform oriented server.
Fee	Open source and Free	Requires Windows Server
Avoiding Duplicate Addresses	It checks IP address by pinging before trying to assign it to client	Simply uses its database to assign IP address
DHCP Failover	Supports draft DHCP failover protocol	Microsoft DHCP Server does not support failover
DNS Registration	DHCP server can register and remove client's IP from DNS	Client requires configured to register itself with DNS
Using Expressions	DHCP can configure name of host	Host name requires to be configured locally on client

Table above critically compares different type of DHCP (Linux based and Microsoft based). It is basic function of any type of DHCP to automatically allocate IP to host machines. Comparison table shows Linux based DHCP are free and open source while Microsoft based DHCP are not free. In fact, DHCP itself does not cost anything but to implement DHCP requires server version of windows (i.e. windows server 2008, windows server 2012 etc.) which costs money.

Both system has duplicate address avoiding mechanism but Linux based ISC DHCP daemon uses ping mechanism before assigning IP to ensure IP address is free. This process requires very small amount of more time than Microsoft DHCP but it guarantees non duplicate address. While Microsoft DHCP uses lease table database to provide IP address, it is very effective but Linux base system are more defined. One of the main differences between these two systems are ability to distribute machine name. While it is impossible to allocated machine from DHCP itself in Microsoft, ISC DHCP daemon is able to configure machine name centrally from DHCP. However, both system are effective way to provide DHCP service and should be utilized based on networking environment.

DNS Servers

Domain Name System, or DNS is a necessary piece of how resources associate with one another to impart on the web. Without DNS, PCs, and the general population who use them, would be required to interface utilizing just numerical locations known as IP address. Other than the undeniable issue of remembering a substantial number of complex numbers for basic communication, conveying through IP addresses likewise causes some extra issues, describes DIGITALOCEAN (n.d.). Moving site to an alternate facilitating supplier, or moving your servers to distinctive areas would oblige you to illuminate each customer of the new area.

DNS server, otherwise called a name server, is a inter-networking server that is particularly intended to associate with a monstrous database that stores all data about space names and their comparing DNS records. There are basically two types of DNS servers to support Internet services which are primary DNS and secondary DNS (also known as Master DNS and Slave DNS). This paper compares these two DNS while analyzing similarities and differences.

Comparison: Primary and Secondary DNS

The primary DNS server also referred as Master DNS server is read/write copy of DNS database. Whenever DNS server adds DNS records to its database, it is stored in Primary DNS. Database record can be added dynamically by DNS host machines or by administrators manually. According to TOMSHARDWARE (2013) one inter-networking environment can have only one primary DNS. Primary DNS is read/writable hence is placed in secure environment to project from physical as well as internal and external threat of network.

Secondary DNS or Slave DNS, unlike primary DNS is just read only copy of primary DNS records. Records in slave DNS cannot be modified by clients hence provides a layer of security to DNS system. An article in CCM (2015) suggests, Secondary DNS (Slaves) are utilized as backup mechanisms for primary DNS for critical situations. There can be a situation when connection with primary DNS cannot be established, in such condition, secondary DNS provides the naming services. Comparison between primary and secondary DNS is thoroughly demonstrated in table below:

Comparison Mean	**Primary DNS**	**Secondary DNS**
Referred as	Master	Slave

Number in a network	Only one in one inter-networking environment	Can be multiple number of secondary DNS
Database source	Master copy of DNS zones	Read only copy of primary DNS server database
Ability	Read and Write	Read only
Use in system	Store and update DNS records	Retrieve DNS record from primary DNS and provide fail save mechanism
Requirement	It is must to have primary DNS to provide DNS service	It is option to have secondary DNS (but important)
Security requirement	Is located in secured place	Utilized to provide security to primary DNS

Database Servers

A database server is dedicated computer in client-server model network for database system installation and storage. It consists of Database Management system. When host machines request something, database server searchers its database storage for the record and supply them to clients. Client can define and manipulate databases from web applications, desktop based application etc. However, PCMAG (n.d.) insists, database server can be part of file server to store non-database files. Though, term database server implies on system that provides database server services.

In bigger networking setup, the volume of exchanges may be such that one PC will be not able handle the heap. According to Technopedia (n.d.) for this situation, the database programming will dwell on a devoted PC, and the application on another. In this situation, there is a devoted database server, which is the mix of the equipment and programming, and a different committed application server. There are several types of database management system (DBMS) technologies that can be utilized in database server and are very popular due to their unique features. This paper compares three of the most popular database management system that is utilized in most of the database servers.

Comparison: RDMS technologies in database Servers

To start with Oracle upheld just fundamental SQL highlights, and it was composed in a low level assembly language. Now oracle has developed considerably and is a forefront in world of database management system. According to Lee (2013) Oracle Database 12c is the latest arrival of the RDBMS, and it incorporates the accompanying elements:

- New information redaction to improve security of critical information
- Presentation of Oracle Advanced Analytics stage
- Flash Data Archive (FDA) has new database handling
- Support for incorporating with working framework processor bunches
- Support for information pump for database union
- Permits clients to create Web applications utilizing SQL and/or PL/SQL.
- Propelled system compression to upgrade execution

Microsoft SQL server other hand is product of Microsoft for windows platform. Microsoft has endeavored to improve SQL Server to stay aware of evolving innovation. SQL Server 2005 is a case. The extensible Markup Language (XML) got stamp of endorsement from W3C and began making progress in the late 1990s. One of the major new components of SQL Server 2005 was backing for XML information. Other eminent elements of the lead item incorporate the presentation of SQL Server Always On (information administration innovation to diminishing client downtime), support for organized and semi-organized information, upgraded pressure, and a few additional items to bolster different items available. SQL Server 2012 was broadcasted as the last discharge to incorporate local backing for OLE.

Unlike MSSQL server and oracle, MySQL was not developed for commercial use and is an open source DBMS. Now MySQL also owned by oracle as it was brought by Sun Microsystem and them Sun Microsystem was brought by Oracle. Though it is still open source and free. Table below compares these three most popular DBMS that supports database servers.

Comparison Feature	**Oracle**	**MySQL**	**MSSQL Server**
Platform OS	Solaris, Linux, Windows, AIX etc.	Linux, Solaris, OS X, Windows	Windows
Licensing	Proprietary	Open Source	Proprietary
Price	Paid/Free version	Free	Paid/Free Version
Interface	GUI, SQL command	SQL command	GUI, SQL command
Supported Languages	C, C++, C#, Ruby, Java, Objective C etc.	C, C#, C++, Java, PHP, Ruby etc.	.Net, VB, Java, Ruby etc.

Various database management system to support database server in inter-networking server environment is critically compared in table above. MSSQL server is windows based database system whereas Oracle and MySQL support many OS platforms such as Linux, Solaris and

windows etc. While licensing of Oracle and MSSQL server is proprietary, MySQL is open source. Other key difference between these three DBSM is availability of interface, oracle and Microsoft SQL server offers GUI based system along with SQL while MySQL has SQL only. Though PHP provides PHPMYADMIN to allow use of MySQL in GUI interface. All three DBMS has their own features and should be utilized based requirement. Such as PHP based system provides incredible support for MySQL while .NET application supports MSSQL without any problem. Oracle is used in large enterprise network which has very large database.

Email Servers

To provide email service, email servers are required. Rouse (n.d.) explains a mail server (otherwise called a mail transfer agents or MTA, a mail transport operators, a mail switch or an Internet mailer) is an application that gets approaching email from nearby clients (individuals inside of the same space) and remote senders and advances cordial email for conveyance. A PC devoted to running such applications is likewise called a mail server. Microsoft Exchange, qmail, Exim and sendmail are among the more regular mail server programs. Two of the email servers Microsoft exchange and sendmail compared below.

Comparison: Microsoft Exchange and send mail

Comparison component	**Microsoft Exchange**	**Sendmail**
Licensing	Proprietary	Open source
Availability	Add-ones product for windows server	Included free with most of the
Interface	GUI	Command line
Platform	Windows	Linux/Unix
Ease	Easier to deploy and manage	Requires expert level knowledge while managing is easy
Extra features	Provides contacts, calendars etc.	Just email server

Table above demonstrates critical comparison between two of the popular email server options. Microsoft Exchange is owned by Microsoft and costs moneys while Sendmail is opensources and can be used for free. Other key difference is sendmail is command line based system where as exchange server provides GUI interface for ease of use. It is also worth mentioning that exchange only supports Microsoft windows whereas sendmail can be deployed in any Linux/Unix based server. Nonetheless, both system are Reliable, robust, stable in Intranet environment.

Conclusion

This paper has critically compared various internet services along with various inter-networking servers. Intranet service is compared with extranet service, in scenario of Kathmandu hospital, for now intranet can satisfy the business requirements. Though in future, organization may require extranet if they plans to expand their service and connect with partner organization's intranet. Organization right now does not requires to have transactional ecommerce site. Though they want to provide information about products and services they provide. Information delivery site is suitable for Kathmandu hospital to satisfy current need. In future, organization may want to sell their production online which will require transactional type of e-commerce hence, Internet server should be implemented to address these future needs.

This paper also differences between Microsoft based and Linux based DHCP. Selection of DHCP will be based on the platform organization choose. Existing systems in current network are Microsoft based hence moving to another Microsoft based system will reduce the cost of implementation. DHCP is a must for inter-networking environment. Various types of DNS shows how they complement each other, secondary DNS solely depends on records of primary DNS while it provides added layer of security. For now, only primary DNS can satisfy the requirement of hospital but to address future requirement secondary DNS is also recommend. Developed system will be able to publish PHP, Java, .Net based application hence necessary database server should also be installed to provide database service. Though Oracle is not necessarily required. MSSQL and MySQL implementation is recommended. And finally, various email servers to provide email services are compared. Current networking environment will not include email service as it is not requirement of the hospital but in future they may want to add email service to their network. Since, implemented system is based on Microsoft, Microsoft exchange is recommended, as going for free mail server will require whole network to be modified to Linux based system.

References

- Afriyie, B. S. (2012). Concise ICT fundamentals (volume one). Trafford Publishing
- CCM (2015) Primary DNS and Secondary DNS [Online] Available: http://ccm.net/faq/904-primary-dns-and-secondary-dns Accessed [10/13/2015]
- COMPTECHDOC (n.d.) DHCP [Online] Available: http://www.comptechdoc.org/independent/networking/guide/netdhcp.html Accessed [10/12/2015]
- COMPUTERHOPE (n.d.) E-mail [Online] Available: http://www.computerhope.com/jargon/e/email.htm Accessed [10/12/2015]
- Dellpe (2014) Cisco Network Technology [Online] Available: http://cisco2960.over-blog.com/2014/02/internet-intranet-and-extranet.html Accessed [10/12/2015]
- DIGITALOCEAN (n.d.) a Comparison of DNS Server Types: How to Choose the Right DNS Configuration [Online] Available: https://www.digitalocean.com/community/tutorials/a-comparison-of-dns-server-types-how-to-choose-the-right-dns-configuration Accessed [10/12/2015]
- Export dot GOV (n.d.) Types of E-Commerce Web Sites [Online] Available: http://www.export.gov/sellingonline/eg_main_020795.asp Accessed [10/12/2015]
- HYPEROFFICE (n.d.) Intranet vs. Extranet Disadvantages [Online] Available: http://www.hyperoffice.com/intranet-vs-extranet/ Accessed [10/12/2015]
- INTRANETEXTRANET (n.d.) Intranet and Extranet Advantages and Disadvantages [Online] Available: http://intranetextranet.blogspot.com/2012/12/intanet-and-extranet-advantages-and.html
- Lee (2013) Oracle vs. MySQL vs. SQL Server: A Comparison of Popular RDBMS [Online] Available: https://blog.udemy.com/oracle-vs-mysql-vs-sql-server/ Accessed [10/13/2015]
- MAILJET (n.d.) the difference types of Email [Online] Available: https://www.mailjet.com/docs/email_types Accessed [10/12/2015]
- Microsoft (n.d.) Selecting Internal CAs vs. Third-Party CAs [Online] Available: https://technet.microsoft.com/en-us/library/cc758439%28v=ws.10%29.aspx Accessed [10/12/2015]

- NAMECHEAP (n.d.) what is Certificate Authority (CA)? [Online] Available: https://www.namecheap.com/support/knowledgebase/article.aspx/334/38/what-is-certificate-authority-ca Accessed [10/12/2015]
- NETWORKSOLUTIONS (n.d.) what is Ecommerce? [Online] Available: http://www.networksolutions.com/education/what-is-ecommerce/ Accessed [10/12/2015]
- PCMAG (n.d.) database server [Online] Available: http://www.pcmag.com/encyclopedia/term/40885/database-server Accessed [10/13/2015]
- TechNet (n.d.) What Is Certificate Services? [Online] Available: https://technet.microsoft.com/en-us/library/cc779149%28v=ws.10%29.aspx Accessed [10/12/2015]
- Technopedia (n.d.) Database Server [Online] Available: https://www.techopedia.com/definition/441/database-server Accessed [10/13/2015]
- TOMSHARDWARE (2013) What Are the Primary and Secondary DNS Zones in DNS Server? http://www.tomshardware.com/faq/id-1932385/primary-secondary-dns-zones-dns-server.html Accessed [10/12/2015]
- Webopedia (n.d.) extranet [Online] Available: http://www.webopedia.com/TERM/E/extranet.html Accessed [10/12/2015]

Task3

Discuss network management concerns and make recommendations to sustain network security, reliability and performances [1.3]

Introduction

The network and internet services has turned into a business-basic resource for most companies. Dealing with various networking issues and preparing all-inclusive safety measurements essential part of inter-networking environment. There was a time when it was adequate to requires password from user accounts to provide reasonable defense barrier to critical data, no several tools and techniques are required to go against various network security issues. Network management also has to face service performance concerns, reliability of resources etc. This paper discusses some of the common network management concerns while making recommendations to provide sustainability to reliability, security and performance of the network.

Data and Resource Management

One of the key requirement of network management is efficient resource and data management. It has always been one of the main concern for administrator to manage resources securely and efficiently. To share data, people are require to use external storage and transfer data manually. Moreover, Computers requires access resources such as scanners, printers etc. Allocating resources for each computer can become very expensive. Hence, proper mean of sharing such resources and data is required. Instead of moving files using USB drive or disks, network allows quick and easy mechanism to share files.

With proper resource management, computers in network can share files far too easily. It also enables to access shared files/information/data easily reducing the time and cost of data transfer. Another benefit of proper data and resource management is convenient resource sharing. Shared resource can be both hardware and software. This helps to reduce the operational cost significantly by sharing available scanner, printers etc. and helps to improve productivity of the organization. Another example of resource sharing is computers sharing from one high bandwidth internet connection rather than establishing small connection for all computers. A big concern in resource management is chances of data loss, data corruption and unreliable resource access if proper resource management is not provided. Network management has to ensure secure and reliable sharing of data and resources. While managing a network, proper planning and monitoring of resources and data sharing plan is required. While sharing information, management should allow to set security measurement on the share data.

User and group management

Another fragment of network management is management of user access. Users can be computer, or a person with user account in network environment access network resources and information. Network administrator has to prepare proper access plan to allow or deny users from using resources. Privilege and access right should be planned for each users and groups to ensure data/resource security. User and group management includes planning and enforcement of various rules to specify what a user/group can do and cannot do. Access time and privilege level of a user is maintained via user and group management. To properly maintain user accounts, similar accounts can be made associated with groups. For example, all accounts of students from IT can be associated with single group IT_STUDENTS. This helps to set and modify various policies for each users via single group instead of applying rules to each users.

Security Management

One of the biggest concern of the network management is security management. With advancement in technology, each day new tool or techniques is developed to harm a network. Ensuring security of resources is most critical task in any network. System Security is an association's methodology and procurements for guaranteeing the security of its data and resources. Security management includes planning, implementation and management of proper security policies, software tools and hardware resources. Network administrator analyzes the security requirement of a network and implement security measurements. Security management has to ensure access to any critical network resource/data requires proper authentication and authorization. It is also must to ensure all critical data should be transferred using secure/encrypted path only. While maintaining the security measurements, user's satisfactory access to shared data/resources should be ensured to achieve business requirements. Security management is not only deal with implementation of security policies but also includes monitoring and troubleshooting of identified security issues. Some of the top network attack includes brute force attack, denial of service, browser attack etc. are discussed below.

Brute force attack is basically a network attack in which combination of username and password is attempted hundreds and thousands of times to gain access to the system. It's a trial and error method utilized to guess the password. Another network attack type is denial of service. This sort of attack is done to prevent organization from providing services to clients. Also known as DOS, common DOS method is overloading the resource with illegitimate requests for service. So that resource cannot handle the requests and becomes unworkable. Browser attack is another attack that

is utilized targeting users that uses web browser, enforcing them unwillingly download malicious files and damage the network. Proper security management is required to prevent these security concerns.

Recommendation

This paper has discussed various network management concerns. To address these concerns following recommendations are provided:

Client Server Environment

Client server environment is sort of network architecture in which resources behaves as service consumer (clients) and service provider (server). At least one particular computer requires to serve as server in such environment. One of the key benefits of client server environment is it provides centralized mechanism for user and group management, security management and data/resource management. Server can centrally manage shared data, shared application and resources. Implementation of proper client server network model provides following benefits to overcome various network management concerns:

1. Centralized management of shared information and resources
2. Implement security policies centrally
3. Provide central user account storage allowing users to use any computer in network
4. Plan and implement user privilege and access rights centrally via user management and group policy
5. Maintain security of data by encrypting the path
6. Allows to set account lock down rule to prevent brute force attack.
7. Allows to centrally monitor resources, hosts, and applications to provide easy maintenance which improves reliability and performance of the system

Security tools

While addressing security concerns of a network, implementation of security policies are not enough. There are various software and hardware based tools and technology available to improve security of network. Implementation of proper Anti-virus application is essential for network security. It regularly scans storage and prevents viruses, malwares and adware in the system. Additionally, it is recommended to use proper firewall device to filter inbound and outbound packets to ensure network safety.

Task4

Critically Analyze different internet server technologies and their performance. [2.1]

Introduction

Internet server technologies includes web servers which is a computer or grouping of computer connected via LAN or internet to satisfy client's requirements through web agents (browser). It is basically a large storehouse of web pages which transfers to clients up on their request. Internet server technologies utilizes several internet and communication protocols such as HTTP, SMTP, FTP etc. for different purposes. Each server has their own unique IP address along with domain name which enables them to be recognized in networking environment.

This paper critically analyzes various internet server technologies and their performance while discussing their interrelationship. There are several types of web server technologies are available in market from different manufacturer. Two of the most popular web server technologies are analyzed below.

IIS

Internet Information Server (IIS) is a standout amongst the most well-known web servers from Microsoft that is utilized to provide Internet-based administrations to ASP.NET and ASP based Web applications. IIS (Internet Information Server) is a gathering of Internet servers (counting a Web or Hypertext Transfer Protocol server and a File Transfer Protocol server) with extra capacities for Microsoft's Windows NT and Windows 2000 Server working frameworks. When a request arrives from client, web server is in control for providing response. Web Information Server (IIS) has its own ASP.NET Process Engine to handle the ASP.NET request.

Basic Functionalities

Internet Information Server (IIS) consists of fundamental functionality of to enable implementation of websites and web applications. IIS includes core functionality of web application deployment and administration as well as other support for IIS services. IIS web servers store websites, web application and location for database servers for instance SQL server. IIS allows to take benefits of HTTP, HTTPS, FTP, and SMTP based services. Some of the core functionalities of IIS is discussed below.

- **Server Configuration**: IIS enables administrators with ability to deploy HTTP and FTP based websites as well as ability to manage them. IIS also allows to set security measurements such as allowing or denying users from accessing files, websites, application

- **Content Development: IIS web server** allows web developers to program HTML website, ASP.net or ASP or PHP based web application or an extension mapped with DLL in server to listen to clients request and provide necessary response. It also allows to program secure ISAPI (Internet Server Application Programming Interface) filter to improve security as it is first mechanism to process client's requests.
- **Internal Support for IIS Services: IIS webservers** enables to establish and maintain HTTP connection, provide HTTP response to client's request. Instance of the ASP and ASP.NET integral objects is generated with accessible data from each HTTP request, such as client certificate information, error information and session state information.

Web and Application Services

IIS web server provides support for both static as well as dynamic websites deployment. Dynamic websites are also known as web application. A developer utilizes tools like front page or Dreamweaver to create website using HTML, CSS, and JavaScript. They also uses server side scripting languages such as Active server Page (ASP) or PHP to develop dynamic application. Figure 1 demonstrates, client request web server via HTTP to get web pages. Which web server transfers to client as HTTP response. If website is static, files are transferred "as it is". Files stored in webserver are transferred to browser of client without any modification. Whereas if website dynamic shown in figure 2, webserver does not stores webpage itself, it has to generate webpages up on request from clients which client can view via web browser. Though IIS support asp based application and PHP based application, ASP programs run more efficiently than common gateway interface (CGI).

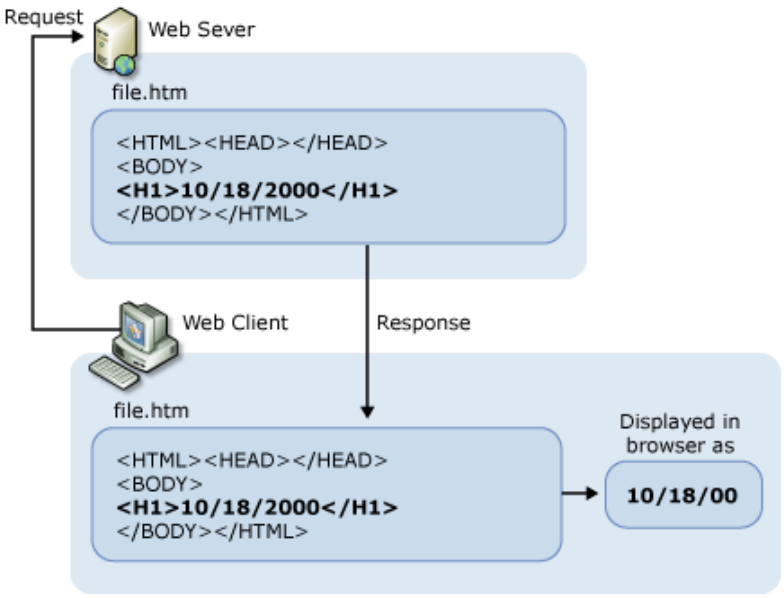


Figure 12 HTTP request in IIS (source: Microsoft.com)

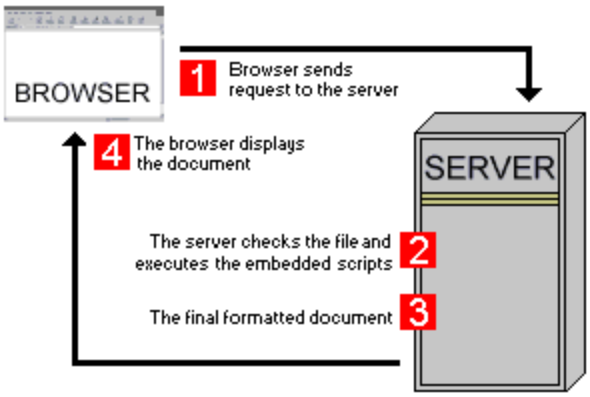


Figure 13 Web application Service by web server (Source: http://www.webdevelopersnotes.com)

FTP Server

One of the other services provided by IIS is its support for FTP sites. FTP is an acronym for File Transfer Protocol. As the name proposes, FTP is utilized to exchange documents between PCs on a system. We can utilize FTP to trade records between PC accounts, exchange documents between a record and a desktop PC, or access online programming records. Unlike network file sharing, FTP allows to share file via web browser. IIS allows to create FTP site and publish them. IIS also allows to enable security options to provide security measurements. Unlike web hosting using HTTP, FTP site uses FTP protocol which is suitable for transferring larger files than HTTP.

Apache web server

Apache web server is also referred as “Apache” and is an open source web server. This is the most prominent web server on the planet created by the Apache Software Foundation. Apache web server is an open source programming and can be introduced on every single operating system framework including Linux, UNIX, Windows, FreeBSD, Mac OS X and that's only the tip of the iceberg. Around 60% of the web server machines run the Apache Web Server.

The Apache server is a product (or program) that keeps running in background under a proper operating framework, which underpins multi-tasking, and gives administrations to different applications that join with it, for example, browser. It was initially created to work with Linux/Unix w, however was later adjusted to work under different frameworks, including Windows and Mac. The apache web server gives a full scope of web server highlights, including CGI, SSL and virtual area. The Apache server structural engineering is made out of a core that actualizes the most essential usefulness of a web server and an arrangement of standard modules that really benefit the

periods of taking care of an HTTP request. Various core functionalities of Apache web server are discussed below.

Modular

Apache server is developed in modular architecture which allows to enable or disable different modules of server to add or remove web services. This allows to improvise security, performance and service ranges. Apache also support third party modules to extend web services.

Multitasking/Multithreading

Apache server supports and response to multiple HTTP request from client at single time. This is achieved by running multiple threads of execution. New thread is created by Apache server for each of the HTTP request. This handles and returns request page to clients as shown in figure 3. This allows apache to response to multiple clients and run multiple application at same time.

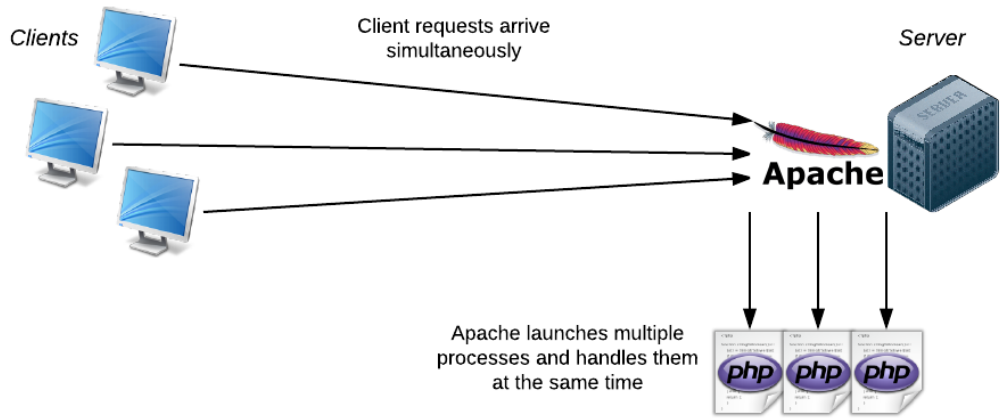


Figure 14 Apache HTTP request Handling (Source: https://sdz-upload.s3.amazonaws.com)

Support for CGI Scripting

Apache server allows to deploy web application developed using server side scripting languages such as PHP, PERL and Python etc. Though ASP programs are supported using Mono project it still has performance and security issues as it's still under development technology.

Security

Apache server provides modules to support deploy authentication, SSL and access control which enables administrator to enhance security of the application/website.

Performance and scalability

Apache allows administrator to distribute apache processes among various web servers for load balancing and enhancing performance of the webserver. Additionally, Apache can compress document before transferring them to client which helps to reduce bandwidth consumption and improve performance.

Summary

This paper has critically analyzed various internet server technologies and their performance. Two of the top internet servers are Apache and IIS. Webservers comes as part of large package of intranet and internet related application for serving FTP download requests, web browsing requests, serving email service etc. Choosing a webs server is based on the platform environment of the network. Microsoft based environment supports IIS web server and can be added as a role. While apache server can support multiple platforms. It organization requires to support .NET application IIS is better suited. While apache provides better support for PHP based application. For current system IIS web server is recommended. Various servicers such as FTP, email, website hosting and web application hosting are interrelated as it can be achieved only via proper implementation of IIS web server in implemented network.

Task5

Explain the hardware and software component of an internet server. [2.2, D3]

Introduction

Implementation of any inter-networking environment requires right combination of hardware and software to achieve business requirement and provide optimal service quality. This document explains various software and hardware component required to build optimal solution for Kathmandu hospital along with their price and features. This report will work supporting document while producing system specification of the system to satisfy business requirements.

Hardware Component

Planned Internet server consists of two dedicated servers; one as domain controller and DNS server and other as webserver (IIS). Hardware requirement for each server is explained below.

Internal Hardware

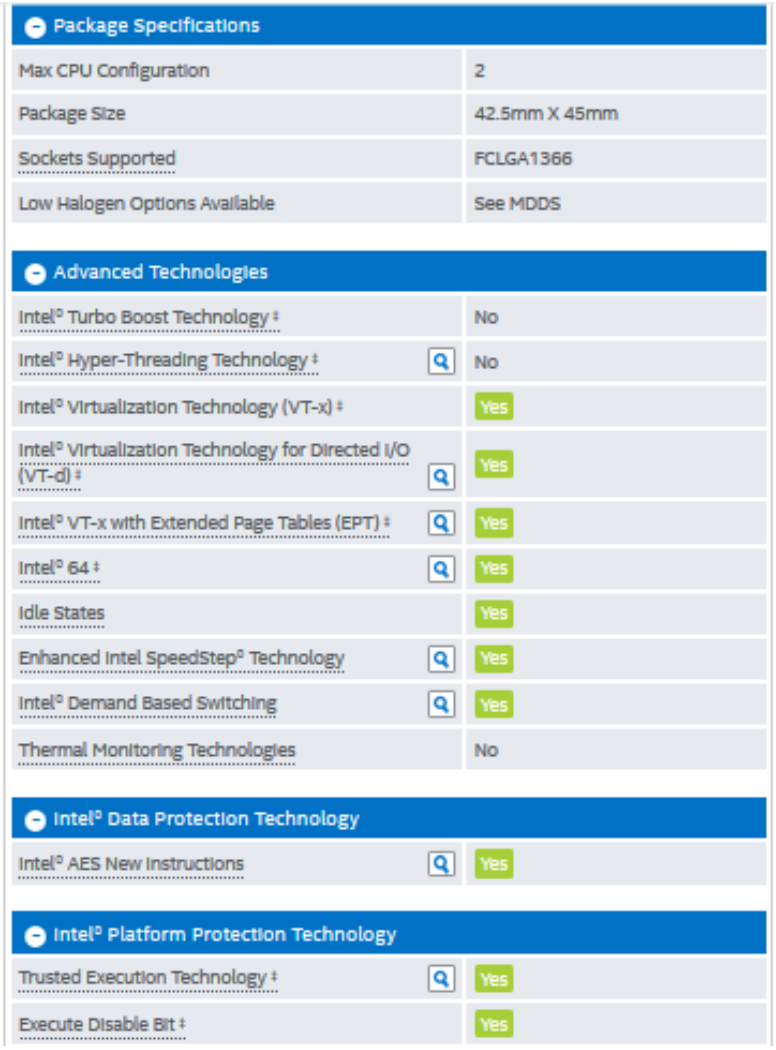
CPU

The Central processing unit (CPU) of a PC is a bit of equipment that does the directions of a PC program. It performs the essential arithmetical, legitimate, and enter/yield operations of a PC framework. CPU is most critical component of any computing system. It is brain of the system where most of the calculation takes place. The CPU itself is an interior segment of the PC (Webopedia,). Present day CPUs are little and square and contain different metallic connectors or pins on the underside. The CPU is embedded straightforwardly into a CPU attachment, pin side down, on the motherboard. There are many powerful CPUs are available in the market. Minimum requirement for windows server 2008 is 1 GHz processor while 2 GHz is recommended. This paper provides suggestion for choosing appropriate CPU for the inter-server.

Suggestion

According to Intel (n.d.) the **Intel® Xeon® Processor E5607** processor conveys noteworthy execution - up to 4 times that of prior era single-center processors. Each of the centers has a L1 and L2 store, and an extra 8MB of shared L3 reserve; this lets the Xeon E5607 handle overwhelming burdens and expansive information sets. The 64bit centers are intended to handle the greater part of today's x86 32bit programming easily, and can easily relocate to 64bit application. This processor is **priced** at **NRS 30,000** and offers advanced features such as virtualization, Data protection, enhanced intel SpeedStep technology etc. Features of this processing unit from Intel is provided below.

Features



Package Specifications	
Max CPU Configuration	2
Package Size	42.5mm X 45mm
Sockets Supported	FCLGA1366
Low Halogen Options Available	See MDDS
Advanced Technologies	
Intel® Turbo Boost Technology ‡	No
Intel® Hyper-Threading Technology ‡	No
Intel® Virtualization Technology (VT-x) ‡	Yes
Intel® Virtualization Technology for Directed I/O (VT-d) ‡	Yes
Intel® VT-x with Extended Page Tables (EPT) ‡	Yes
Intel® 64 ‡	Yes
Idle States	Yes
Enhanced Intel SpeedStep® Technology	Yes
Intel® Demand Based Switching	Yes
Thermal Monitoring Technologies	No
Intel® Data Protection Technology	
Intel® AES New Instructions	Yes
Intel® Platform Protection Technology	
Trusted Execution Technology ‡	Yes
Execute Disable Bit ‡	Yes

Figure 15 Intel Xeon 5607 CPU specification

Alternative

Alternatively for a smaller network like Kathmandu hospital, **Intel® Core™ i5-4440S** CPU can be utilized. Though it is not meant to be used in server computer, specification shows it can handle system load. This processor is cheaper than Xeon CPU and **priced at NRS. 20000**. This processor is easily available in local market though it does not provide optimal performance compared to Xeon processor. These two processor are not supported by same motherboard and usually, motherboard for Xeon CPU has more features such as support for more RAM. This CPU provides 6 MB of cache compared to 8 MB of Xeon's processor. It provides 2.8 GHz base frequency which can be further maxed to 3.3 GHz using turbo technology. Other features includes thermal monitoring, virtualization and OS guard etc. It is still recommended to use the Intel® Xeon®

Processor E5607 processor though if that is not possible due to availability or price, Intel® Core™ i5-4440S should be implemented.

Motherboard

The part of the motherboard is to permit every one of these segments to correspond with one another. Considering the way that the various parts are introduced on the motherboard or joined with it, it is sheltered to say that the motherboard is the focal bit of a PC, the segment that unites it all. Appropriate motherboard for internet server is suggested below.

Suggestion

According to Intel (n.d.) **Intel® Server Board S5500HCV** is a compatible motherboard solution for suggest Xeon® Processor E5607 while it developed by Intel **targeting small and medium business.** For a medium size business like Kathmandu hospital this motherboard is appropriate. It is priced around NRs. 35,000. It is a platform streamlined server board with big business –class execution and adaptable administration for little and medium business application. It supports DDR3 RAM and has features like RAID support, 2 1GbE Ethernet, support for two CPU etc.

Alternative

If instead of CPU Xeon® Processor E5607, Intel® Core™ i5-4440S is selected then above suggested motherboard is not supported. Alternatively, **Intel® H81 Chipset** suggested which is priced around just **NRs.5000**. It has features such as support for USB 3.0 and 2.0, 8 USB 2.0 and 2 USB 3.0, 4 SATA PORT, smart card connect technology, and anti-theft technology etc.

RAM

RAM (Random access memory) is the component of a PC where the working framework, application programs, and information in current use are kept with the goal that they can be immediately come to by the PC's processor (TECHTARGET, n.d.). RAM is much quicker to peruse from and compose to than alternate sorts of capacity in a PC, the hard disk and CD-ROM. For an Internet support appropriate amount of RAM is suggested below.

Suggestion

Kingston DDR3 4 GB RAM is suggested for given environment. Have 4 GB of RAM in server would allow to provide optimal performance. DDR3 is selected as it is supported by motherboard and CPU. This RAM card is priced at NRs. 3000 and has memory clock of 1333 MHz, It is tested thoroughly ensuring efficiency and superior speed.

Alternative

TechNet (n.d.) suggest minimum requirement for windows server 2008 is only 512 GB of RAM, however it is recommended to have 2 GB for better performance. Hence Kingston 2 GB DDR3 RAM is alternatively suggested. This RAM card is priced around **NRs. 2000.**

Internal Storage

Internal storage such hard disk is utilized to install operating system and store documents. Inner capacity permits the information and applications to be stacked quickly into memory, prepared for use explains TEACH-ICT (n.d.). The information can be access much quicker than information which is put away on an outside capacity gadget. This is on account of inner stockpiling gadgets are joined specifically to the motherboard and its information transport while outside gadgets are associated through an equipment interface, for example, USB, which implies they are significantly slower to get to.

Suggestion

Minimum storage requirement for windows server is 10 GB and 40 GB is recommended. For planned internet server, it will contain personal documents, database, websites, web applications etc. To improve ability to store large amount of data **WD Blue 1TB Desktop** Hard Disk Drive is suggest. Priced around **NRs. 5000** only this hard disk demonstrates features like SATA 6.0Gb/s interface, 64 MB cache, improvement in PC performance, data lifeguard etc.

Alternative

Alternatively, WD Blue 500 GB Desktop Hard Disk Drive is suggested but more hard disks will require when 500 GB fills up. This hard disk is priced around NRs. 4000. It offers SATA 6.0Gb/s ad 16 MB of cache. But, with only NRs. 1000 more 1 TB hard disk offer double size of storage space and 4X times cache size.

Network Adapter

To associate with a system, a PC uses a system interface card (NIC). A NIC controls the wired and remote associations of a PC to trade data with different PCs and the Internet. A PC uses a system interface card (NIC) to wind up a portion of a system. The NIC contains the electronic hardware required to convey utilizing a wired association (e.g., Ethernet) or a remote association (e.g., WiFi). A system interface card is otherwise called a network connector, system interface controller, or Local Area Network (LAN) connector. Network card is integrated with both of the suggested motherboards. Though additional NIC card can be added to system on requirement via PCI express

slot. **TP-LINK TG-3468** Network Adapter is suggested if system requires additional NIC port. It is priced around **NRs. 1000** and has features of 10/ 100/ 1000Mbps and supports 1 RJ45.

External Hardware

External Storage

External storage allows portable solution for storage. It is connected to computer via USB port. For planned system **WD - My Passport Ultra 1TB** suggested. This external storage is prices at NRs. 5000 and can be utilized for backup solution. It supports USB 3.0, USB 2.0 interface and provides maximum speed of 625 megabyte per second.

Other Hardware Requirements

To install and manage internet server components, Keyboard and Microsoft Mouse or compatible pointing device and **DVD ROM drive** will be required**.**

Software Components

Operating System

The operating system (now and again alluded to by its shortened form OS), is in charge of making the connection between the material assets, the client and the applications (word processor, computer game, and so on.). At the point when a project needs to get to a material asset, it doesn't have to send particular data to the fringe gadget however it just sends the data to the OS, which passes on it to the applicable fringe through its driver. Operating system handles management of not limited to processor, RAM, input/output (I/O), application execution, files, information and authorization etc. OS for the internet-server and alternative solution is provided below.

Suggestion

Windows Server 2008 R2 is suggest OS for the planned Internet server. System would require two copy of server. One for domain controller and another for web server. System would require additional copy server if dedicated database server is installed. This OS is priced around NRs. 20,000 and can be purchased from eBay. Though various edition of sever 2008 R2 is available such as web, standard, enterprise etc. standard edition is suggested due to its features. Features in **Windows Server 2008 R2** that will be utilized in Internet server and support networking environment:

1. Group Policy Management
2. Active Directory
3. IIS

4. .NET Framework 3.5.1
5. SMTP
6. Server Backup
7. DNS
8. DHCP
9. Application Server
10. Remote desktop

Alternative

CentOS offers clients a noteworthy cluster of devices that framework overseers can use to screen every one of the stations associated with the system, and a great deal more. The OS is **free** for anybody to utilize and it has been produced on top of the Linux RedHat Server OS. The establishment procedure is extremely straightforward and as a result of its base in Linux programming, it needs less upkeep than a Windows Server would require. The item is created to help little organizations yet it can likewise take a shot at a home system that uses document sharing, media gushing and more PCs associated with one system. Likewise, CentOS offers support for email portals and can be effectively overhauled. The designers offer backing and redesigns for every variant of CentOS for a long time after the discharge.

Future requirements

This paper has suggested appropriate hardware and software solution for the internet server. Paper has also provided alternative solutions while planning system specification along with price. To provide scalability and enhanced performance system would require following components in future to satisfy business requirements

RAID Controller

A RAID controller is an equipment gadget or programming program used to oversee hard disk drives (HDDs) or strong state drives (SSDs) in a PC or capacity exhibit so they fill in as a logical unit. A controller provides a level of abstraction between a working framework and the physical drives. Rouse (n.d.) writes, a RAID controller presents gatherings to applications and working frameworks as legitimate units for which information assurance plans can be characterized. Since the controller can get to various duplicates of information on numerous physical gadgets, it can enhance execution and ensure information safety in the case of a framework crash. Average quality RAID controllers are easily available in market for price around **NRs. 20000.**

Recommendation

It is recommended to utilize virtualization technology to reduce cost of the system. **Microsoft® Hyper-V™ Server 2008 R2** is a stand-alone item that gives a solid and advanced virtualization arrangement empowering associations to enhance server usage and lessen costs. With the expansion of new elements, for example, live movement and extended processor and memory support for host frameworks, it permits associations to solidify workloads onto a solitary physical server and is a decent answer for associations who are combining servers and also for advancement and test situations. By being able to connect to existing IT frameworks Microsoft Hyper-V Server 2008 R2 empowers organizations to lessen costs, enhance use and procurement new servers. It permits IT experts to influence existing fixing, provisioning, administration and support devices and systems. This virtualization system is available to download form Microsoft download center for free.

References

- Intel (n.d.) *Intel DH82H81* [Online] Available: http://ark.intel.com/products/75016/Intel-DH82H81-PCH Accessed [10/15/2015]
- Intel (n.d.) *Intel Xeon Processor E5607* [Online] Available: http://ark.intel.com/products/52582/Intel-Xeon-Processor-E5607-8M-Cache-2_26-GHz-4_80-GTs-Intel-QPI
- Rouse (n.d.) *Raid Control* [Online] Available: http://searchstorage.techtarget.com/definition/RAID-controller Accessed [10/16/2015]
- TEACH-ICT (n.d.) *Storage Devices* [Online] Available: http://www.teach-ict.com/gcse_new/computer%20systems/storage_devices/miniweb/pg3.htm Accessed [10/16/2015]
- TechNet (n.d.) *Requirement of Windows Server 2008*[Online] Available: https://technet.microsoft.com/en-us/library/cc731400.aspx Accessed [10/16/2015]
- TECHTARGET (n.d.) *Random Access Memory* [Online] Available: http://searchstorage.techtarget.com/definition/RAM-random-access-memory Accessed [10/15/2015]
- Webopedia (n.d.) *Central Processing Unit* [Online] Available: http://www.webopedia.com/TERM/C/CPU.html Accessed [10/15/2015]

Task6

Produce a system specification to meet a given requirement and evaluate the suitability of internet server component. [3.1, 3.2]

Introduction

To build internet server and manage Internet services system specification plan is required to be prepared. Such specification should provide optimal performance. Prepared specification plan is provided below in terms of specification table.

Hardware Specification

S.N.	Component	Description	Price [in NRs.]	Remarks
1.	CPU	Intel® Xeon® Processor E5607	30,000	
2.	Motherboard	Intel® Server Board S5500HCV	35,000	
3.	RAM	Kingston 4 GB RB*2	3,000*2=6,000	DDR3
4.	Internal Hard Disk	WD Blue Desktop	5,000	1 TB
5.	Keyboard + Mouse	LG wired	1,500	USB
7.	External Hard Disk	WD - My Passport Ultra	5,000	1 TB
9.	Casing + Power	Intel SC5650DP 600 W	35,000	600 Watt
10.	Extra NIC	TP-LINK TG-3468	1,000	RJ45
		Total		**1,18,500**

Table 1 Hardware System Specification

Software Specification

S.N.	Component	Description	Price	Remarks
1.	Operating System	Windows Server 2008 R2	20,000	Volume License Available
2.	Anti-virus/Firewall	Avira Server security	40,000	Trial Available
4.	Virtual Machine	Hyper-V 2008 R2	Free	

Table 2 Software System Specification

Server Roles Specification

S.N.	Component	Description
1.	Domain Controller	Domain control will be installed in windows server 2008
2.	DNS	To provide DNS service DNS role will be added in Domain computer

3.	Web server	To provide web services IIS server role will be added in dedicated server computer and member of domain

Table 3 Required Server Components

Suitability Evaluation

Hardware and software specification above is based on the previous paper which is based on proper research. Each components are identified using proper research and is appropriate for planned Internet server. Intel® Xeon® Processor E5607 enables server to load large number of services with each. It is planned that instead of managing two different servers, virtualization will be utilized to create two servers. Intel® Xeon® Processor E5607 will allow to support each virtual computers. Selection of Intel® Server Board S5500HCV motherboard is based on selection of the CPU above. Intel® Server Board S5500HCV supports selected CPU and have additional CPU slot if organization wanted to upgrade their processing capacity and provide dedicated CPU for each of two virtual computer. It is recommended to have 2 GB of RAM for server, however price of RAM is not that high and having 4 GB of RAM will certainly improve performance and provide administrator flexibility while running various application. Hence 4 GB RAM is selected, two 4 GB RAM will be required for each of the virtual computers. Having 1 TB of internal storage is enough for each virtual server computers to install OS, store documents and websites. Other hardware components are chosen based on their price and support for other selected components.

Windows server 2008 R2 is selected as OS due to its ease in management and deployment as well as its support for web applications, web sites, email, security features, FTP site hosting and other features such as access control, firewall, active directory etc. Two server system is required for the system as mentioned above. One for domain controller and other for IIS web server, to create virtual system, Hyper-V windows server 2008 is selected which is available for free and manufactured and supported by Microsoft.

Task7

Build and configure an internet server including services to meet a given requirement.[3.3]

Introduction

This paper documents building and configuration of various internet server technologies as well as server technologies that supports network infrastructure. To establish networking environment for Kathmandu Hospital Pvt. Ltd. Domain controller, Domain name server, IIS server (Web server) in FTP server is implemented and documented in this report.

Static IP Configuration

To setup network environment and configure various Internet server technologies static IP allocation technique is utilized. For static IP configuration, following procedures are practiced:

1. Go to RUN by pressing WIN + R key (Image 1)
2. Right click on Network adapter and left click properties(Image 2)
3. In the Networking Tab click on Internet Protocol Version 4 (TCP/IP4) (Image 3)
4. Click on properties
5. In the General Tab click on Use the following IP addresses
6. Provide valid IP address, Subnet mask, gateway address (Image 4)
7. Click on Use the following DNS server address
8. Provide valid DNS server IP address
9. Click on OK
10. Click OK again to complete the procedure

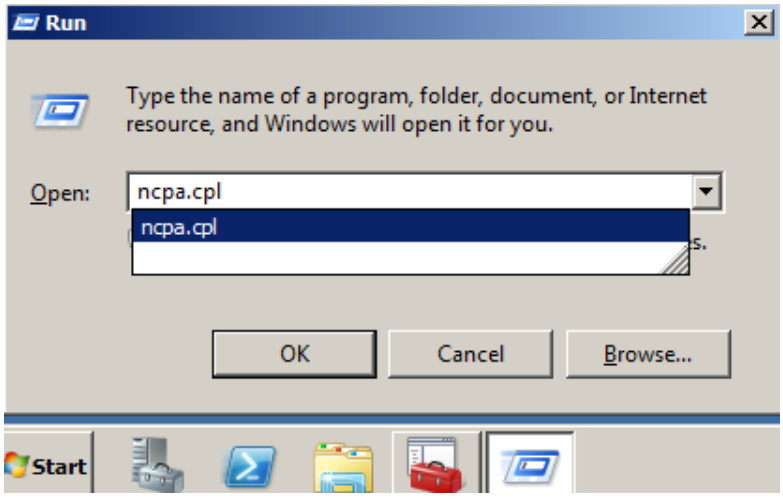


Image 1 Static IP configuration Procedure

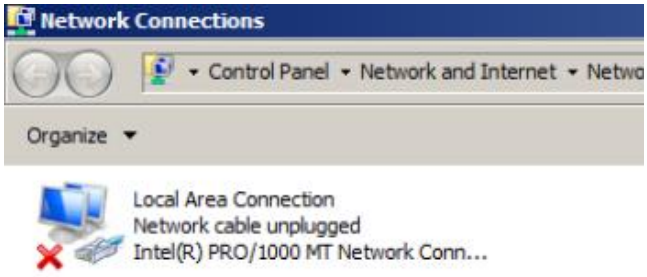


Image 2 Static IP configuration Procedure

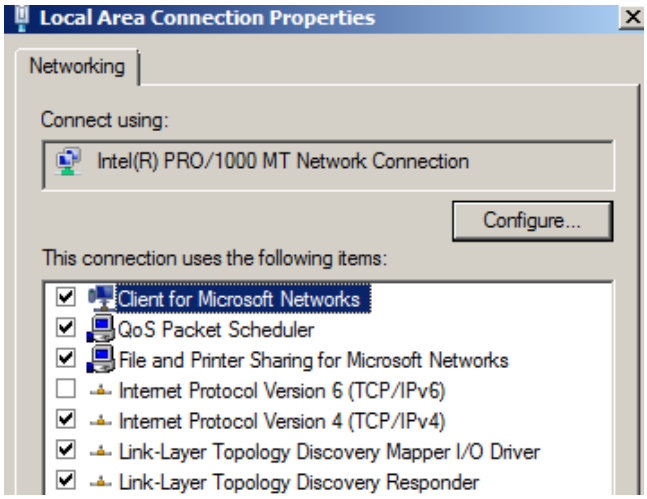


Image 3 Static IP configuration Procedure

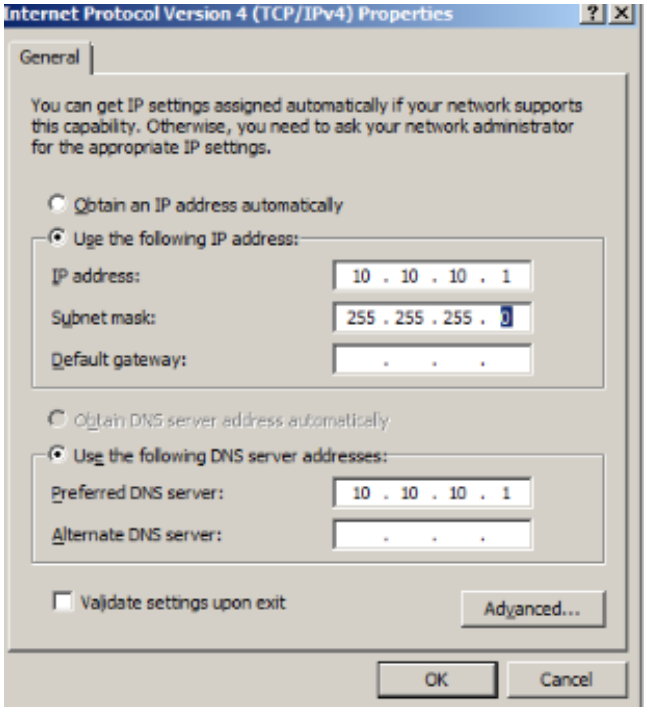


Image 4 Static IP configuration Procedure

Domain Controller and DNS Setup

To support network infrastructure and provide centralized management, Domain controller server is installed. DNS is also installed during setup of active directory. For DC Active Directory and DNS configure procedure practiced are as follows.

1. Set Static IP address 10.10.10.1 and subnet 255.255.255.0
2. Press WIN + R → RUN (Image 5)
3. Type in **DCPROMO**
4. Once Active Directory Domain Service Installation Wizard loads (Image 6)
5. Click Next→Click Next
6. Choose Create new domain in new forest (Image 7)
7. Type in Fully Qualified Domain Name→ Kathhospital.com→Click Next (Image 8)
8. Choose forest function level→ windows server 2008→click Next (Image 9)
9. Choose domain function level→ windows server 2008→click Next
10. Put Check on DNS for future requirements→ click Next(Image 10)
11. Leave all fields value to default→ click Next
12. Click Next
13. Provide directory services restore password (Image 11)
14. Click on Next (Image 12)
15. Let the process finish→Restart the system→ Done
16. (Optional tick on reboot on completion to reboot system after installation automatically) (Image 13)

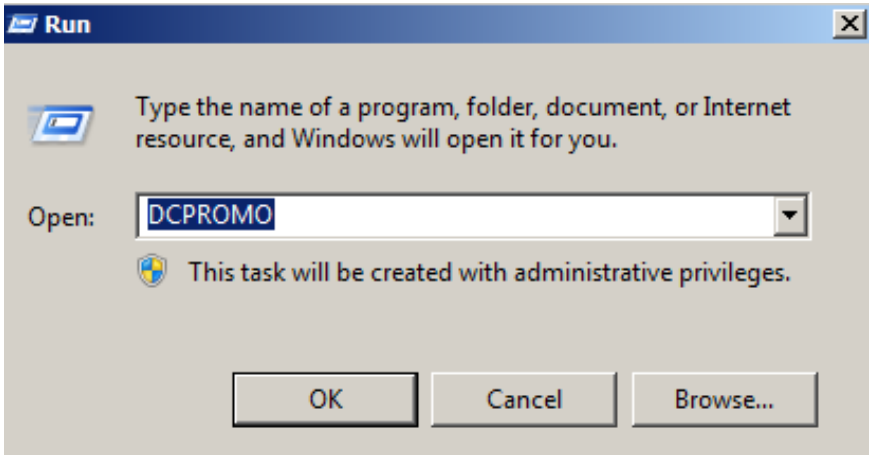


Image 5 DC and DNS Setup procedure

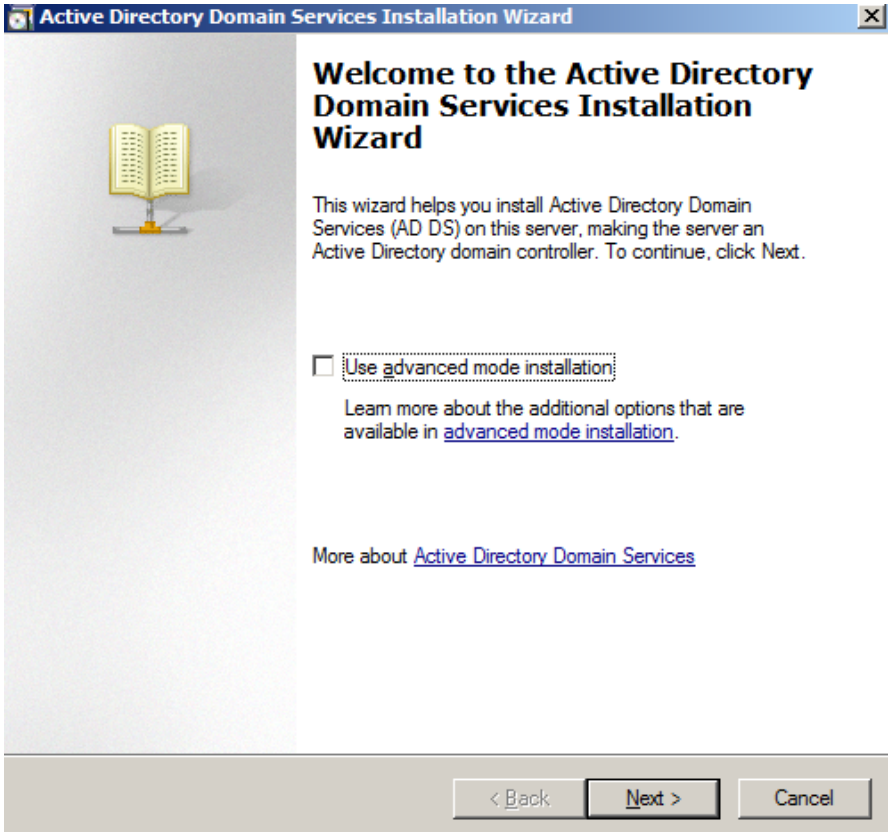


Image 6 DC and DNS Setup procedure

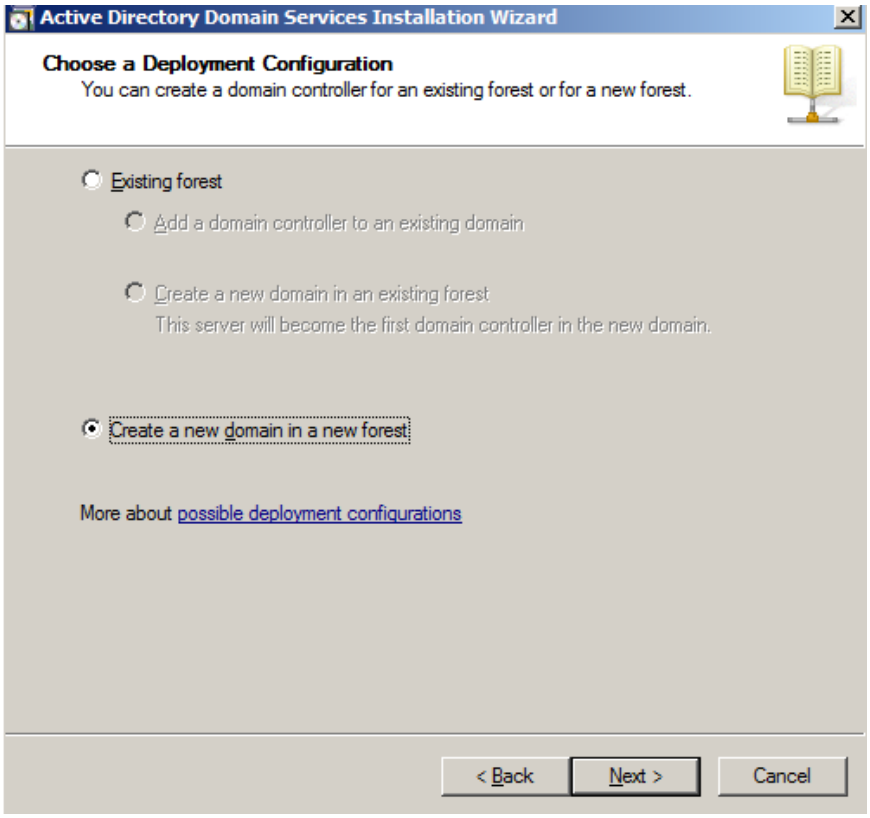


Image 7 DC and DNS Setup procedure

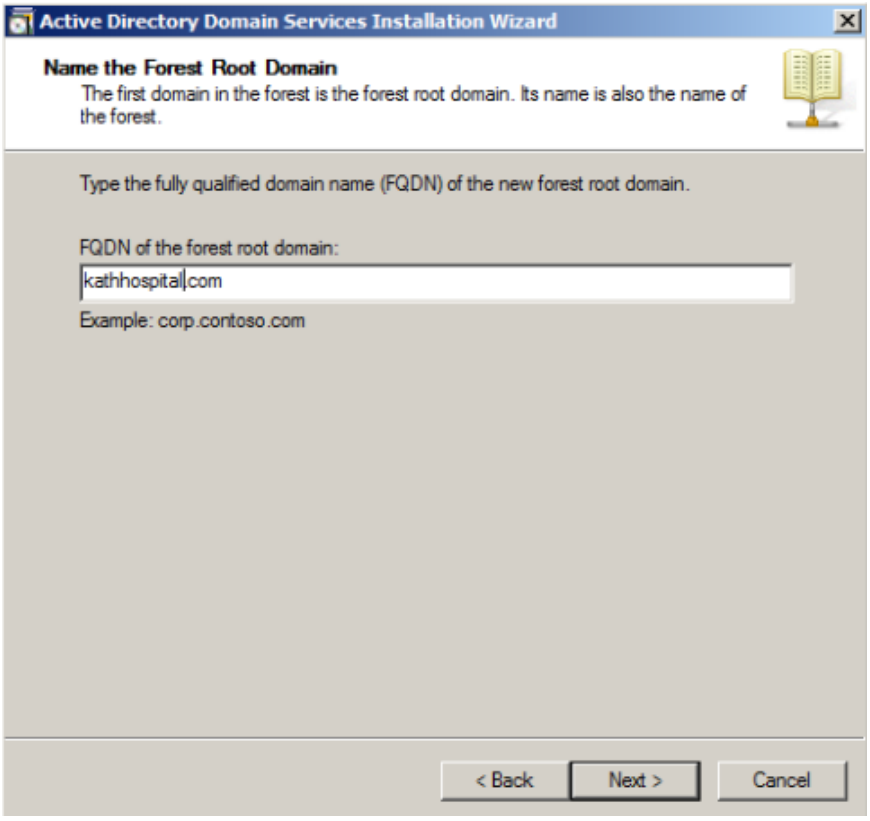


Image 8 DC and DNS Setup procedure

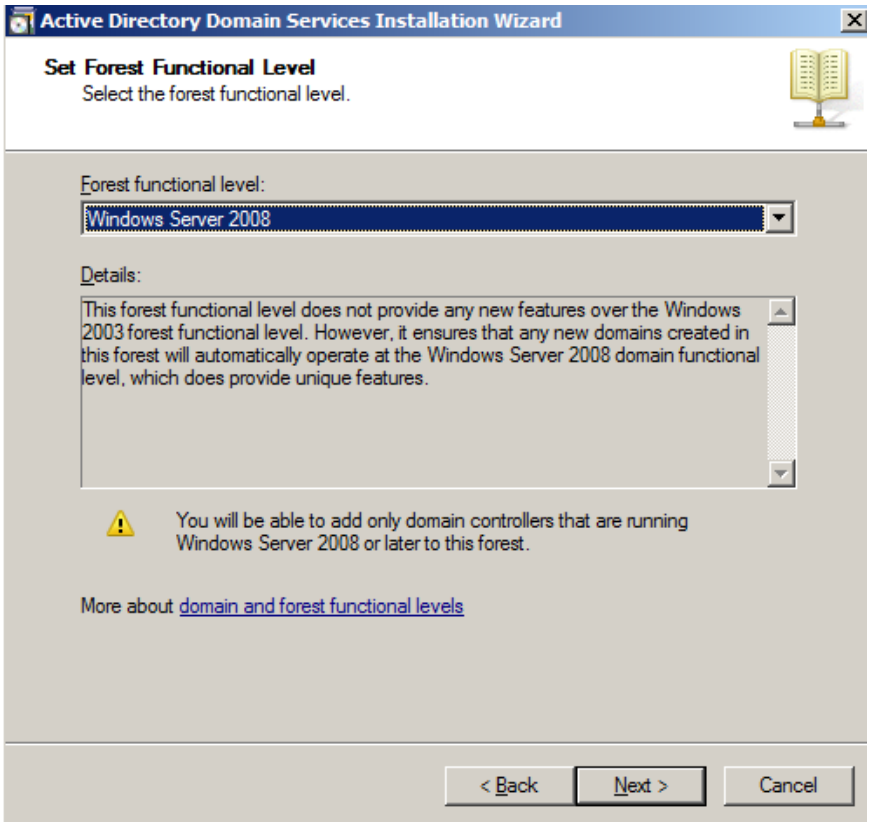


Image 9 DC and DNS Setup procedure

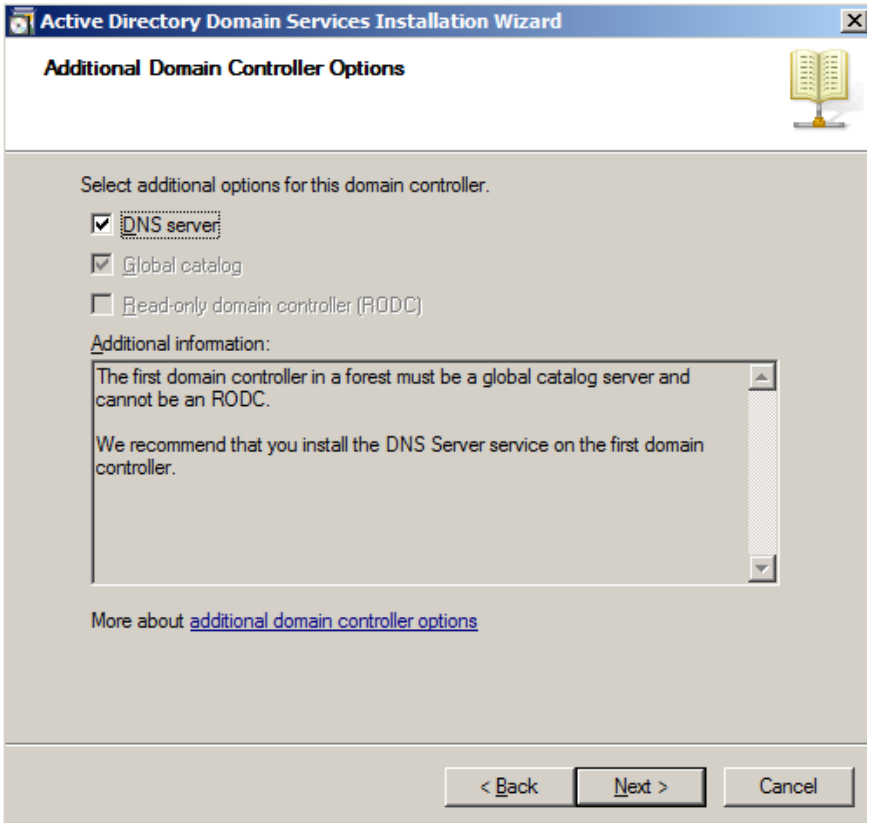


Image 10 DC and DNS Setup procedure

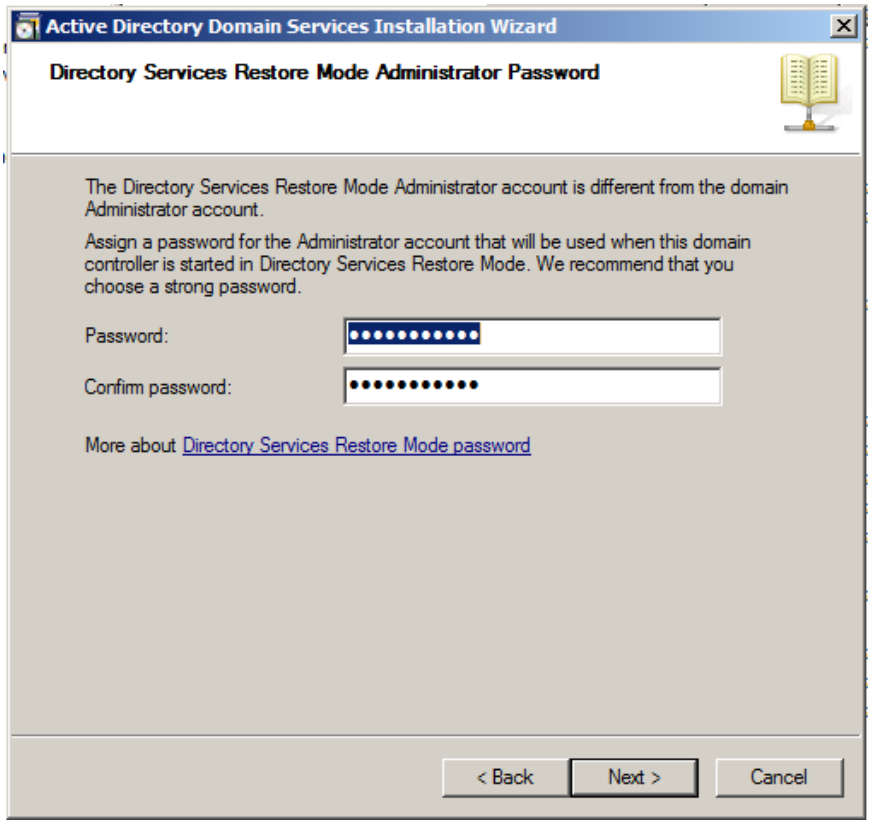


Image 11 DC and DNS Setup procedure

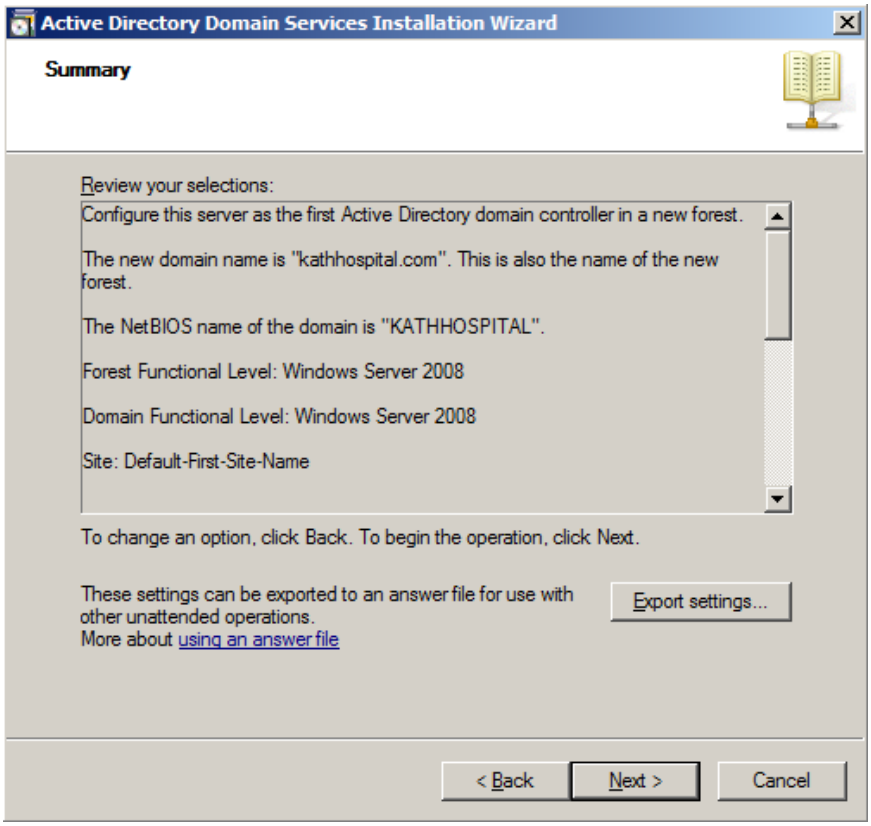


Image 12 DC and DNS Setup procedure

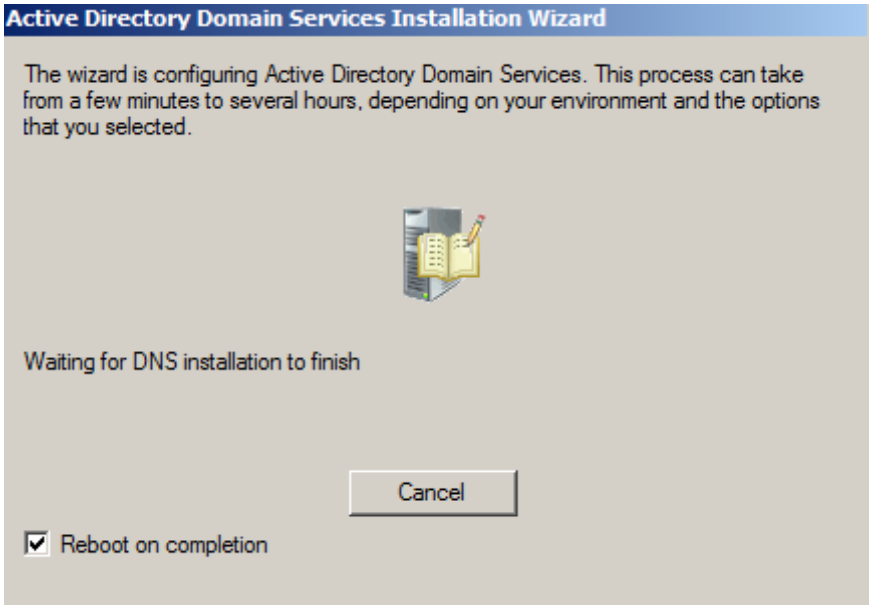


Image 13 DC and DNS Setup procedure

DNS Configuration

DNS server is already installed in Domain server during active directory installation. Now, DNS forward lookup and reserve lookup zone need to be configured. Procedure followed during build and configuration is documented below in form of steps.

1. Login to Domain Computer as domain admin
2. Press WIN + R→ RUN
3. Type in DNSMGMT.MSC→ OK→ This will open DNS manager (Image 14) alternatively, click on Start→ All Programs→ Administrative tools→DNS
4. Delete existing Forward lookup zone.
5. Right click on Server Name
6. In Configure a DSN wizard (Image 15) → choose Create forward and reserve lookup zones (Image 16)
7. Choose yes, create a forward lookup zone now. (Image 17)
8. Chose Primary Zone (Image 18)
9. Put Check on Store DNS in Active Directory→Click Next
10. Choose To all DNS server running on domain controller in this domain: kathhospital.com (Image 19)
11. Click Next
12. Choose yes, create a reserve lookup zone now. (Image 20)
13. Chose Primary Zone
14. Put Check on Store DNS in Active Directory→Click Next
15. Choose To all DNS server running on domain controller in this domain: bank.prabhu.com
16. Click Next
17. Choose IPv4 Reserve lookup Zone→ click Next (Image 21)
18. Choose Network ID and provide→ 10.10.10→ click Next (Image 22)
19. Set Dynamic Update → only secure update→ click Next→Click Next
20. Click Finish (Image 23)

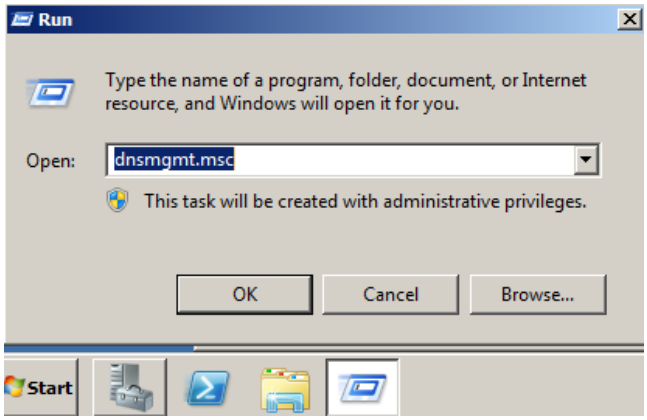


Image 14

Image 15

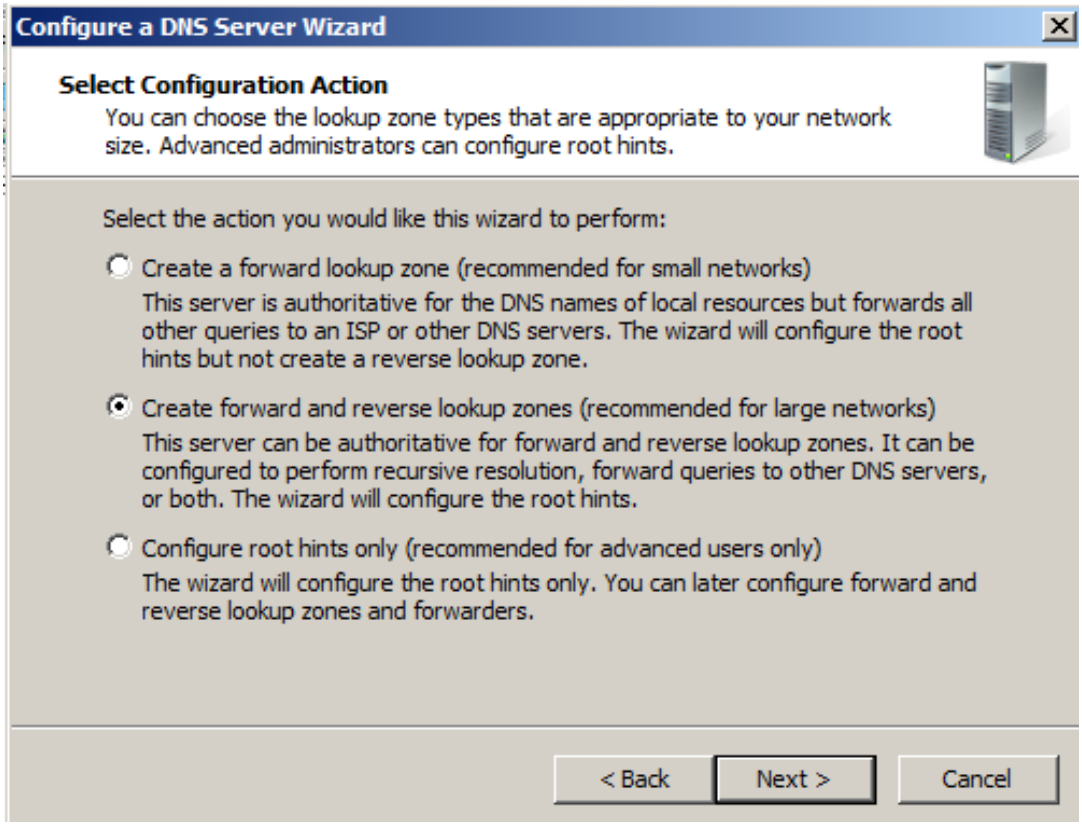


Image 16

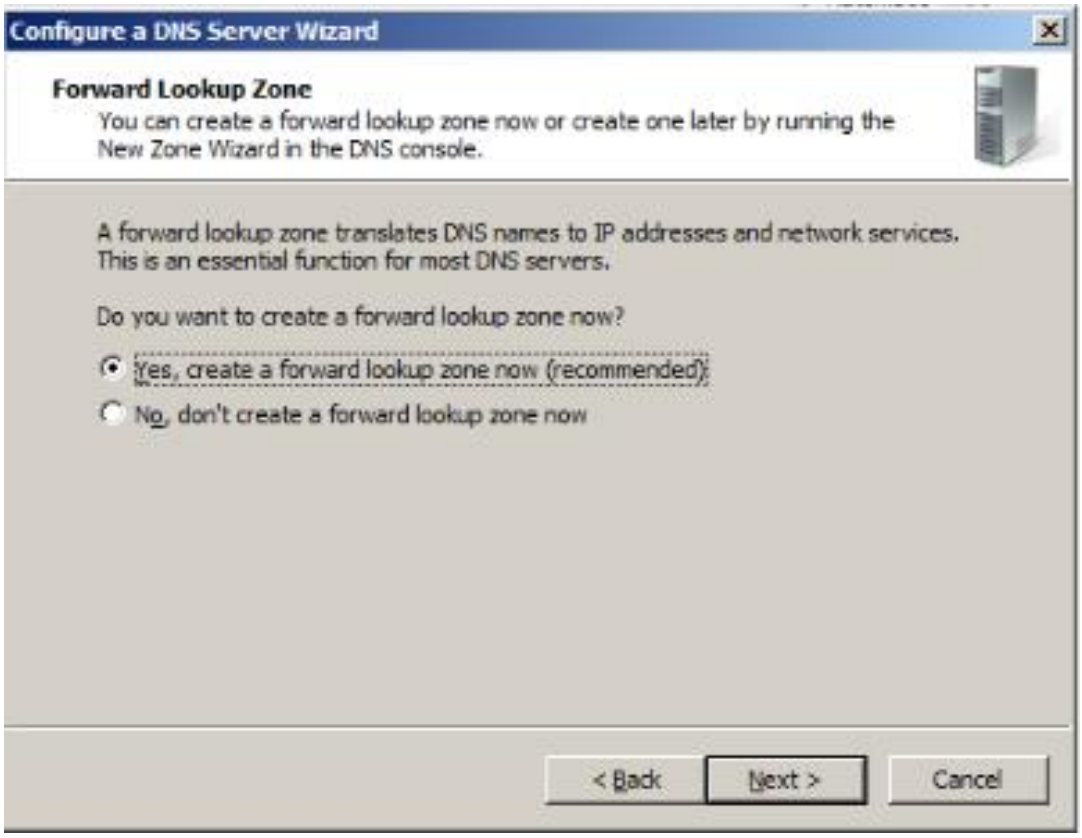


Image 17

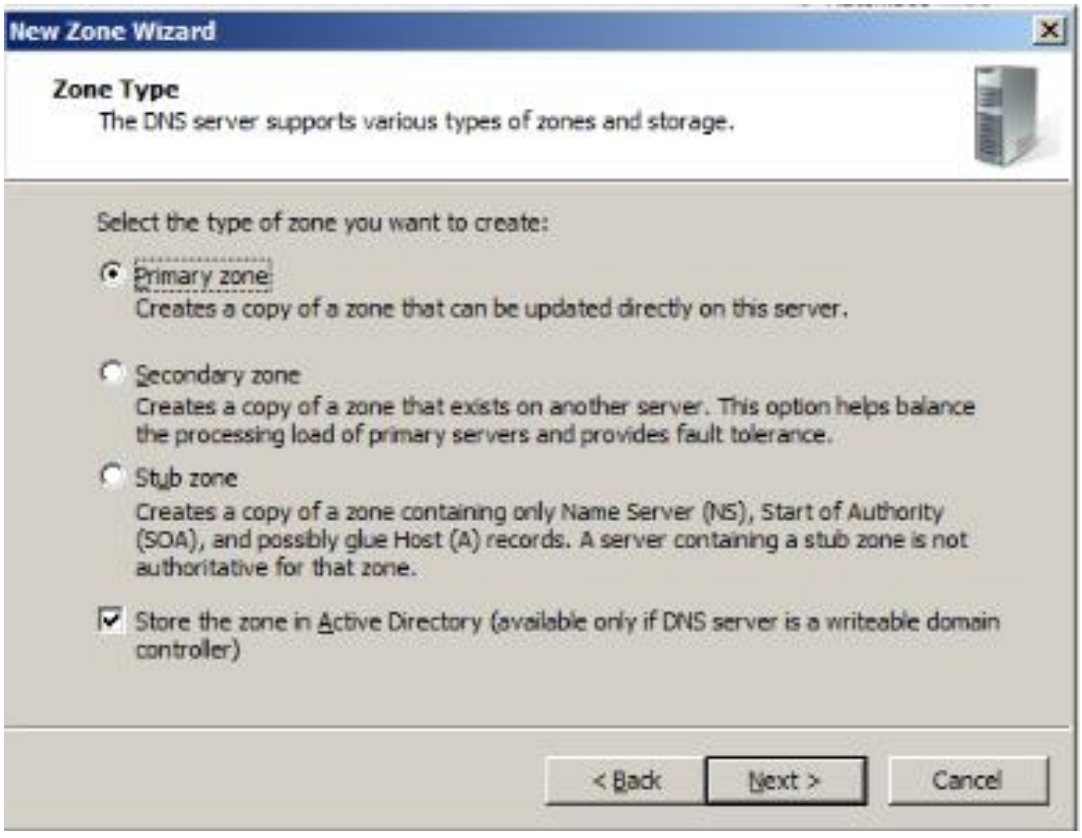


Image 18

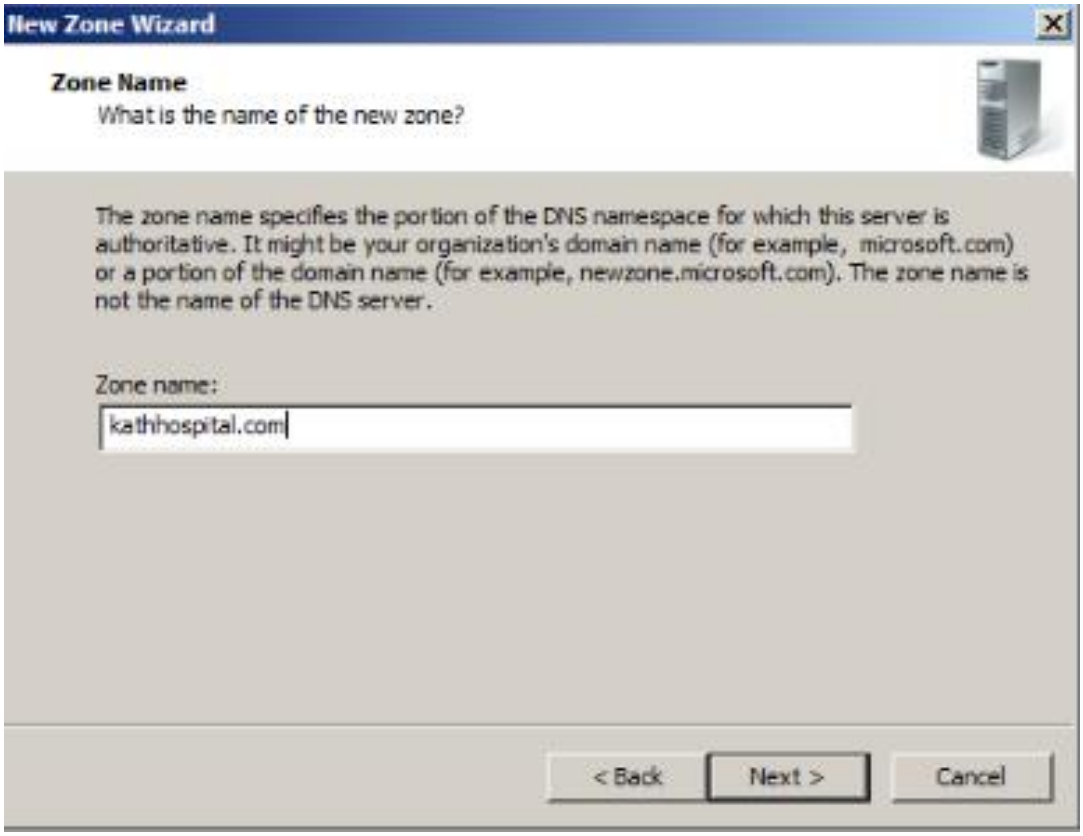


Image 19

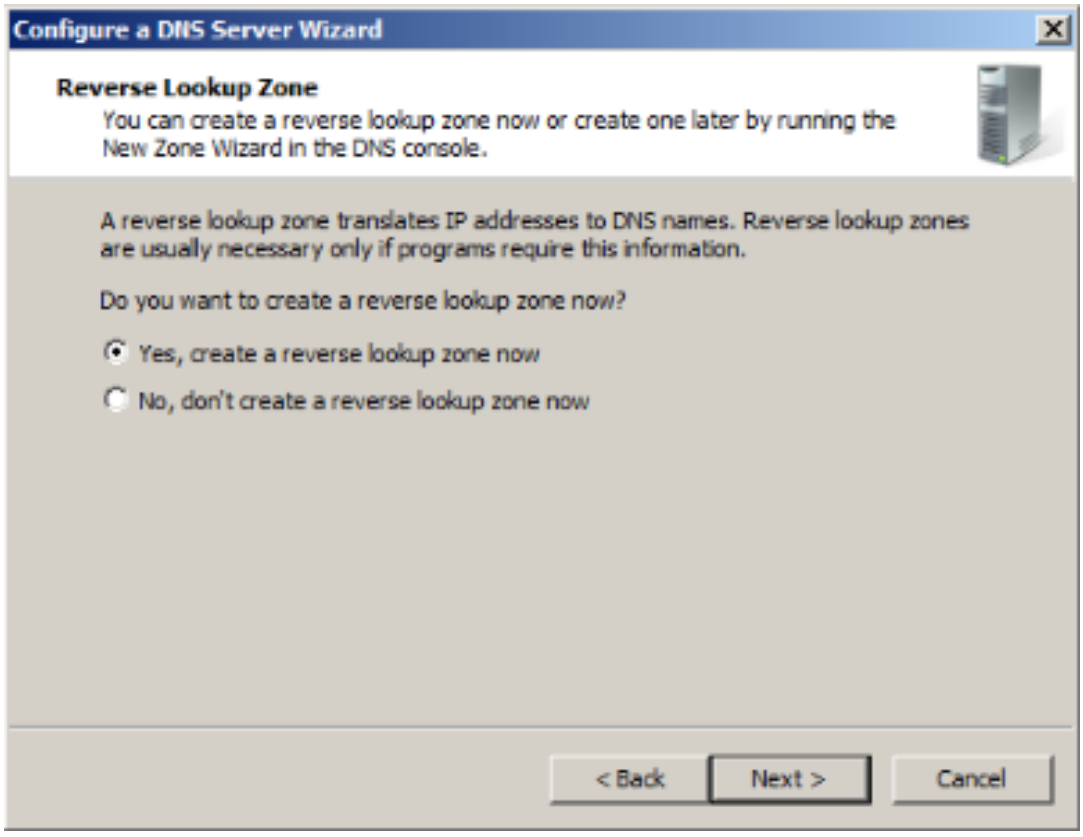


Image 20

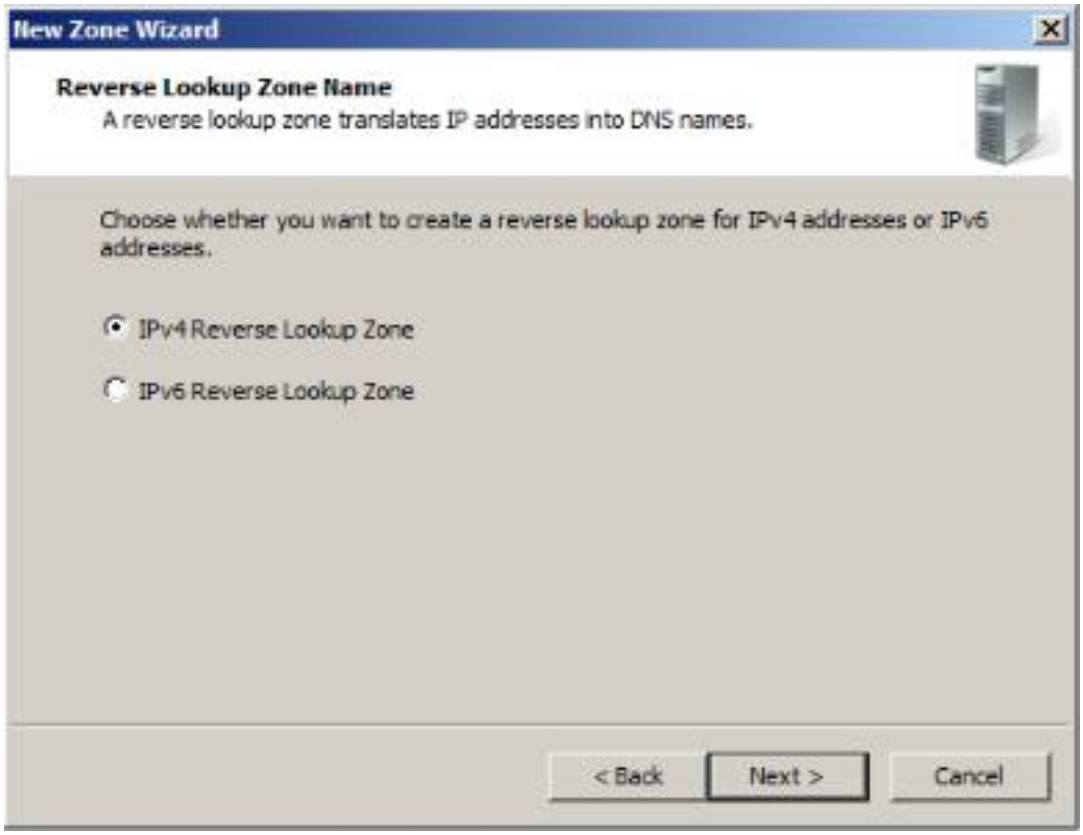


Image 21

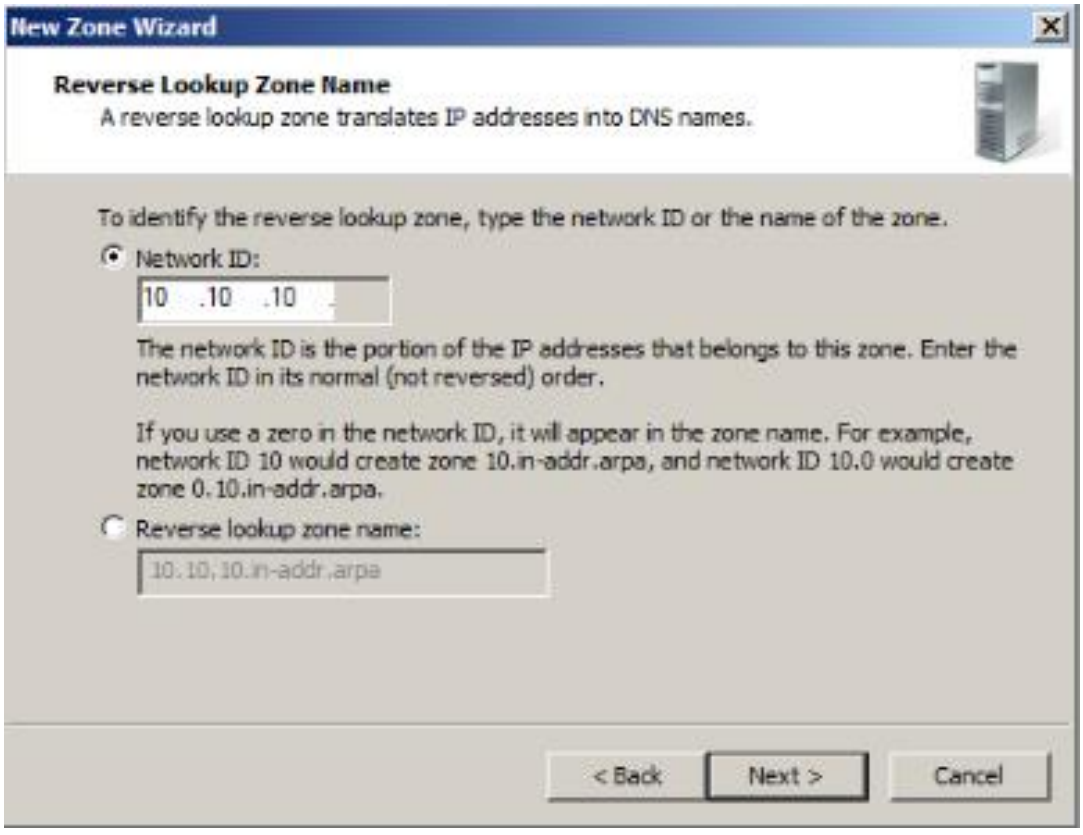


Image 22

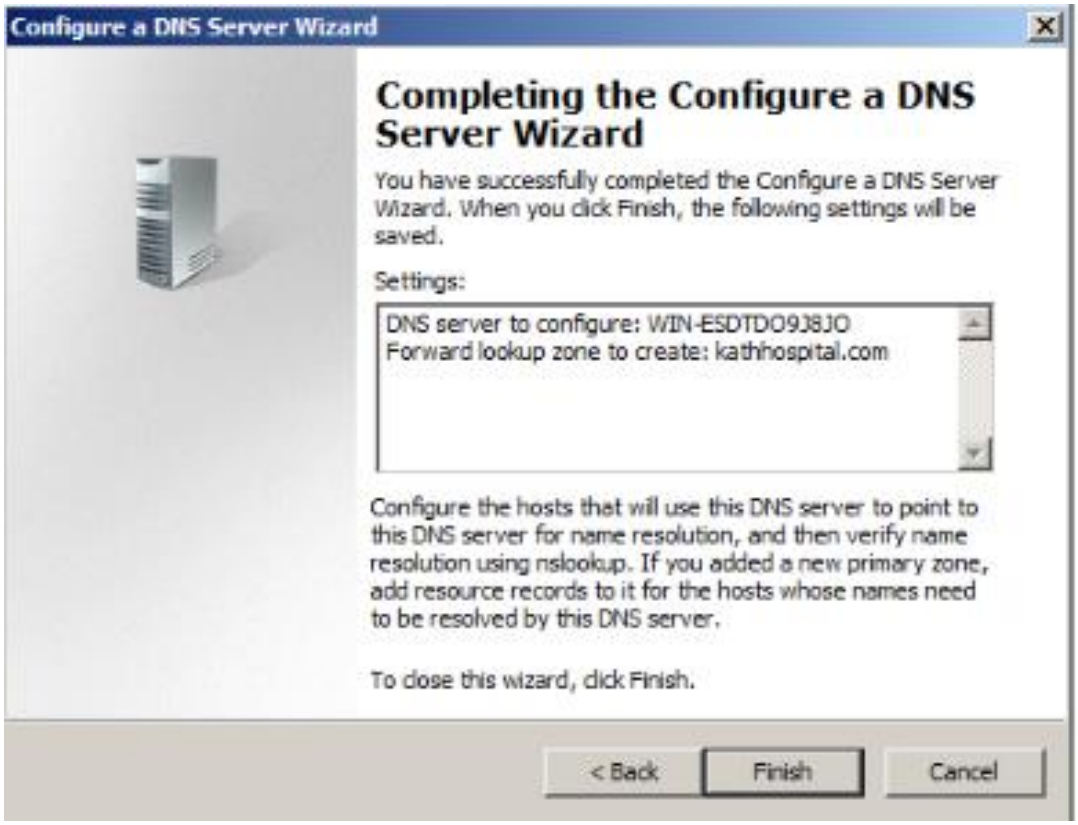


Image 23

NSLOOKUP (DNS configuration Check)

NSLOOKUP check is performed to ensure DNS configuration.

1. Press WIN + R→RUN
2. Type in CMD (Open command prompt)
3. Type in NSLOOKUP
4. Should display name and address→ Done (Image 24)

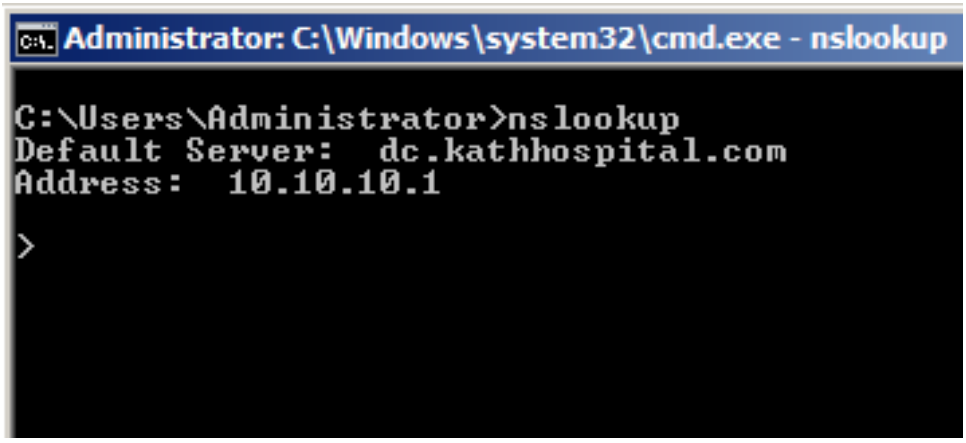


Image 24 NSLOOKUP Check

Domain member configuration

To make a computer member of domain network, for that member needs to join domain using following procedure.

1. Set static IP address 10.10.10.100, subnet 255.255.255.0, DNS server 10.10.10.1
2. Right click on My Computer→ Properties
3. From Computer Name Tab→Click on Change (To rename or change domain or workspace)
4. Supply valid Domain name (From Domain Controller)→BANK→ click OK (Image 25)
5. Provide Valid credentials (Admin username and password of domain)→click OK (Image 26)→Click OK when welcome message arrives
6. Restart Computer and login using domain credential→ Done

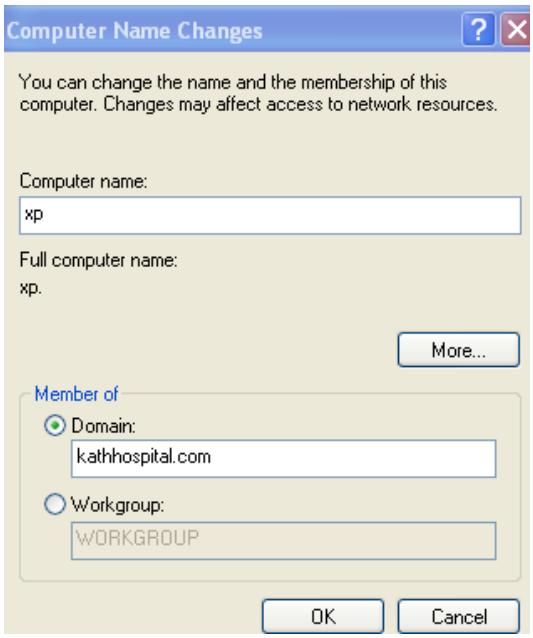


Image 25 Domain member configuration

Image 26 Domain member configuration

Web Server Configuration

To build and configure web server (IIS) following procedures are taken.

1. Setup static IP address of 10.10.10.2 while providing subnet mask of 255.255.255.0
2. Set DNS address of 10.10.10.1
3. Become member of Domain network
4. Login as administrator
5. Go to Start →Programs →Administrative Tools →Server Manager.
6. In the Server Manager → Select Roles
7. Select Add Roles.
8. In the Add Roles wizard →select the Check box for Web Server (IIS). (Image 27)
9. Select the Check box for HTTP Redirection. (Image 28)
10. Click next and click Install. (Image 29)
11. Click Finish.

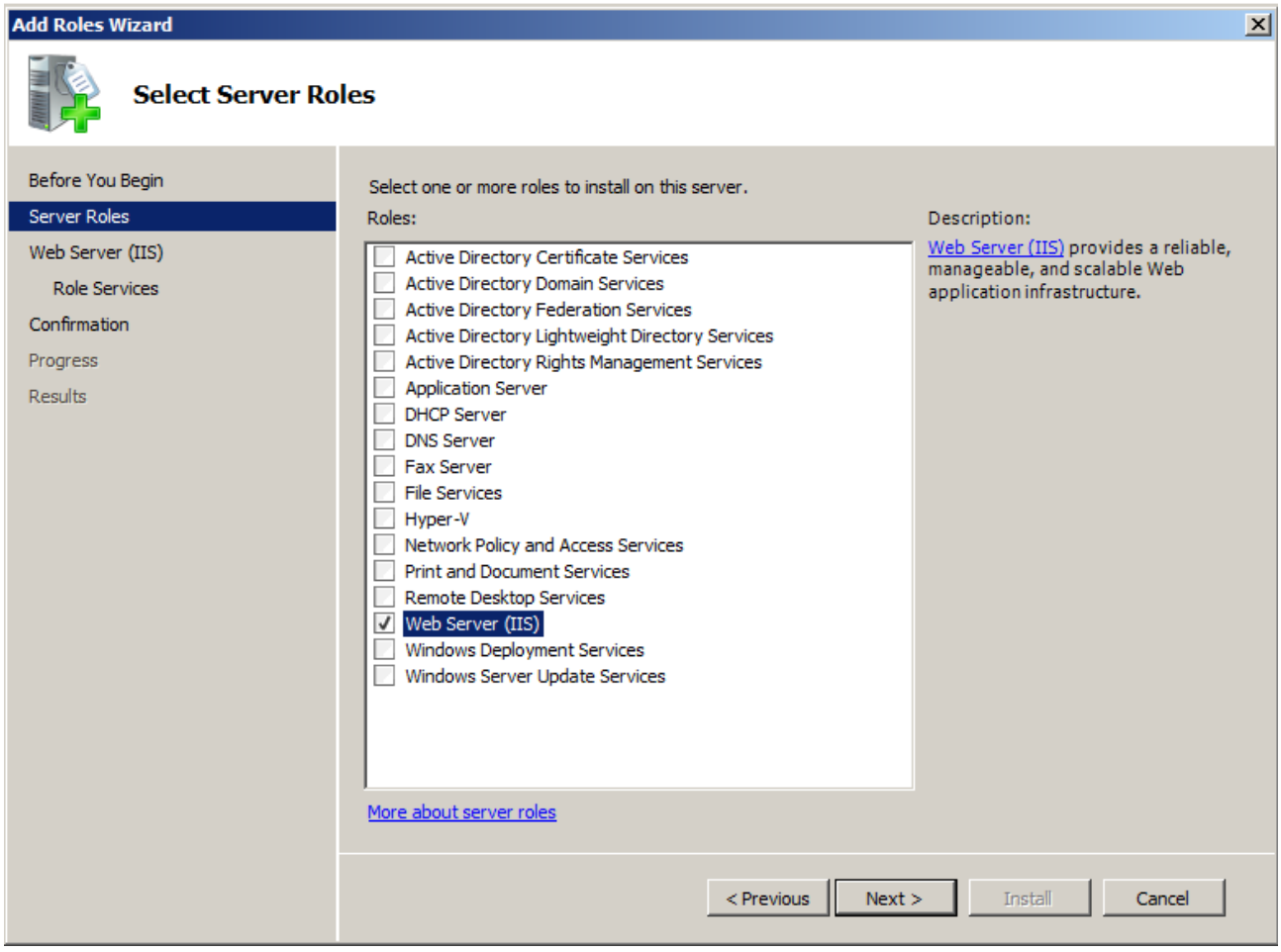


Image 27 Web server (IIS) Installation

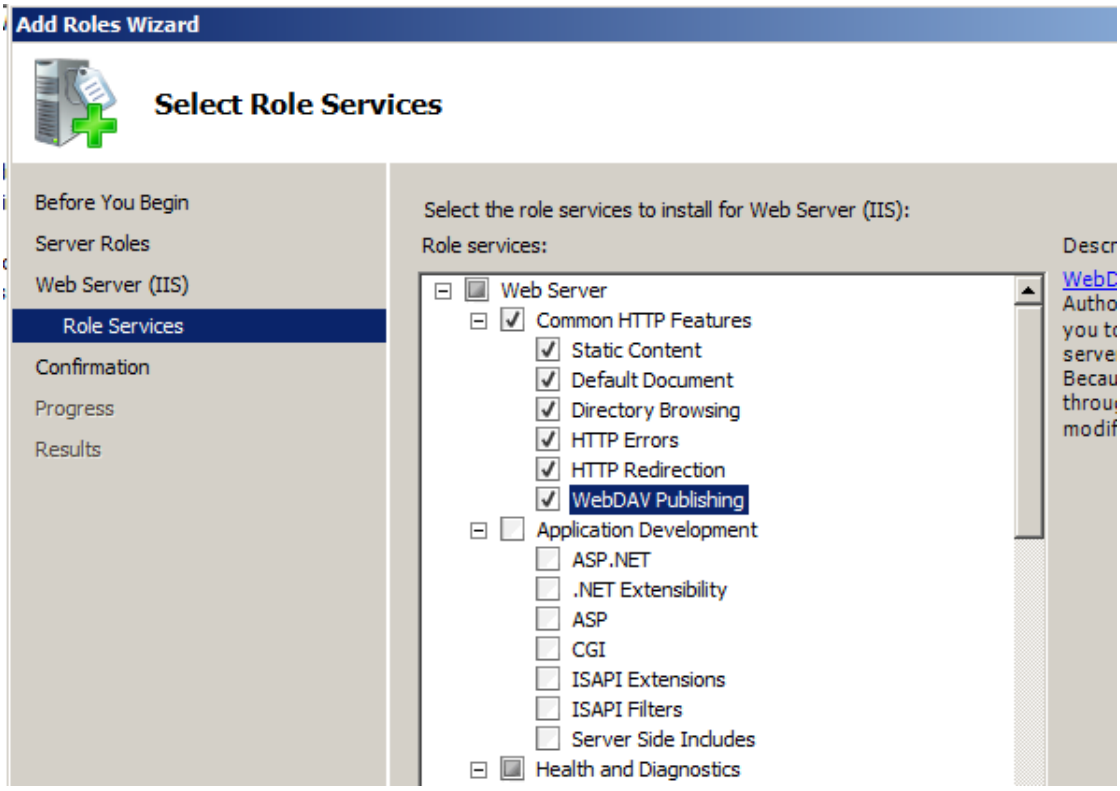


Image 28 Web server (IIS) Installation

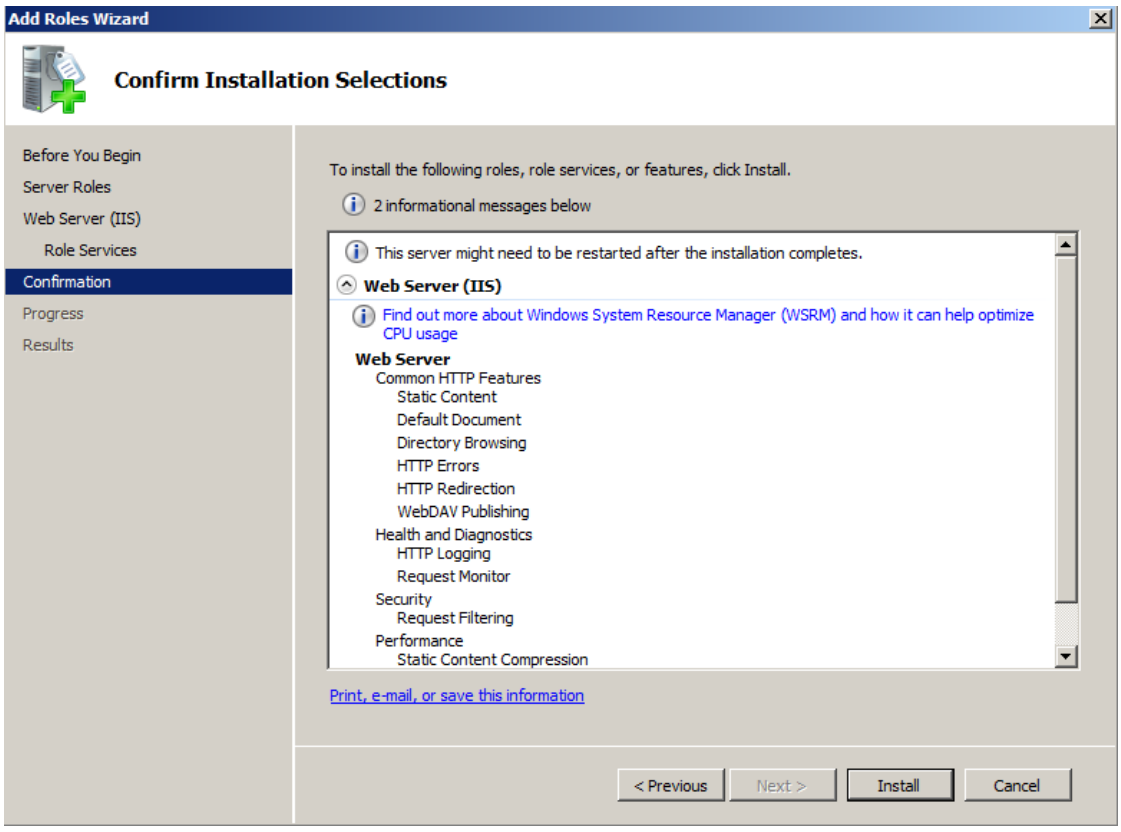


Image 29 Web server (IIS) Installation

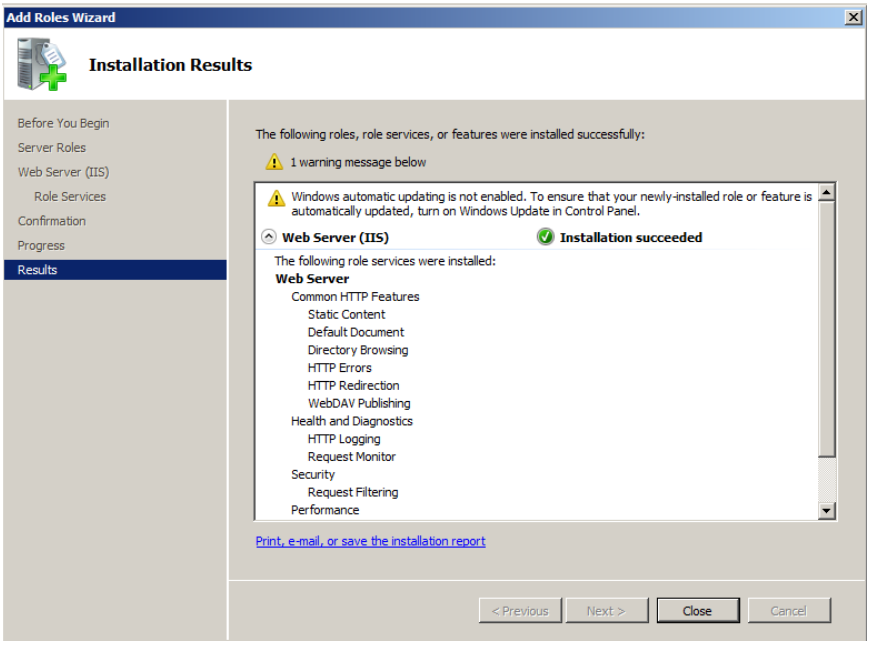


Image 30 Web server (IIS) Installation

FTP Server Configuration

FTP server is configured together with IIS server. Hence, to install FTP server, IIS is required which is already installed. After IIS installation following procedure is performed.

1. Login server computer (with IIS installed) as administrator
2. Go to Start →Programs →Administrative Tools →Server Manager.
3. In the Server Manager → Select Roles and select Add Role Services. (Image 31)
4. Scroll down and tick on FTP Server (Image 32)
5. Click on next→ Click on Install→ Finish (Image 33)

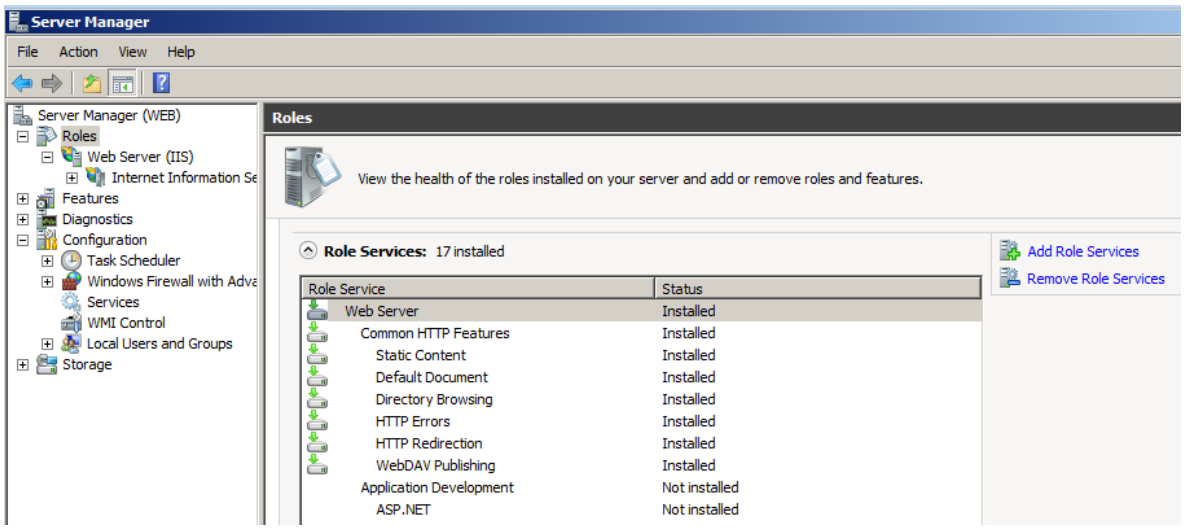


Image 31 FTP Server Configuration

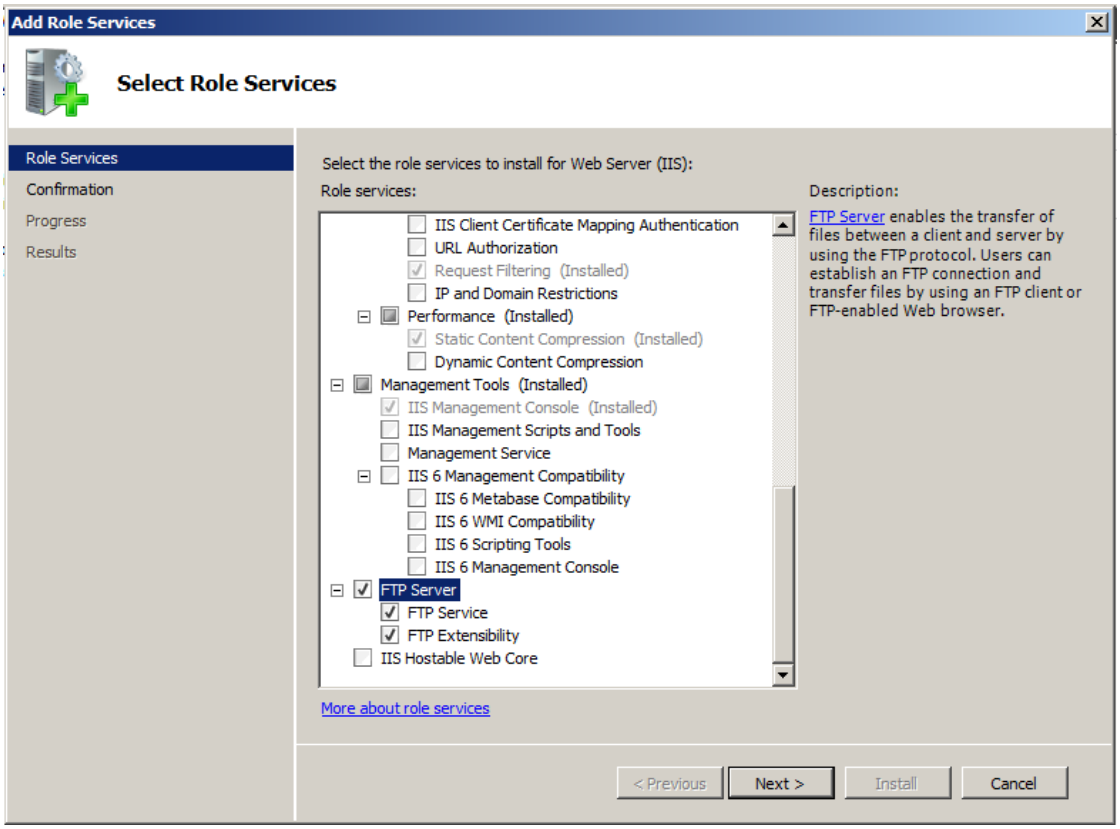


Image 32 FTP Server Configuration

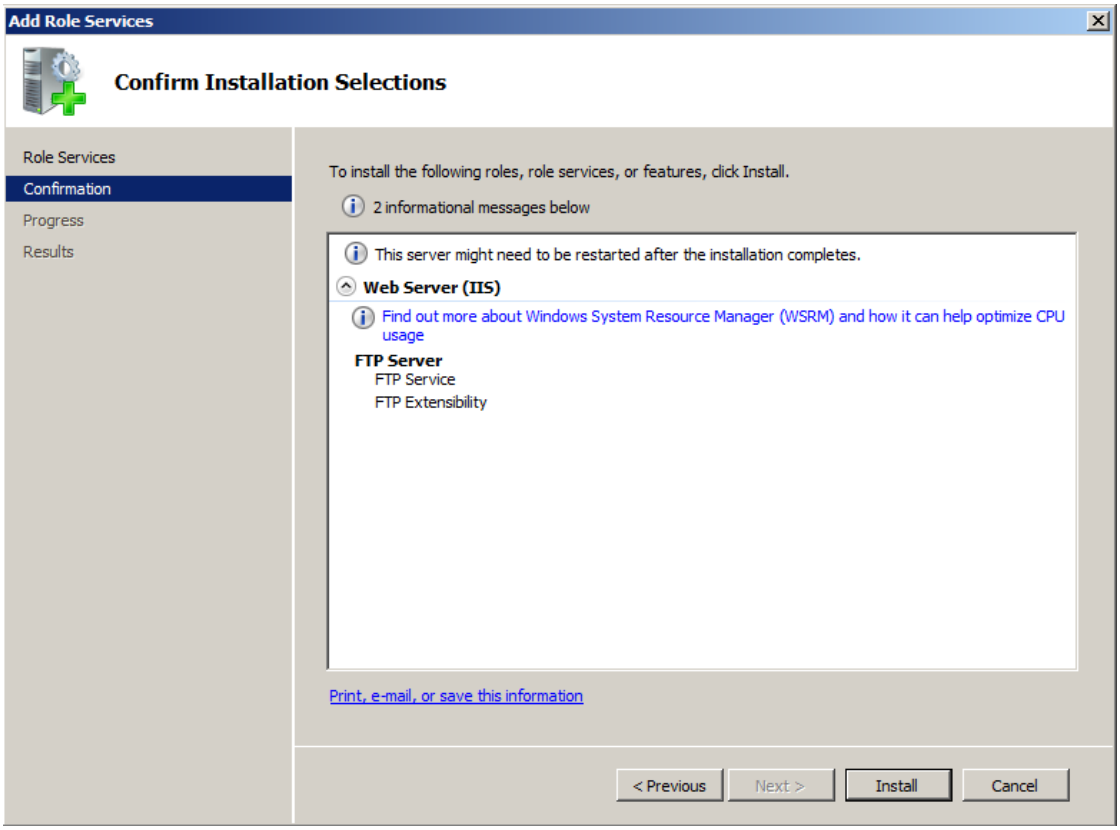


Image 33 FTP Server Configuration

Ecommerce Server Configuration

Asp.net based web application is required be published as Ecommerce site. Hence to satisfy this requirement, web server should be able to support ASP.NET as well as PHP and host such web applications. To enable ASP.NET and PHP based web application hosting for ecommerce site publication, procedure performed are as follows:

1. Login IIS Server as administrator
2. Go to Start →Programs →Administrative Tools →Server Manager.
3. In the Server Manager → Select Roles
4. Select Add Role Services. (Image 34)
5. Scroll down and tick on Application Development (Image 35)
6. Click on next→ Click on Install (Image 36)
7. Click Finish

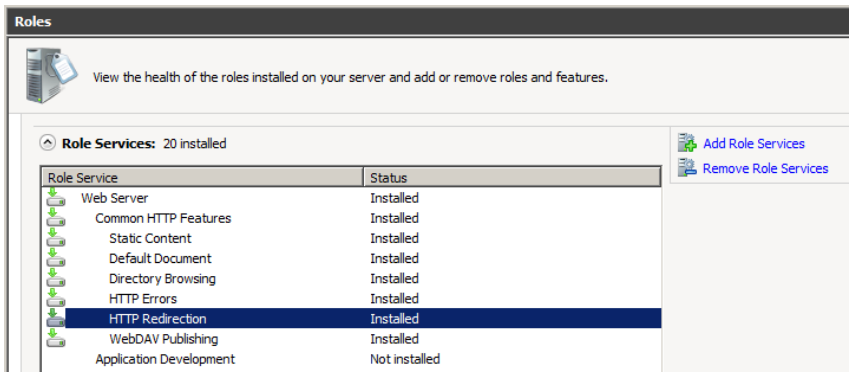


Image 34 Enabling ASP.NET Hosting

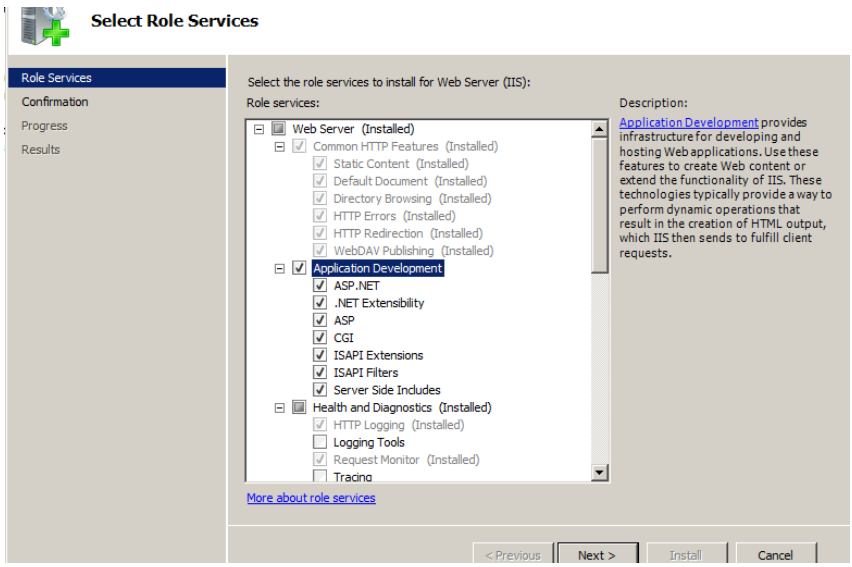


Image 35 Enabling ASP.NET Hosting

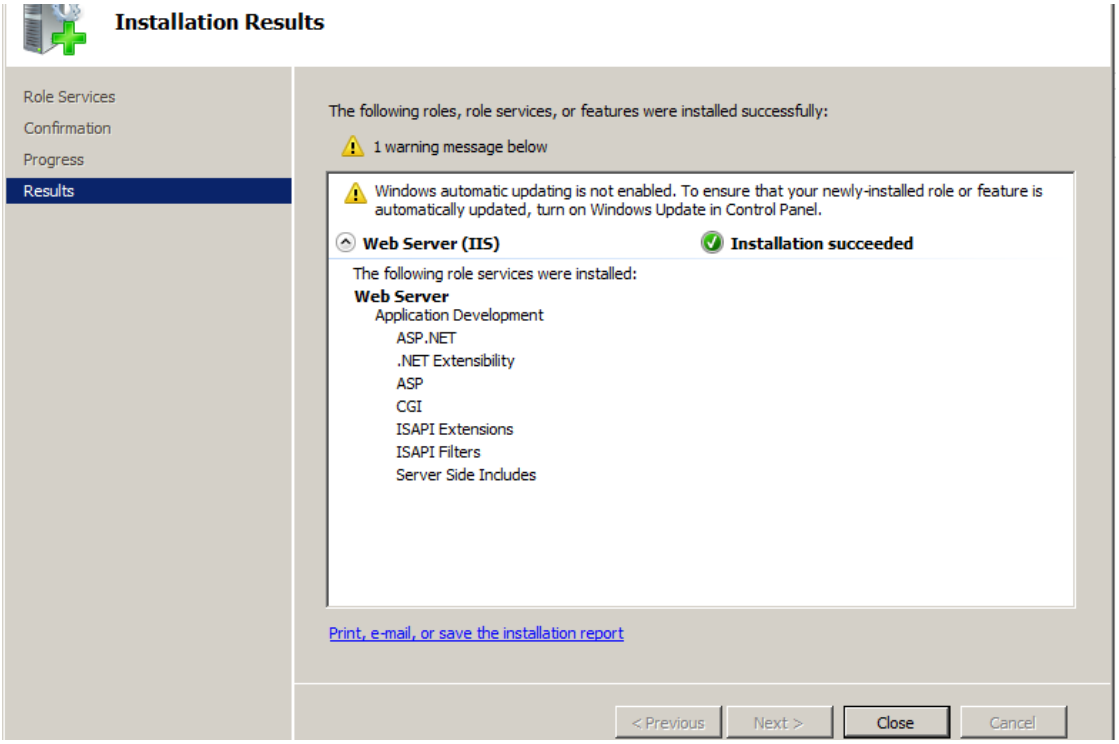


Image 36 Enabling ASP.NET Hosting

Summary

This paper documents building and configuration of internet server and supporting server technologies. Now system is built and configured to support publishing of website, web application, FTP sites.

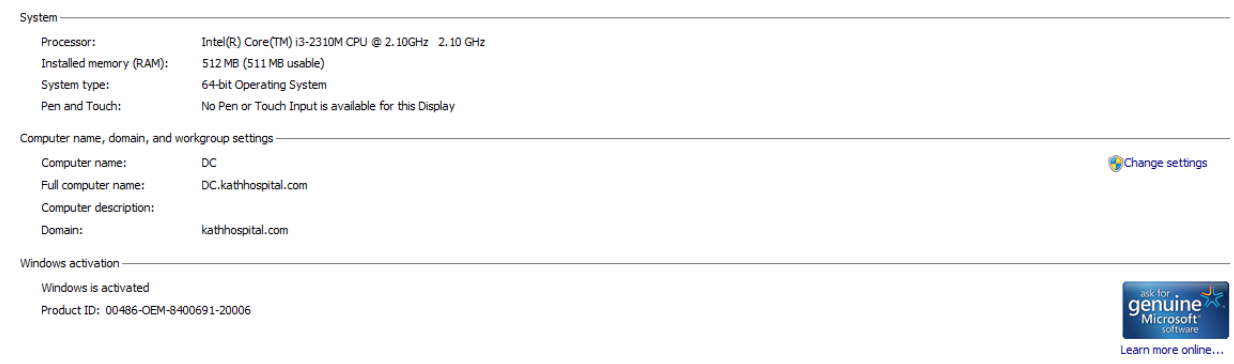
Task8

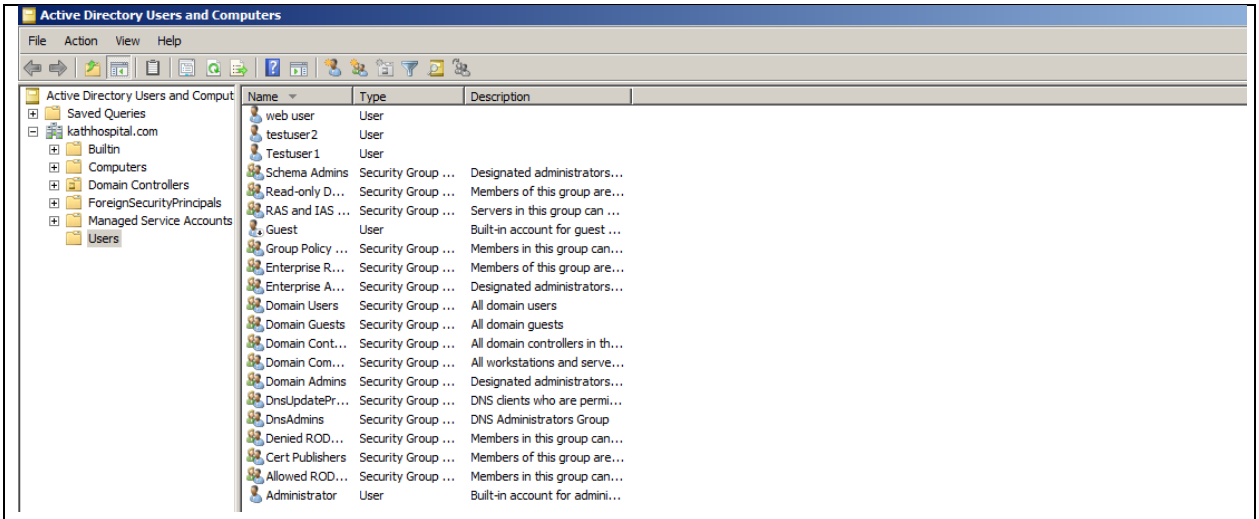
Critically review and test an internet server [3.4, D1]

Introduction

After implementation of Internet server and required supporting server environment, it is essential to conduct tests and developed environment while also analyzing critical review of the system. This is important phase for any project that involves implementation of networking system as it enables administrator to identify any misconfiguration during installation or security management, which is not addressed correctly can jeopardize the whole network. This paper documents conducted tests as a test logs and also prepare critical review of the system identifying strengths and limitations.

Testing of Implemented Server

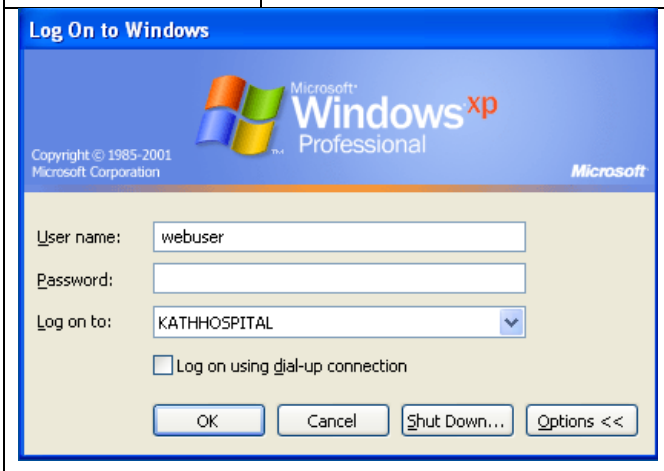
<table>
<tr><td></td><td colspan="2">What was tested: Domain Controller Configuration</td><td>Date: 29/11/2015</td></tr>
<tr><td>S.N.</td><td>Expected Output</td><td colspan="2">Actual Output</td></tr>
<tr><td>1.</td><td>Domain computer should be able to login to Domain</td><td colspan="2">Login allowed to Domain network</td></tr>
<tr><td colspan="4"> 
</td></tr>
<tr><td>2.</td><td>Users and groups should be displayed in Active directory users and Computer</td><td colspan="2">users, groups, OUs of viewed from DSA.MSC</td></tr>
</table>



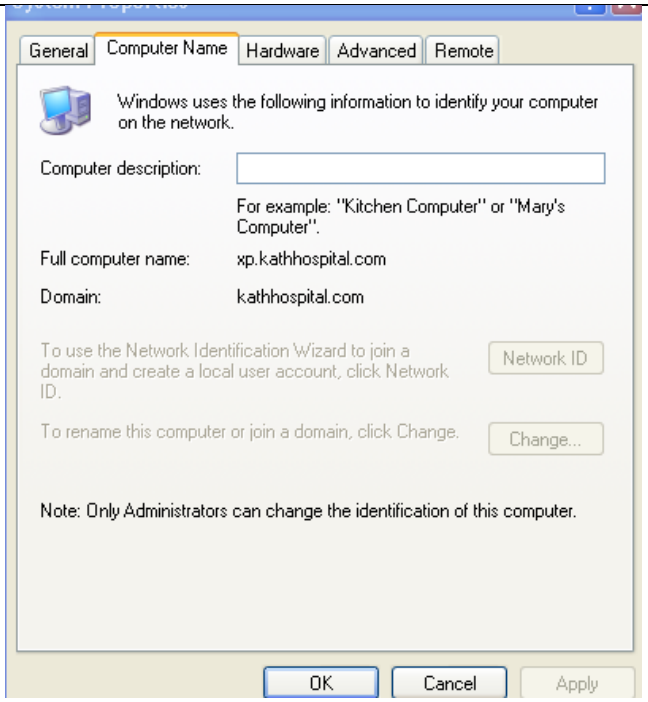
Test Analysis:

To check the domain computer, computer on which domain was installed is utilized. As a domain controller, it should allow to login using domain username and password which test result shows successful login. Additionally, DC should show user account information in active directory. Test results shows DC is configured correctly.

	What was tested: DC Member configuration	**Date: 29/11/2015**
S.N.	**Expected Output**	**Actual Output**
1.	Member should able to login to domain network	Member successfully logged into domain



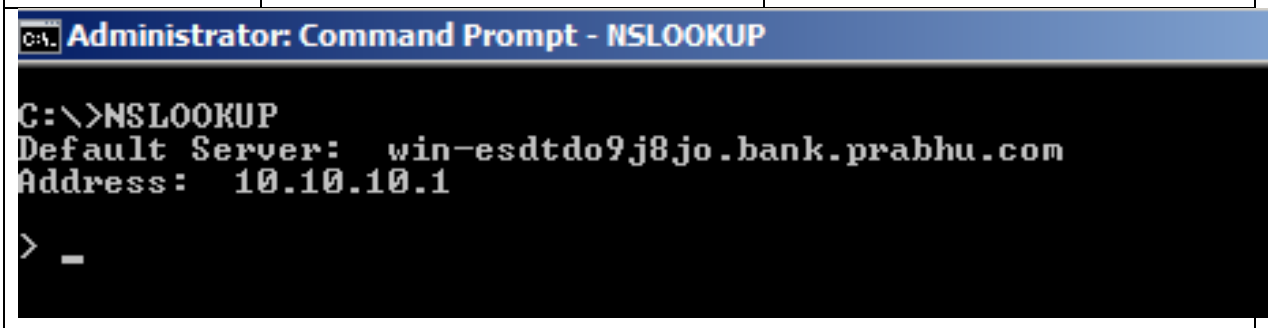
2.	System properties should show host name as as	Domain of member is showing as bank.prabhu.com



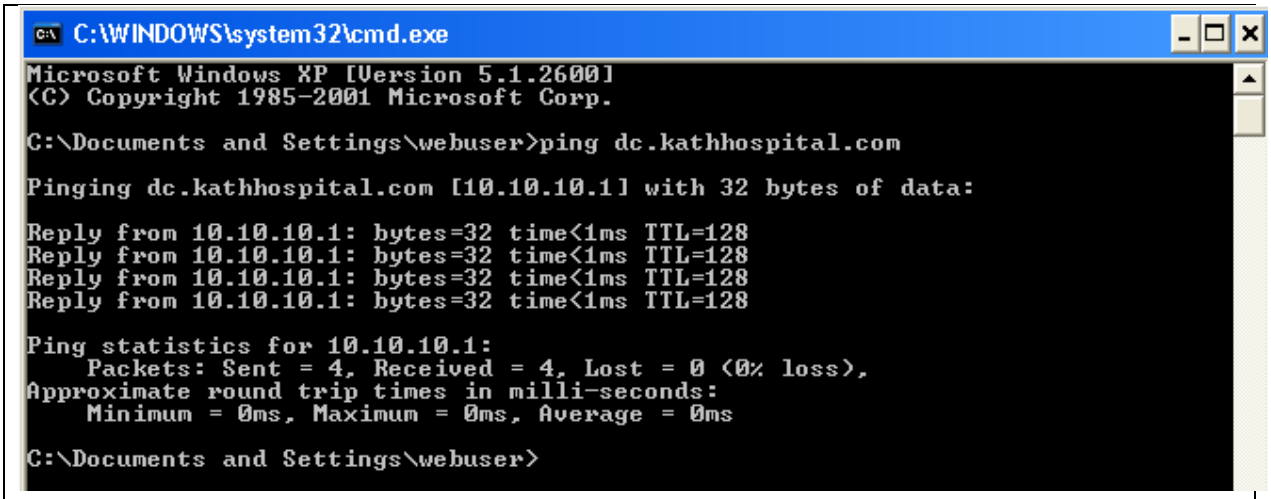
Test Analysis:

A domain member should be able to login to domain network and its properties should show domain as kathhospital.com. Test results shows member computers are correctly configured.

	What was tested: *DNS SERVER Configuration*	**Date: 29/11/2015**
S.N.	**Expected Output**	**Actual Output**
1.	NSLOOKUP tool should show IP address and FQDN of the network	Showed FQDN of DC and corresponding IP address



2.	Should allow to ping other resources using both IP and corresponding text-based friendly name	Supported pinging client computer using name and IP.

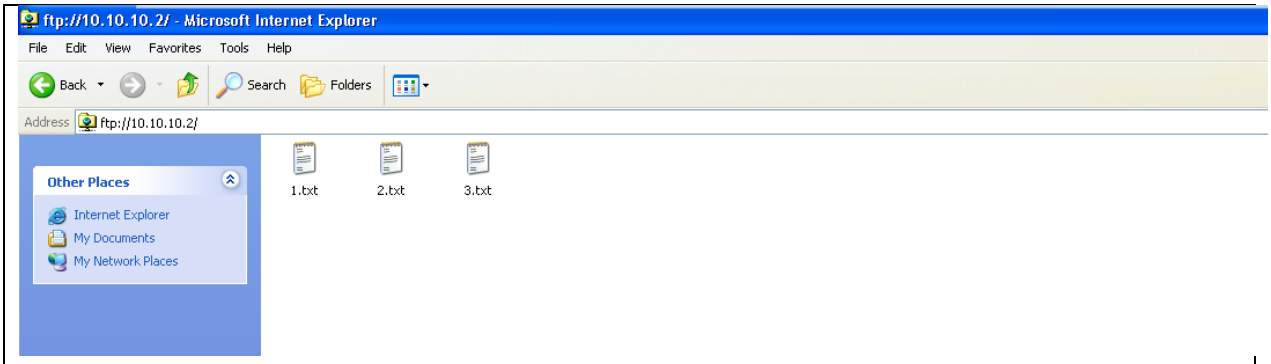


Test Analysis:

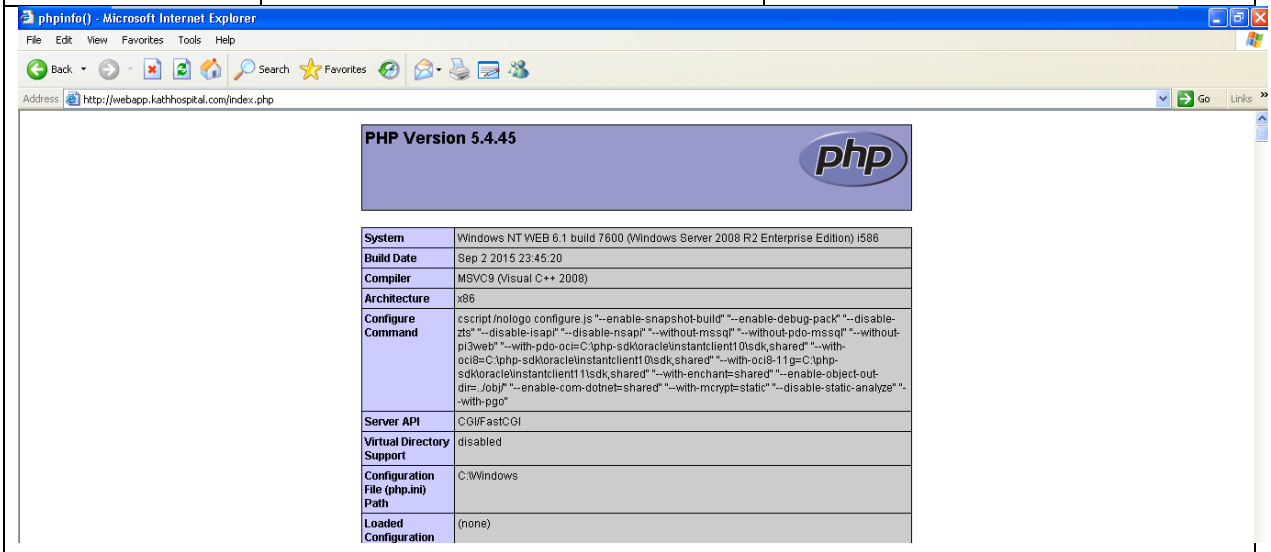
DNS is used for IP to friendly name conversion and vice versa. To test DNS configuration NSLOOKUP and pinging is utilized. NSLOOKUP test shows correct results while pinging resources using their friendly name is also successful. This shows DNS is correctly configured.

	What was tested: *Web server Static*	**Date: 29/11/2015**
S.N.	**Expected Output**	**Actual Output**
1.	Should able to browse published website	Members are able to browse published website

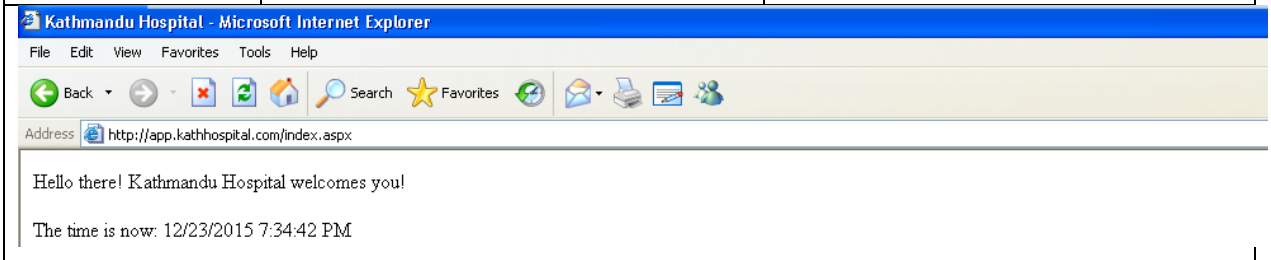
	What was tested: *FTP server*	**Date:**
S.N.	**Expected Output**	**Actual Output**
1.	Should able to browse published FTP website	Members are able to browse published FTP site



	What was tested: *Web application server*	Date: 29/11/2015
S.N.	**Expected Output**	**Actual Output**
1.	Should able to browse PHP site	Members are able to browse published FTP site



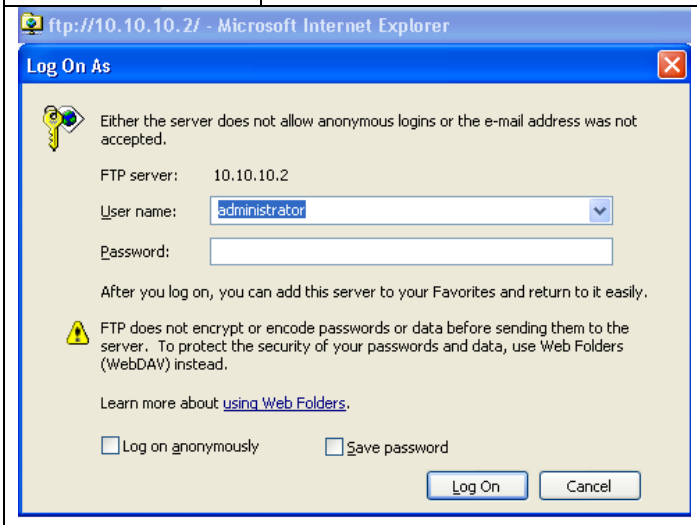
2.	Should able to browse ASP site	Members are able to browse published ASP site



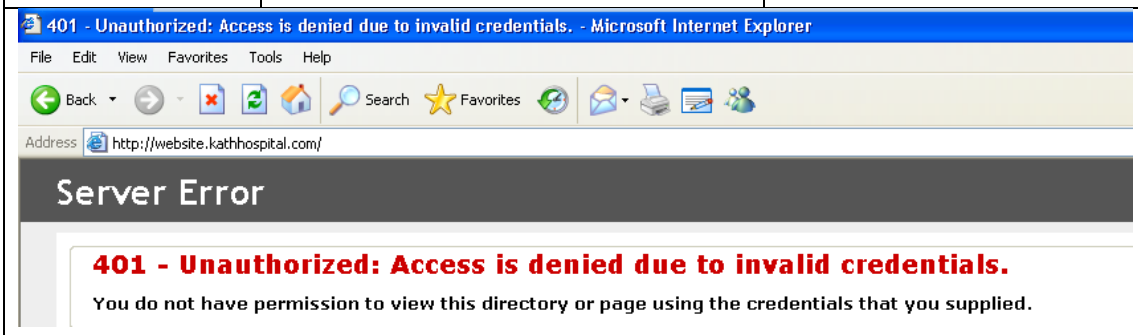
Test Analysis:

Testing of the web server configuration included testing of static website hosting, FTP site hosting and dynamic website site hosting of both ASP.NET and PHP types. Test results shows all website are accessible from web browser and hence functioning correctly. This shows web server is configured correctly to publish sites of various types.

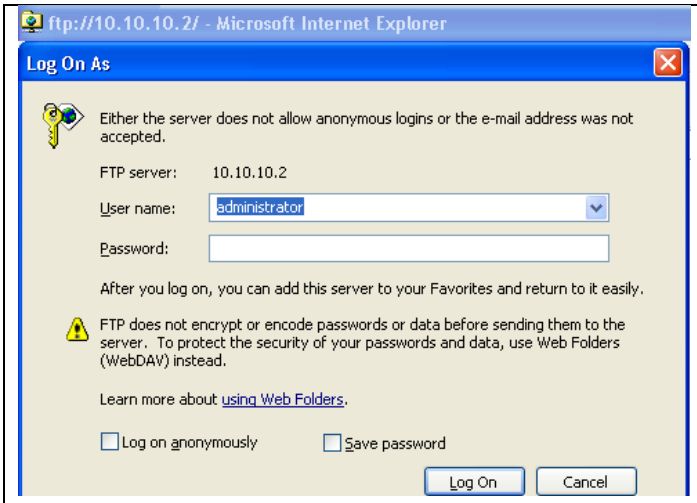
	What was tested: *Security Test*	Date: 29/11/2015
S.N.	**Expected Output**	**Actual Output**
1.	Should require authentication to browse website	Members are able to browse published FTP site



2.	Should block webuser from accesing website based on authorization rule	Denied access to website based on authorization rule

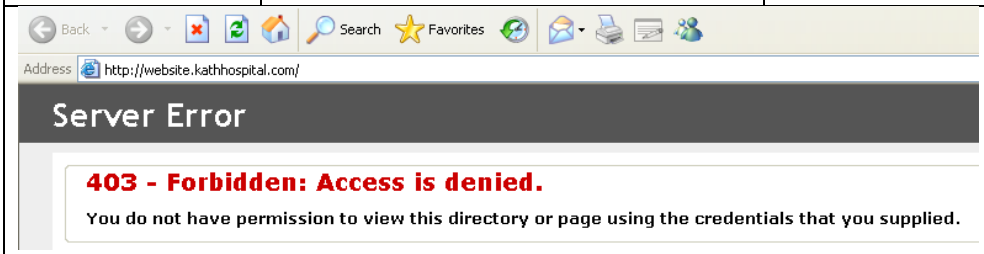


3.	Should require authentication to browse FTP site	Members are able to browse published ASP site



3.	Access control should block deleting files that are denied	Denied deleting file based on access control

4.	Block computer accessing website based on IP restriction	Denied accessing website from computer with IP address in IP restriction denied list



Test Analysis:

Built, configured and managed inter-networking server environment consists of various security mechanism such as FTP security, website security etc. Basic website and FTP security enables webservers to ask for authentication before authorizing webpage transfer. Tests also shows IP restriction mechanism is functioning correctly to deny access from specific IP address specified in IP restriction deny list. Results of the tests shows security of the Internet server is configured correctly.

Critical Review

Introduction

Kathmandu Hospital Pvt. Ltd. is a forefront health and research industry in Nepal. The organization already has public domain www.kathmanduhospital.com which enables them to provide several facilities and services to their clients and patients. Company now requires to implement local internet server to cut the cost of outsourcing dedicated hosting. This project plans, implement and manages web server utilizing appropriate technologies. Developed system requires to provide internet services such as static website hosting, web application hosting, dynamic website (Web application hosting) and FTP site hosting to share large amount of files and directories.

To enable these services inter-networking environment requires to have server technologies such as FTP server, HTTP server etc. Meanwhile, environment also requires server technologies such as Domain controller and DNS server to support inter-networking infrastructure. Administer also requires to plan proper system specification to provide optimal internet server performance and security.

Body: Positive Aspects

Implemented networking project utilizes several hardware as well as software technologies to provide quality and secure internet services. First of all, proper system specification of required hardware and software is planned utilizing various resources to provide optimal and cost effective service performance. Windows 2008 R2 is utilized as server technology due to its easiness and support to large number of hardware and software components. Domain controller server technology enables administrator to provide central administration. While DNS is essential to provide Internet services as it is almost impossible for all users to remember numerical IP address to access services. Windows server 2008 R2 allows system administrator to implement **IIS** web server. IIS provides internet services such as webpage hosting, FTP site hosting, site security, web application hosting etc. Which can single handedly satisfies requirements of the organization.

In implemented inter-networking environment, IIS is utilized to provide hosting service of static websites. Which allows clients and patients to access web pages from their web browser and get information about researches, services etc. It simply transfers web pages from website directory (network drive/local drive of IIS) to client's browser without modifying anything. FTP sites are also implemented in network utilizing FTP server component of IIS. FTP allows to share large files over internet using file transfer protocol which is mot efficient way of transferring large files.

IIS server is configured to provide support to ASP and CGI application. Added roles in IIS allows to host ASP and ASP.NET bases dynamic websites (web application) and PHP based application. Which by default is not supported. These web application services allows organization run web based management, information, calculation or research applications. Each internet services are DNS configured to allow clients to access those using friendly names instead of number IP addresses.

Negative Aspects (Limitations)

While system is well planned, implemented and managed to satisfy business requirements of Kathmandu hospital. It also have some of the significant limitations. Absence of Email server forbid clients and administrator to send and receive email which is significant component of internet services. Another drawback of developed inter-networking environment is absence fail over mechanism. Absence of secondary DNS and Secondary DCs. If connection with primary DNS and DC breakdowns by any mean, whole network will be suffer. It is also worth mentioning that IIS does not allow administrator to modify and configure server component using single configuration file which one of the main drawback of IIS over apache system. Dedicated database server is absent in implemented environment which means added load pressure on server on which database is installed.

Conclusion

This paper documented testing phase of implemented environment as test logs while analyzing test results. Test results shows supporting server technologies such as DC and DNS is configured correctly to provide central administration and naming services. Test results also shows web hosting, FTP hosting and web application hosting configurations are done correctly and functioning well. Management of security components in web server and supporting environment is also configure correctly to provide secure network performance. Though it is recommended to conduct more detailed tests and continuous monitoring to identify misconfigurations.

This paper also provides critical review of the project. Review of system shows inter-networking servers are able to provide internet services required by Kathmandu hospital. Proper user of hardware and software plan enables to provide optimal service quality and security. Based on the critical review analysis it is recommended to email server to provide email services to its clients. Finally, it is also recommended to implement proper fail over mechanism in case of connection breakdown with main DC. This can be achieve via proper implementation of secondary DNS and

DC. Though it will raise to cost of implementation and management it will ensure continuous service even in critical situation.

Task9

Install and manage websites and services to meet a given requirement. [4.1, D2]

Introduction

Networking environment and Internet server including services are already built and configured for Kathmandu Hospital. Now to achieve requirements of Kathmandu Hospital, several services are required to be installed and managed on implemented server environment. This paper documents installation and management and website, ftp sites, ASP.net based web application as well as PHP based web application. Additionally, components such as DNS is also configured and documented in this report.

Website Publish

Kathmandu Hospital requires to implement both static and dynamic website. Implemented internet server is capable of serving both static and dynamic websites. Static website publication is much simple and IIS support it by default. To host the web site of organization in webserver following procedure in performed.

1. Login IIS Server as Administrator
2. Select Start→Programs→Administrative Tools→Internet Information Services Manager. (Figure 1)

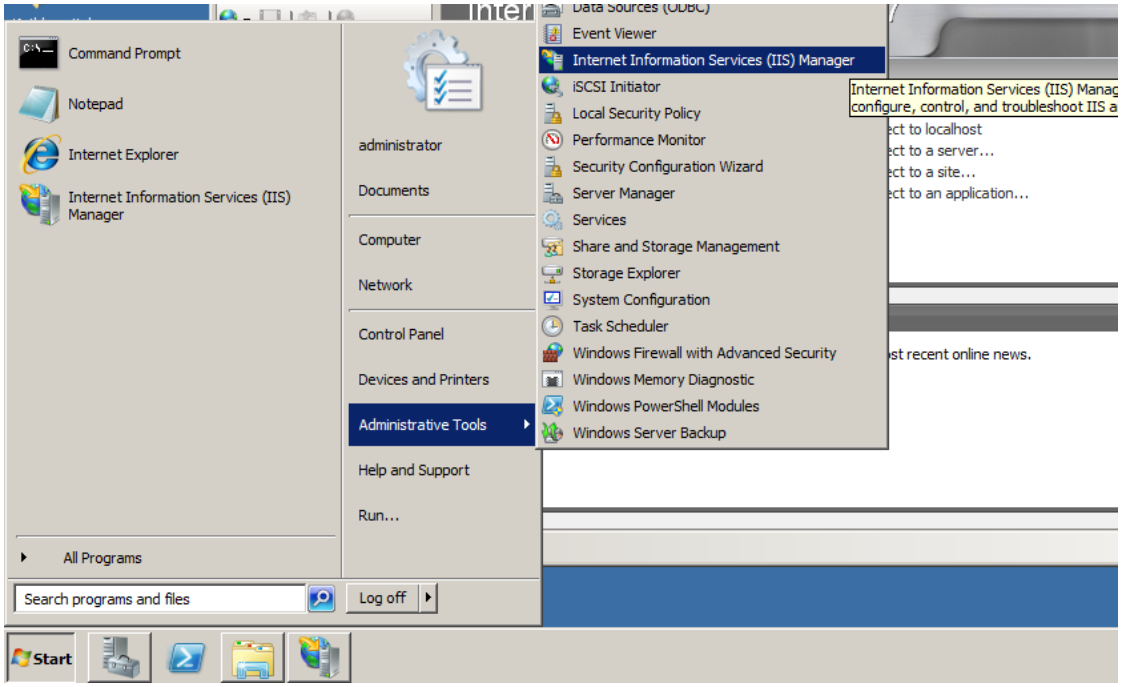


Figure 16Adding new website

3. In the left pane of the Internet Information Services, Expand the server →Right click on sites and select Add Web Site. (Figure 2)

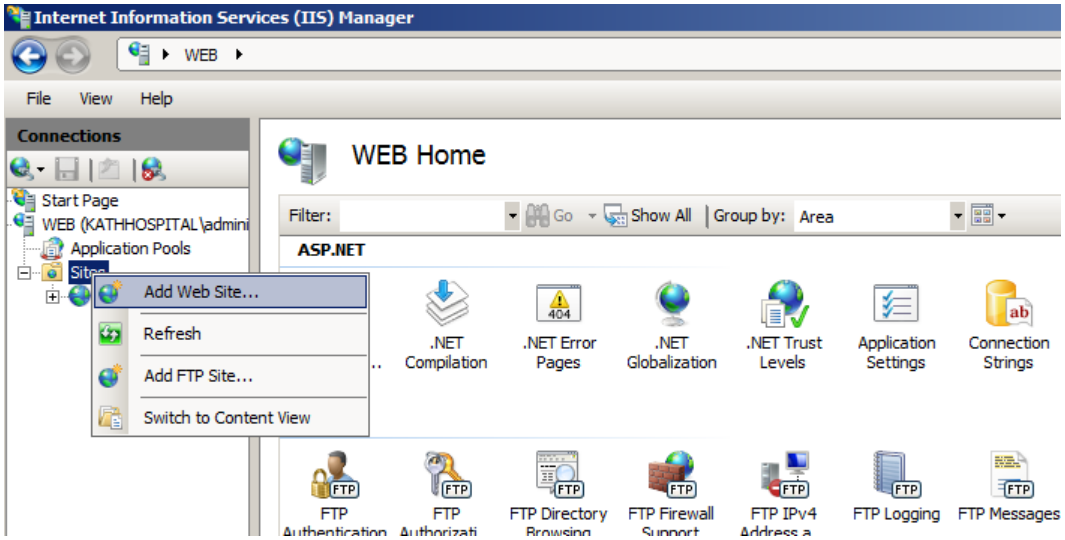


Figure 17 Adding new website

4. In Web Site wizard type name for the site **WEBSITEKATHHOSPITAL** (Figure 3)

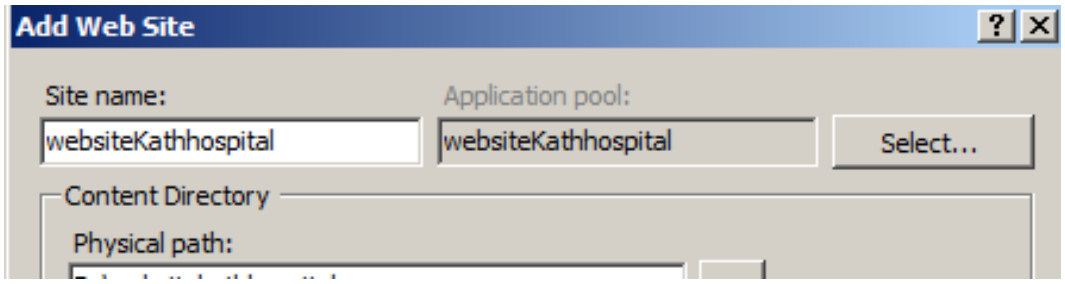


Figure 18 Adding new website

5. In Physical path, browse and select the location of Home Directory (webpage) (Figure 4)

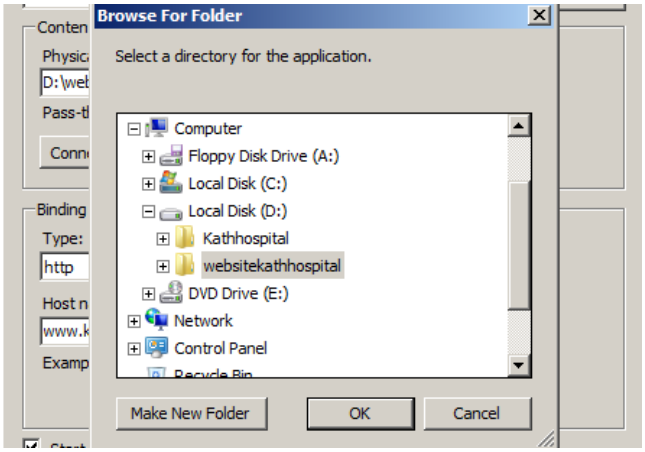


Figure 19 Adding new website

6. Select IP address (10.0.0.2) of web server from the drop-down list. (Figure 5)

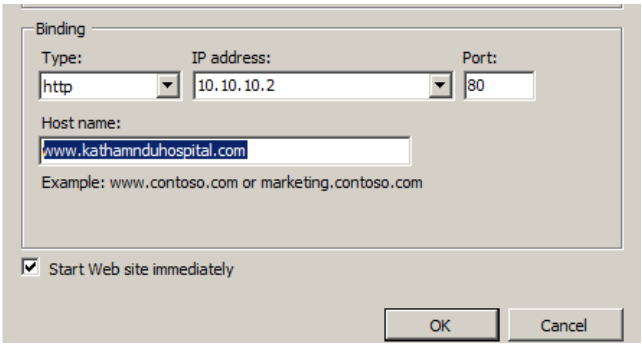


Figure 20 Adding new website

1. Specify the Host name for the website (**WWW.KATHAMNDUHOSPITAL.COM**) → Click OK. →Web Site will be added successfully.

DNS Configuration WEBSITE

A web server can host multiple websites, each website requires unique host name to access them. To bind host name with IP address of web server, DNS needs to be configured in DNS server which in this scenario is located in domain server. To configured DNS for website procedures below are followed:

1. Login DNS Server as Administrator
2. Select Start → Programs → Administrative Tools →DNS
3. Select forward lookup zone →**KATHHOSPITAL.COM**→ Right click select New Host (Figure 6)

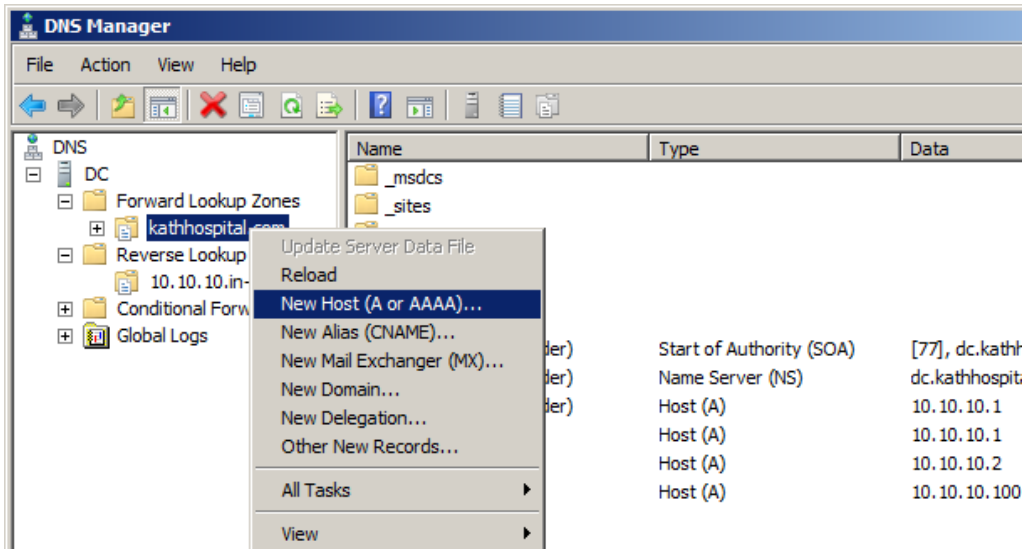


Figure 21 Website DNS configuration

4. Mention the name (Website) and IP Address (10.10.10.2) (Figure 7)

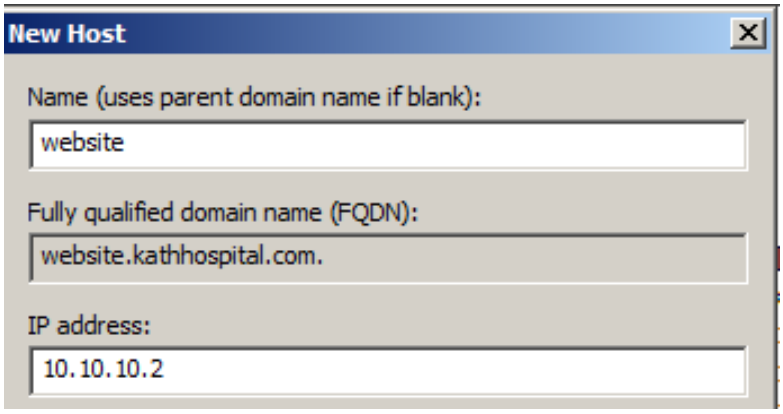


Figure 22 Website DNS configuration

5. Put tick mark on Create associated pointer (PTR) record→Add Host (Figure 8)

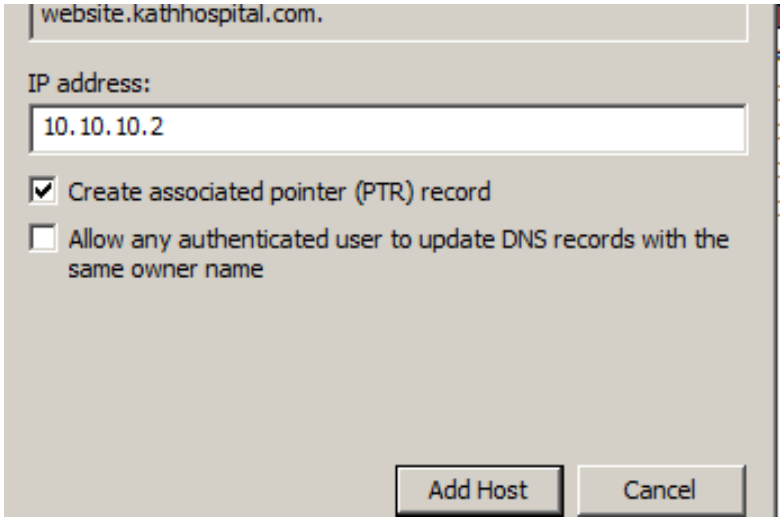


Figure 23 Website DNS configuration

6. Click on OK () →Done (Figure 9)

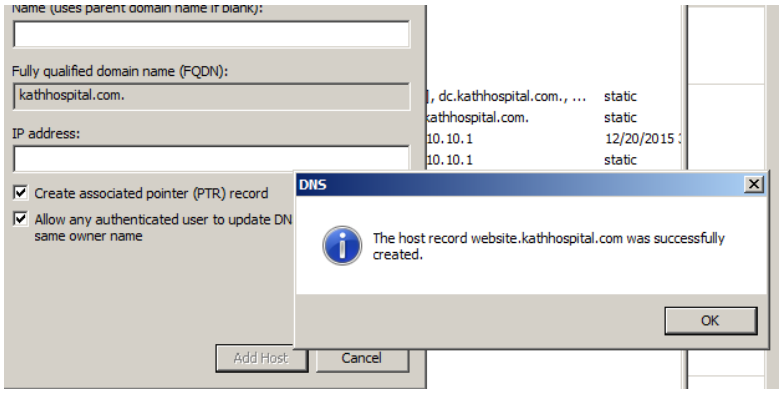


Figure 24 Website DNS configuration

Verifying website hosting

1. Open web browser
2. Type address of the website→ Press Enter (Figure 10)

Figure 25 Verifying website hosting

HTTP Redirection

HTTP redirection is done to allow accessing website using multiple host name. For Kathmandu hospital, host name required to access website is website.kathhospital.com. HTTP redirect allows clients to access that website using additional hostname www.kathhospital.com to ease the access process. Following procedure is performed for URL redirection.

1. Select Start →Programs →Administrative Tools →Internet Information Services Manager
2. Add new website **WWW.KATHHOSPITAL.COM**
3. Configure DNS for new website in DNS server
4. Select **WWW.KATHHOSPITAL.COM** in IIS (Figure 11)

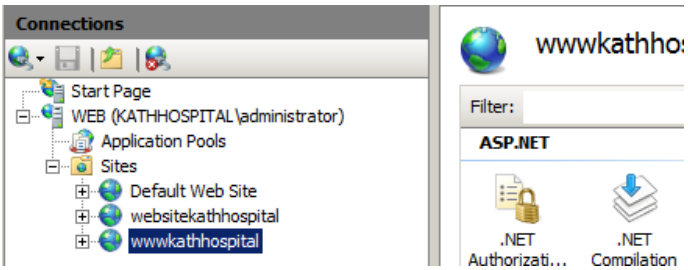


Figure 26 HTTP Redirection

5. Open HTTP Redirect feature (Figure 12)

Figure 27 HTTP Redirection

6. Select the check box Redirect requests to this destination give the destination as **WEBSITE.KATHHOSPITAL.COM** (Figure 13) → click Apply in the actions Pane

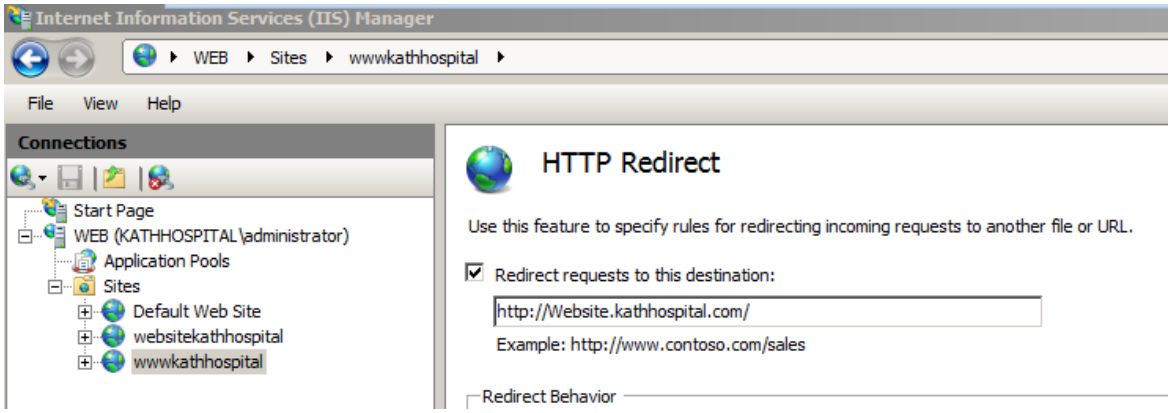


Figure 28 HTTP Redirection

FTP Publish

Kathmandu hospital allows clients to access public documents such as help files, enquiry forms, fee information form, public licenses etc. via their FTP site. Which is basically sharing files via web browser. To publish FTP site from web server which has already installed FTP server, following procedure is performed:

1. Open any drive and create a folder (Ex: FTP Dir.) → Open the folder and create some files (1.txt, 2.txt, 3.txt.) (Figure 14)

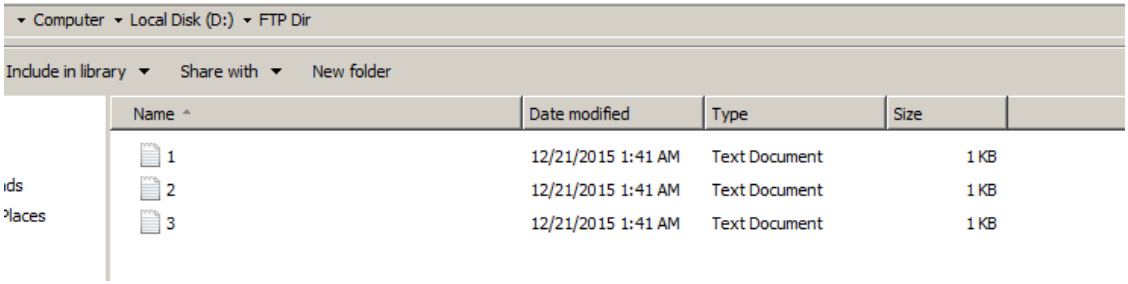


Figure 29 FTP Publishing

2. Select Start → Programs → Administrative Tools → Internet Information Services (IIS) Manager.
3. In the left pane of the Internet Information Services dialog box →Expand the server →Right click on Sites and select ADD FTP Site (Figure 15)

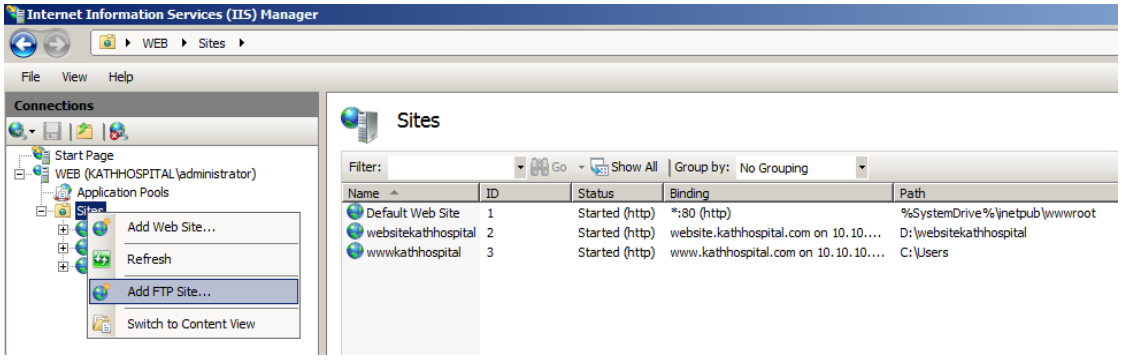


Figure 30 FTP Publishing

4. In Site Information screen, enter the FTP site name (**FTPSITE**) (Figure 16)

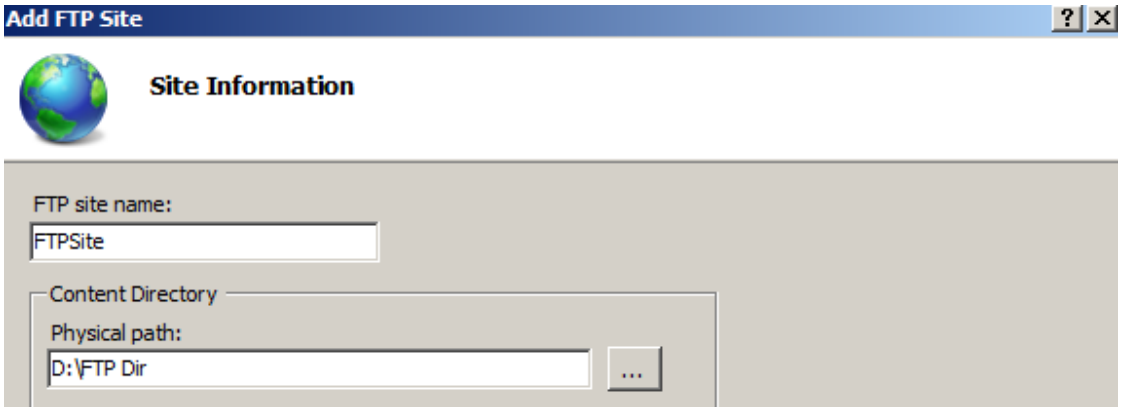


Figure 31 FTP Publishing

5. Enter the path to the home folder (Content Directory) (Figure 17)

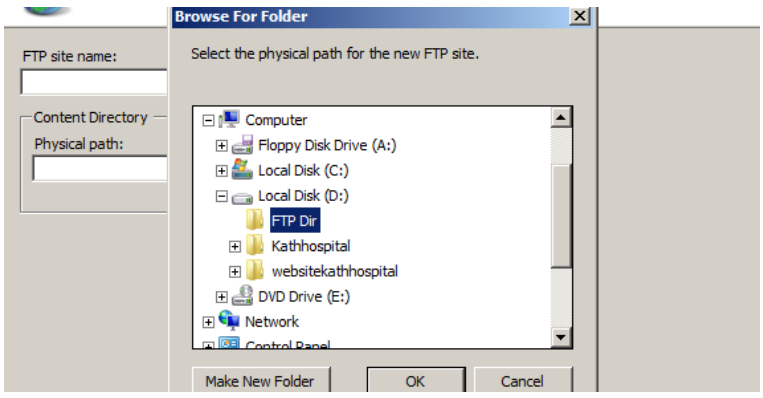


Figure 32 FTP Publishing

6. In the Bindings and SSL Settings dialog box select the IP address and port no. and select "NO SSL". (Figure 18)

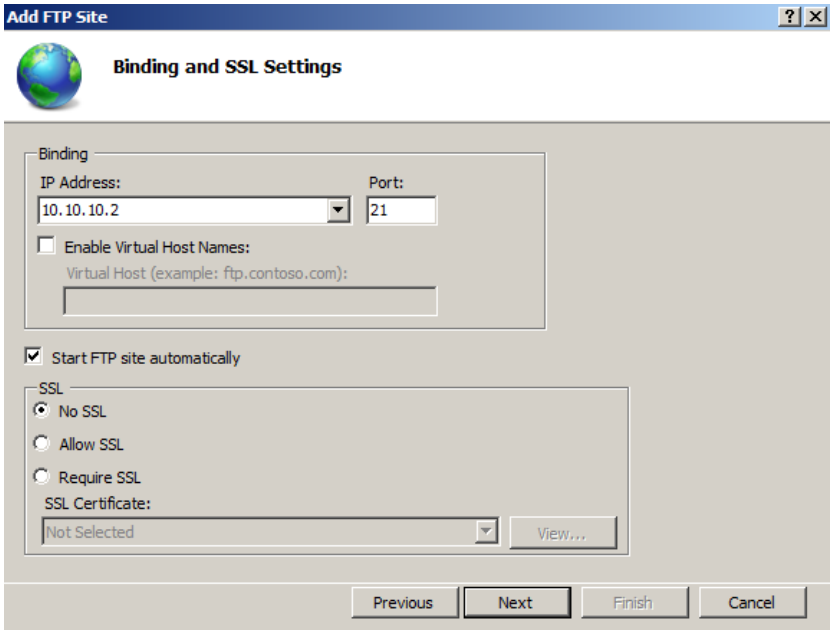


Figure 33

7. In Authentication and Authorization Information dialog box Check the box for Anonymous and Basic, Select All Anonymous users, Check the box for Read and Write (Figure 19)

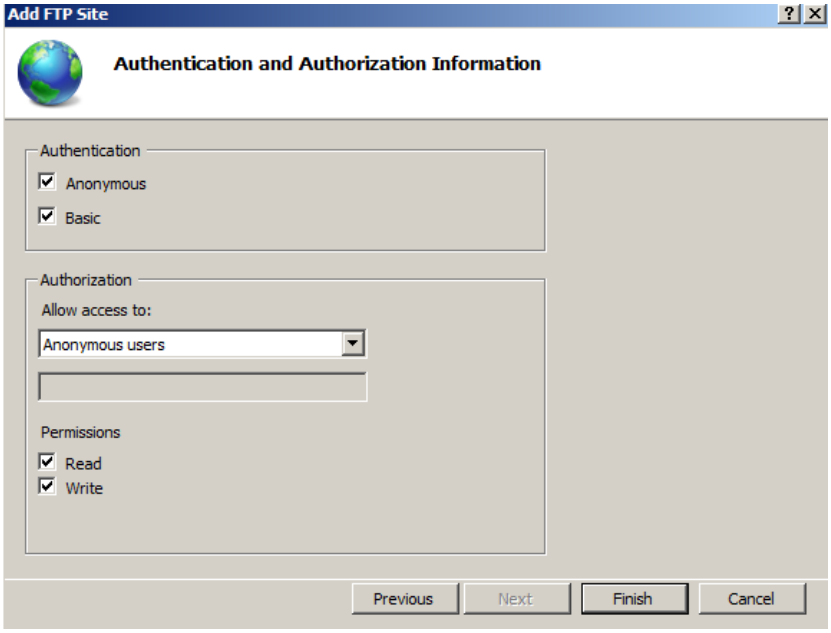


Figure 34 FTP Publishing

8. Click Finish. → Done

Verifying FTP publishing

1. Open web browser
2. Type address of the FTP in format (**ftp:// Address**)→ Press Enter (Figure 20)

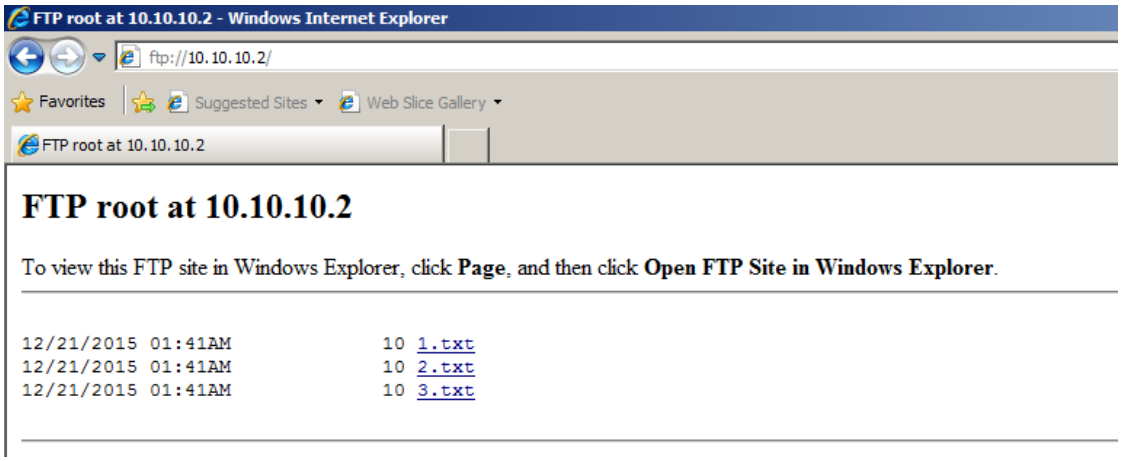


Figure 35 Verifying FTP Hosting

Web Application Publish

Kathmandu Hospital requires to publish both PHP based and ASP.NET based web application. PHP based Web application developed for hospital is more client oriented and ASP.NET based web application are more information management oriented. Internet server requires to support both ASP as well as PHP based web application. Required components for installing and publishing web applications are already configured during server implementation. Now following procedure is performed.

ASP.NET site publication

1. Login web server as administrator and open IIS
2. Add new website and provide Name (figure 21) and select physical path

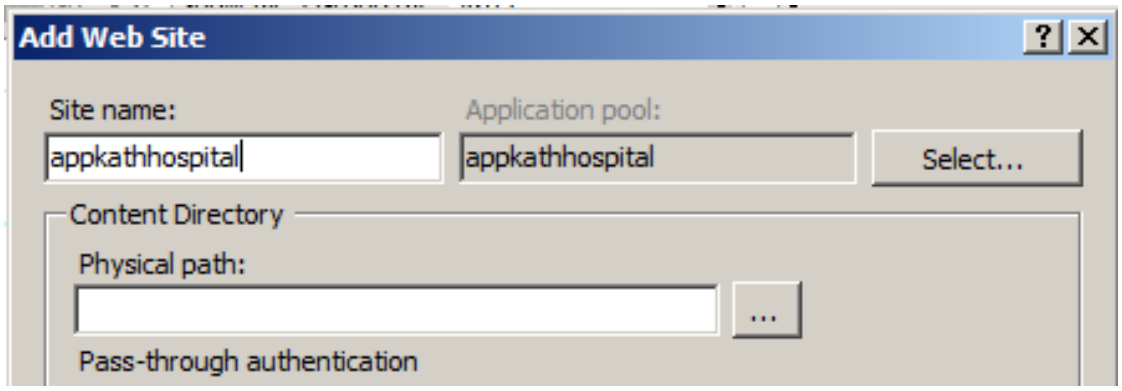


Figure 36 Asp.net publishing

3. Select IP address (**10.10.10.2**), port and provide host name (**app.kathhospital.com**) (figure 22)

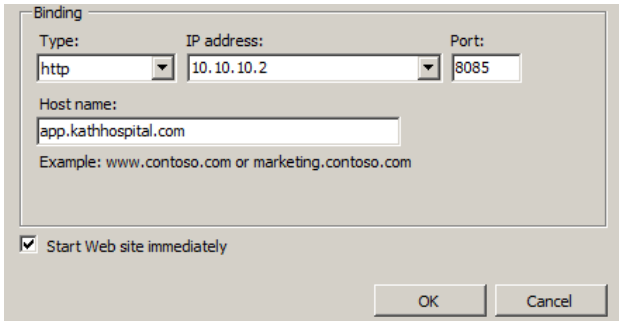


Figure 37 Asp.net publishing

4. From left panel select Application Pools→ select added website→ right click→ advanced setting
5. Provide .NET framework version for application pool (Figure 23)

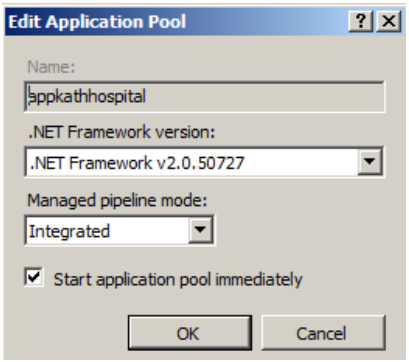


Figure 38 Asp.net publishing

6. Login DNS server as admin and Configure DNS for newly added website in DNS server (Figure 24)

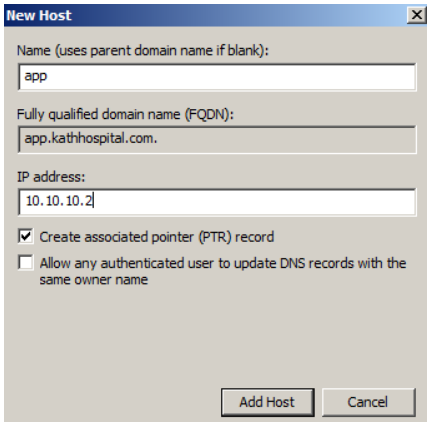


Figure 39 Asp.net publishing

7. Open Default document feature in IIS and Add default page to index.aspx (Figure 25)

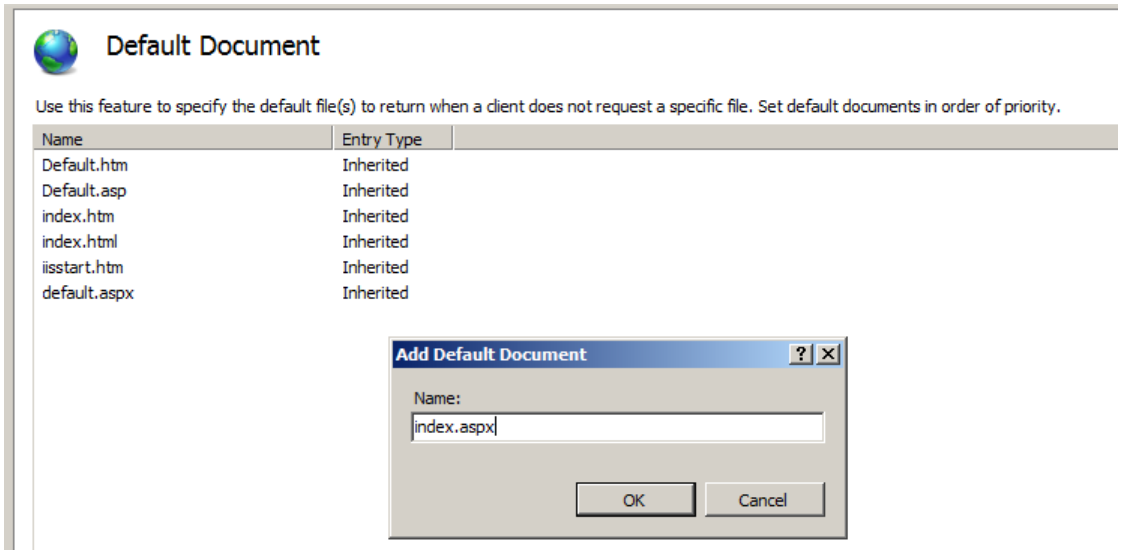


Figure 40 Asp.net publishing

Verify

1. To verify aps.net publishing open browser
2. Type hostname http://app.kathhospital.com/ press Enter (Figure 26)

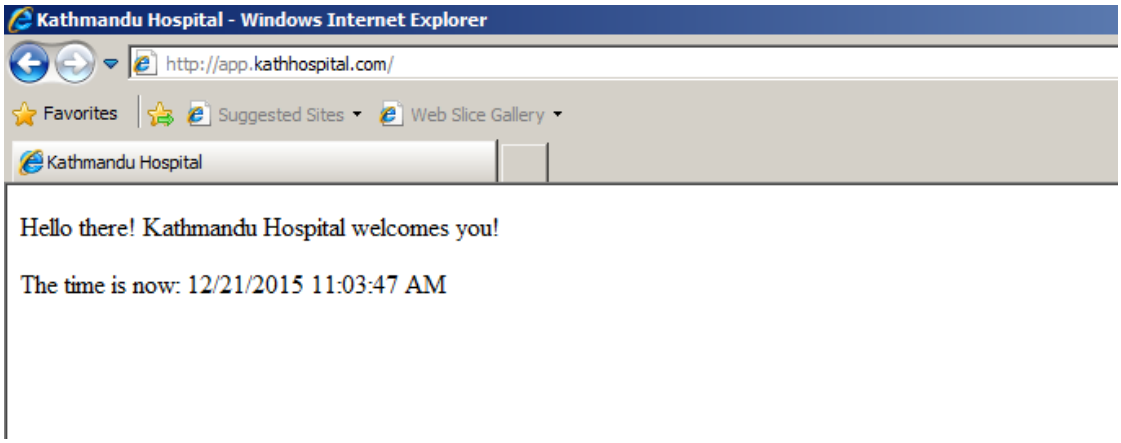


Figure 41 Verifying ASP.NET publication

IIS Configuration for PHP

First PHP is downloaded and extracted in web server. Then, Fast CGI configuration is done to work with PHP under the "FastCGI Settings" option. CGI is already installed during web development package installation in IIS web server.

1. Login web server as administrator
2. Select Start→Programs→Administrative Tools→Internet Information Services Manager.

3. From left panel Click on WEB (IIS Server) (Figure 27)

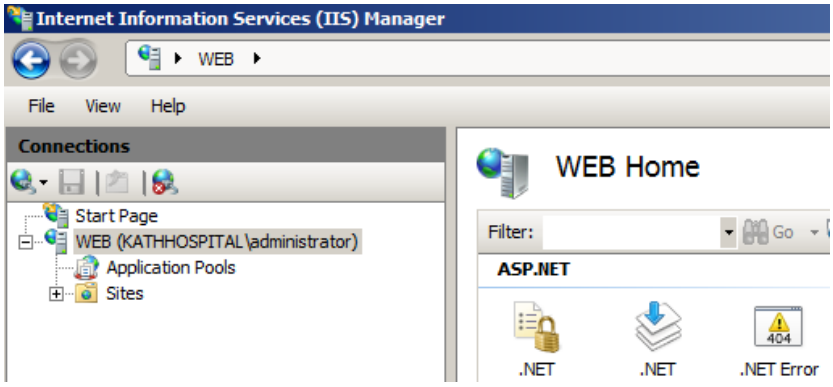


Figure 42IIS configuration for PHP

4. In the IIS section open the **Handler Mappings** feature (Figure 28)

Figure 43 IIS configuration for PHP

5. In the Actions panel click on **Add Module Mapping**

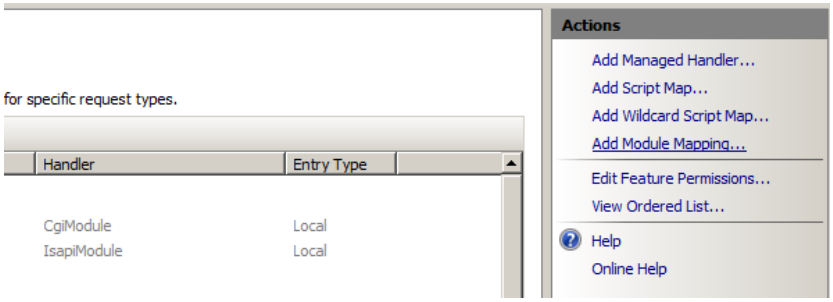


Figure 44 IIS configuration for PHP

6. In the "Add Module Mapping" dialog enter the following (Figure 30)
   - Request path: *.php
   - Module: FastCgiModule
   - Executable: C:\[Path to PHP installation]\php-cgi.exe

- Name: PHP

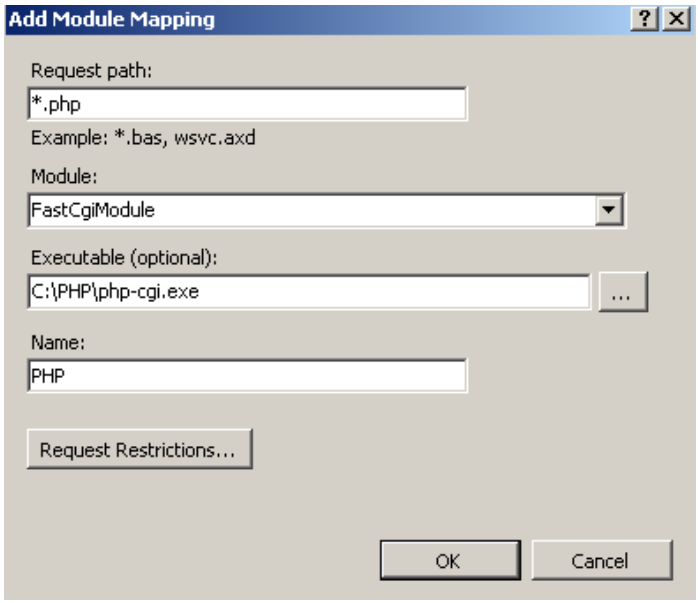


Figure 45 IIS configuration for PHP

7. Click **Request Restrictions** button → then configure the mapping to invoke handler only if request is mapped to a file or a folder
8. Click OK on all the dialogs to save the configuration
9. Click yes in add module mapping configuration (Figure 31)

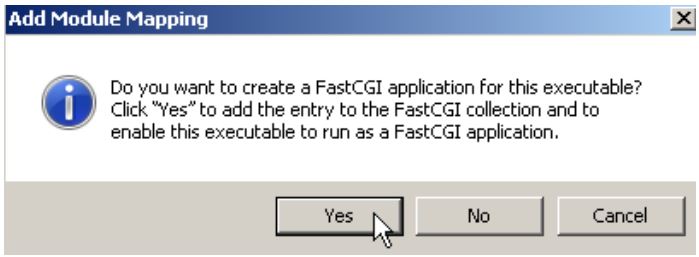


Figure 46 IIS configuration for PHP

10. From left panel Click on WEB (IIS Server)
11. Click on FastCGI Settings (Figure 32)→ from setting screen edit PHP FasgCGI setting.

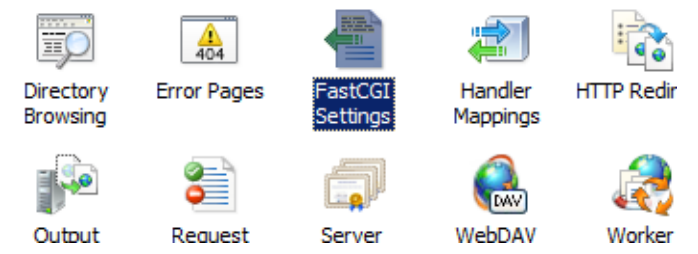


Figure 47 IIS configuration for PHP

12. Set the path to the 'php-cgi.exe' executable located in the folder where you extracted the PHP Windows binaries. Additionally, change the "InstanceMaxRequests" to a value higher than the default (i.e. 10000). Under the "EnvironmentVariables" setting, click the ellipses button to configure additional options. (Figure 33)
13. Add a new variable named "PHP_MAX_REQUESTS" and set the value to the same amount as the "InstanceMaxRequests" setting above (i.e. 10000). (Figure 34)
14. Apply all settings until you get back to the primary IIS Manager screen.
15. Apply all your changes, close and restart IIS to make sure the new settings take effect. (Figure 35)

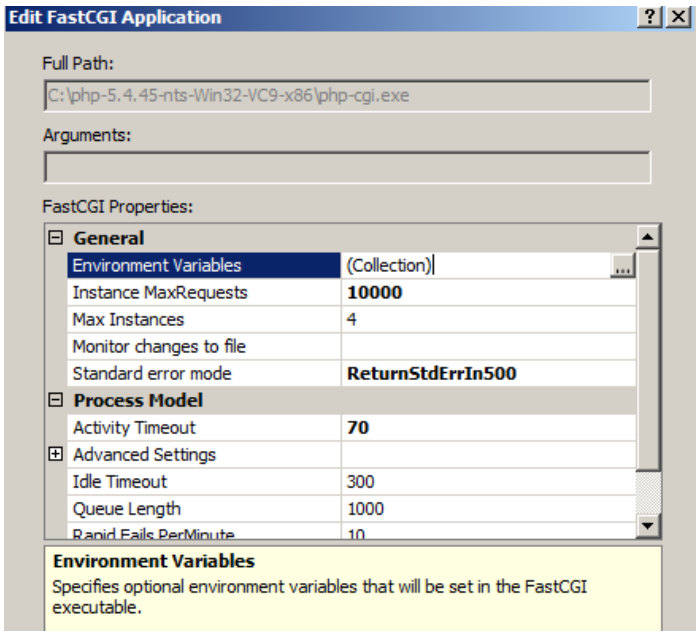


Figure 48 IIS configuration for PHP

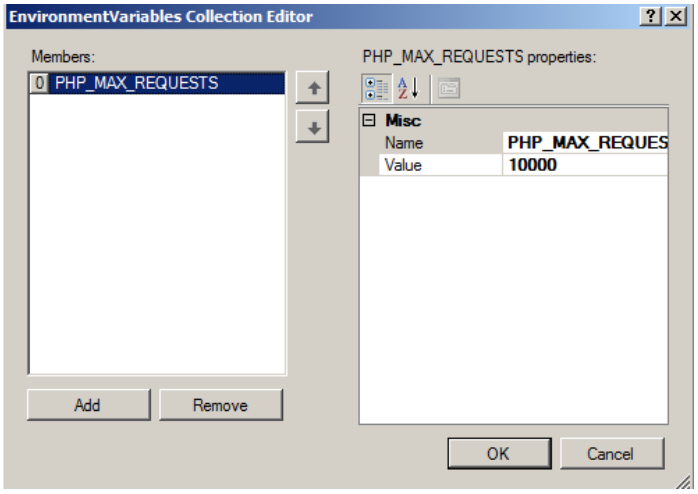


Figure 49 IIS configuration for PHP

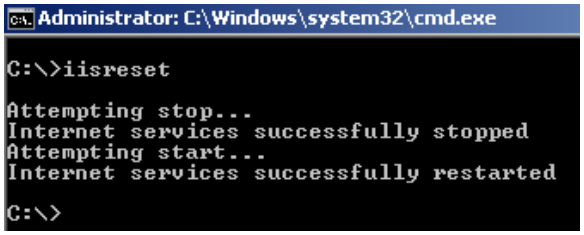


Figure 50 IIS configuration for PHP

Verifying

To verify PHP configuration of IIS, first a PHP file is created which is scripted to display all information of installed PHP. Following process is performed to verify PHP installation.

1. Create a directory →index.php → php script to display php version info (Figure 36)

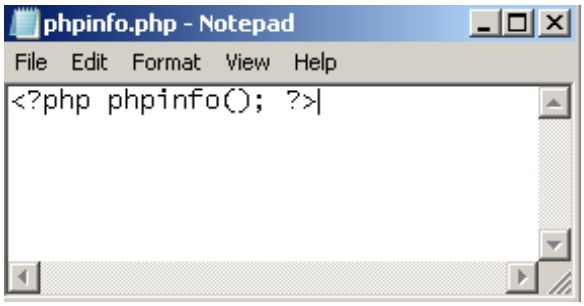


Figure 51 Verifying PHP support

2. Add new website and provide site name, physical path and host name for the PHP web application(Figure 37)

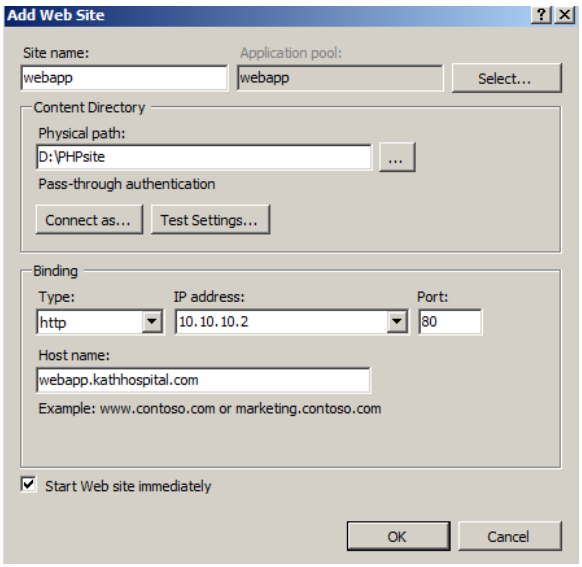


Figure 52 Verifying PHP support

3. Go to DNS server and add new host for newly added web application (figure 38)

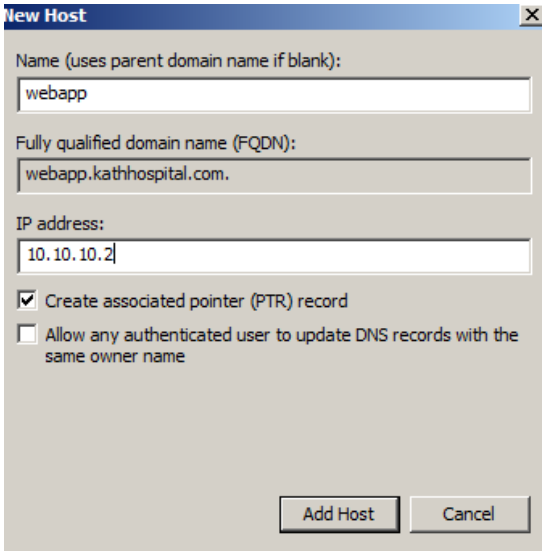


Figure 53 Verifying PHP support

4. Open web browser→ in address bar provide hostname of the application and press enter→
5. PHP version is displayed successful which verifies support for PHP. (Figure 39)

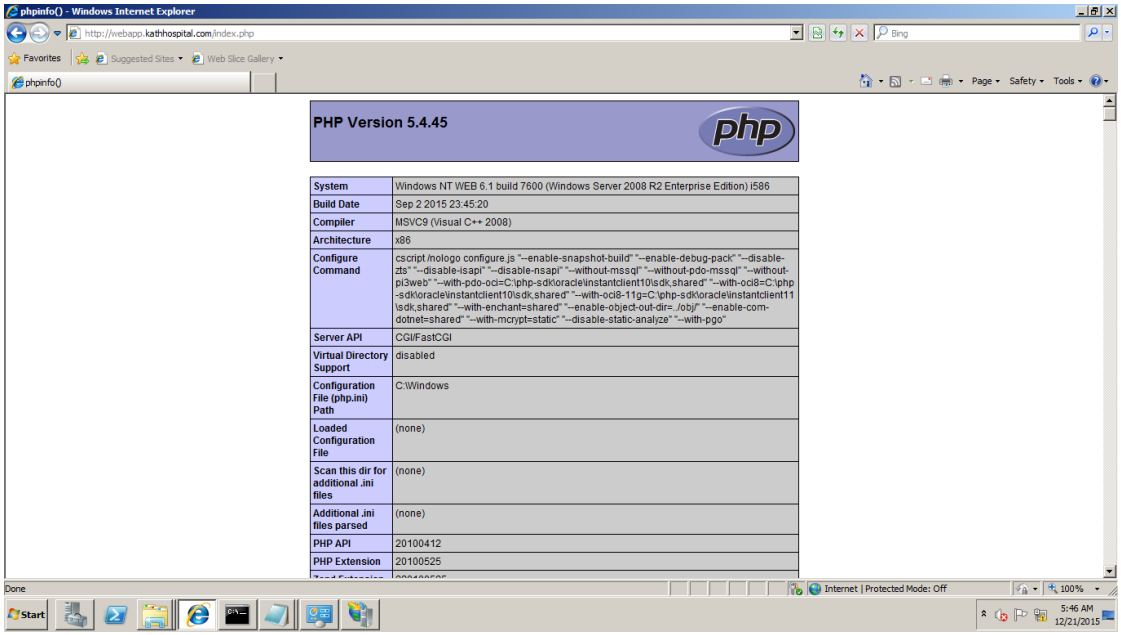


Figure 54 Verifying PHP support

Summary

Website and services are installed and managed in this document. Website was published and DNS configuration is done. ASP.NET based web application is also published. Web application is now capable of hosting PHP based web application which is documented in this paper. System now can take advantage of the multitude of PHP based applications available as well as develop and deploy its own.

Task10

Implement secure network access to meet a given requirement. [4.2]

Introduction

Security measurements are a major concern for growing organization like Kathmandu Hospital. Internet servers in the network contains information about patients, doctors, medicine etc. If there are vulnerabilities in the system, it can allow hackers to get into the system to jeopardize the internet services and steal or destroy information. This can cause lose in services, lose is customer trust and can even cause serious issues like stealing critical information. Beside hackers and unauthorized access the internet services, there is also security threats such as viruses, Trojans etc. To reduce such threats and provide secure network, various security measurements are required to be implemented. This paper documents implementation of security measurements such as anti-virus, FTP security, Website security and IP address restriction etc. in built inter-networking servers.

IP address restriction Configuration

IP address restriction is great tool to allow or deny particular IP address from access the web application/website. To implement IP address restriction following procedure is performed:

1. Login Web server as administrator
2. Open IIS console (Select Start→Programs→Administrative Tools→Internet Information Services Manager)
3. From the left panel expand WEB\Administrator→Click on website on which rule is required to be implemented (Figure 1)

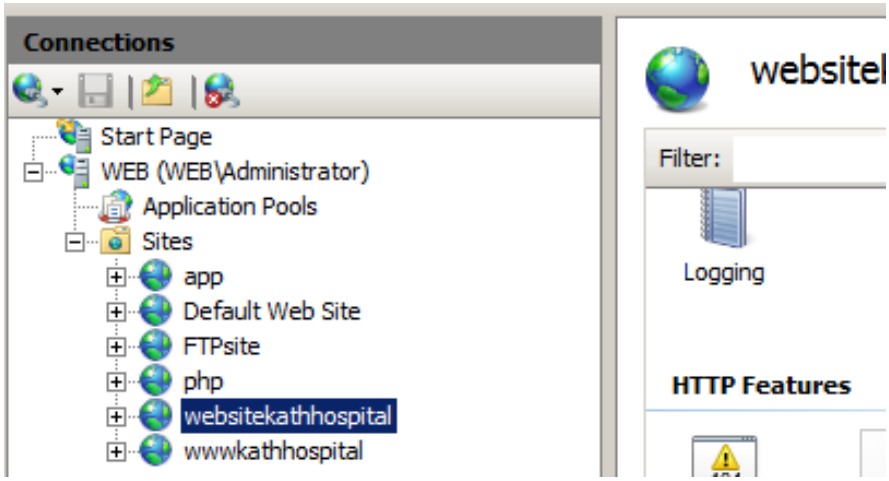


Figure 55 IP address restriction

4. From feature view click on **IP Address and Domain Restriction (**Figure 2**)**

Figure 56 IP address restriction

5. Now in the IP address and domain restriction page→From right panel click on add new Deny Entry to block the resource with particular IP (figure 3)

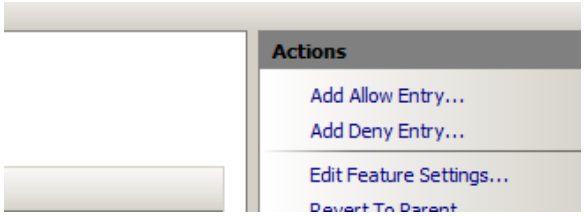


Figure 57 IP address restriction

6. In add deny restriction rule window→Provide IP address (10.10.10.100) to deny access (figure 4)

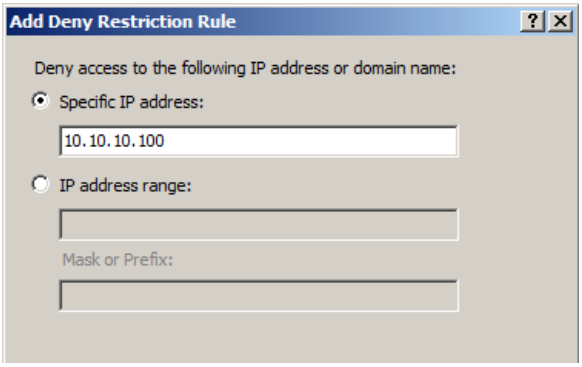


Figure 58 IP Address restriction

7. To verify the configuration try accessing website from denied IP address→Access is denied (Figure 5) Done

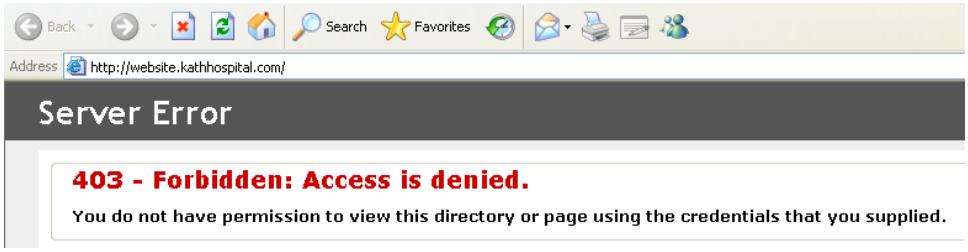


Figure 59 IP address restriction

Basic FTP Security

By default, installed and managed FTP sites in Kathmandu Hospital network are allowed to access without any authentication. To improve FTP security, basic security is implemented which requires client to go through authentication before viewing contents. This allows administrator to monitor client's access to FTP site. To implement basic security, these procedures are followed:

1. Login Web server as administrator
2. Open IIS console (Select Start→Programs→Administrative Tools→Internet Information Services Manager)
3. From the left panel expand WEB\Administrator→Click on FTP site on which rule is required to be implemented (Figure 6)

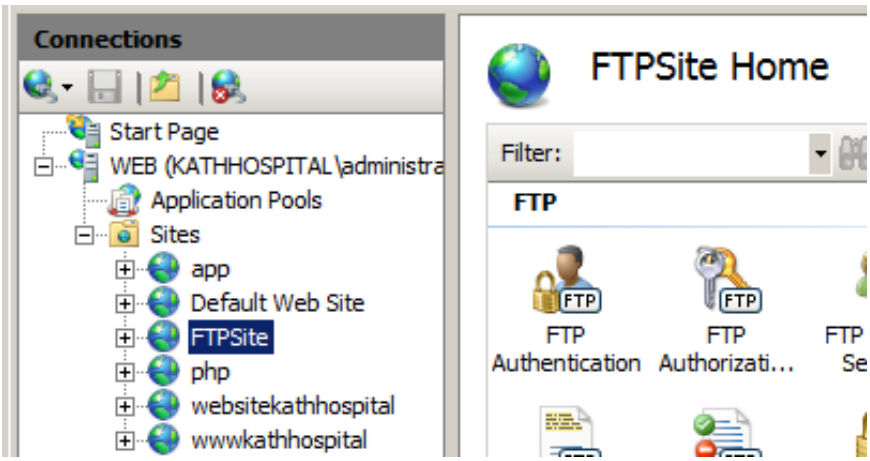


Figure 60 Basic FTP security

4. From feature view →Choose FTP authorization

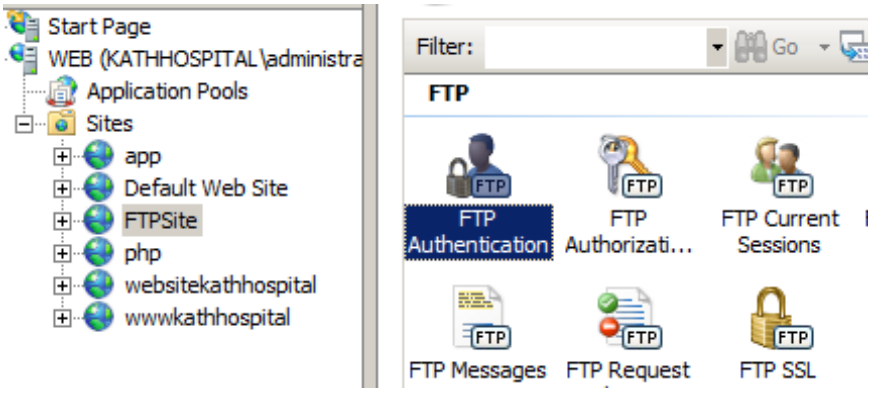


Figure 61 Basic FTP security

5. Enable Basic authorization and disable anonymous authorization (Figure 8)

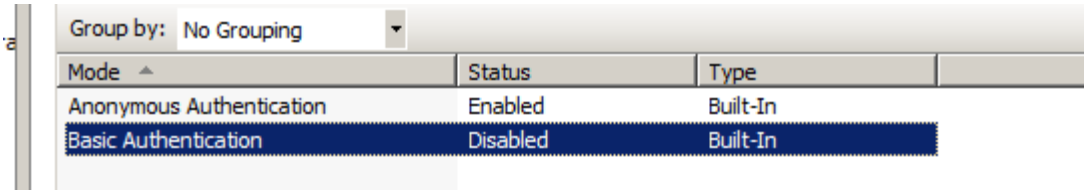


Figure 62 Basic FTP security

6. To verify the basic FTP security, access the FTP server from any client computer → Instead of allowing access to FTP it demands FTP server authentication→ Provide valid username and password (figure 9)

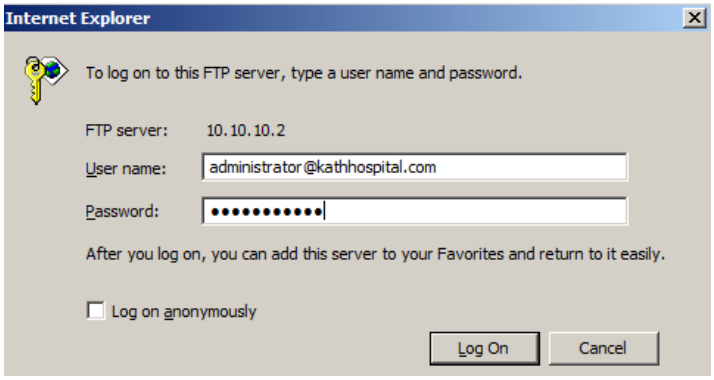


Figure 63 Basic FTP security

7. After valid authentication FTP site is accessible (Figure 10)

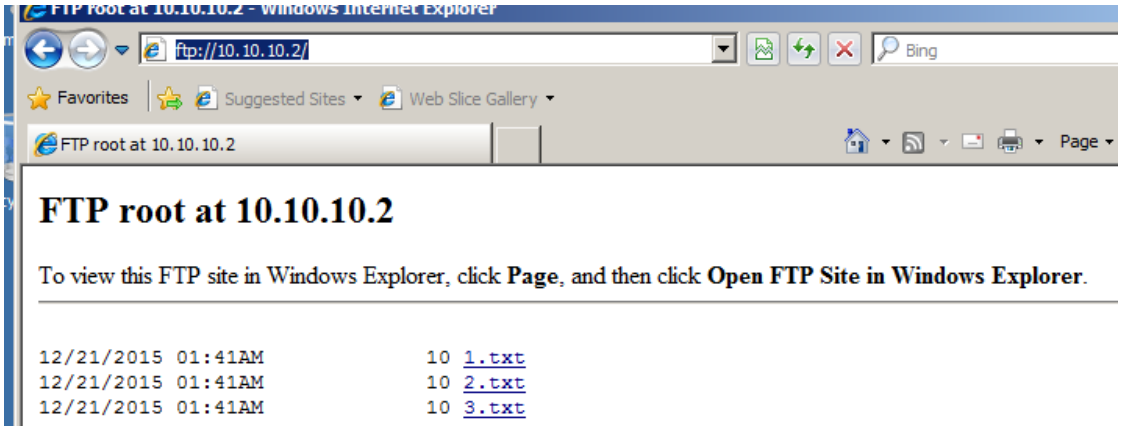


Figure 64 Basic FTP security

Access Control and File Permission

With basic FTP security is already configured, implementing Access Control and File Permission is great tool to limit user's ability of accessing the file, directory. With access control, users ability to read, write, modify the file can be configured. This allows to ensure security of files. For example, web user should not able to modify or add documents in FTP directory. This can be

configured easily via access control. Procedures performed during implementation of access control is documented below.

1. Locate the FTP directory → Right click and go to properties
2. In Directory Properties go to Security Tab (Figure 11)

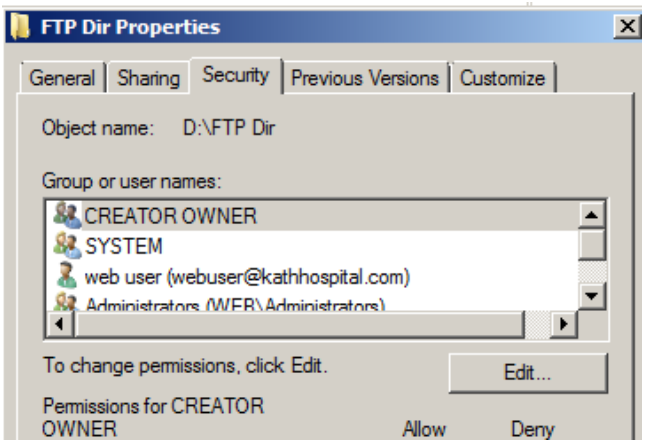


Figure 65 Access Control and File Permission on FTP Directory

3. Click on Edit button and add Web user (webuser@kathhospital.com) → deny write ability form permission for web user panel (Figure 12)→ Apply → Ok

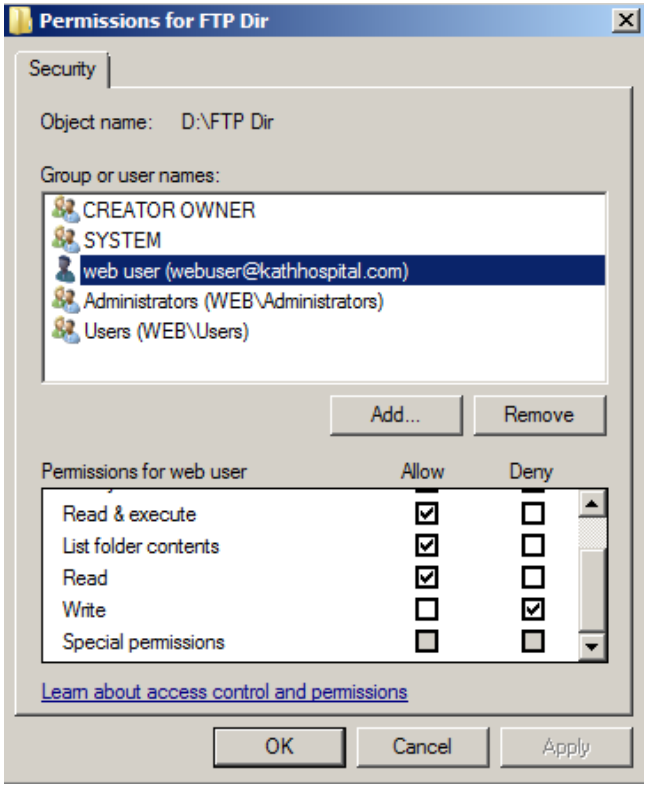


Figure 66 Access Control and File Permission on FTP Directory

4. No to verify Access control security implementation → Browse the FTP using web user username (webuser@kathhospital.com) and password
5. Try deleting content from FTP directory → 550 Access is denied error should pop up blocking deleting the content (Figure 13) → Done

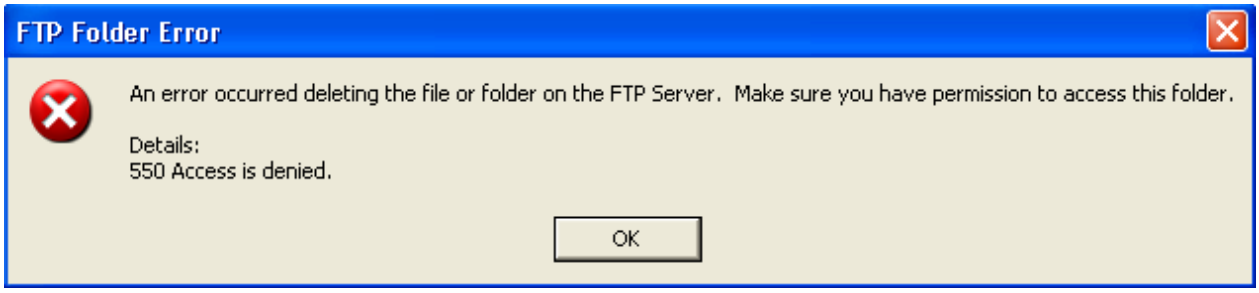


Figure 67 Access Control and File Permission on FTP Directory

Website Security

Basic Authentication

Like FTP basic security, basic security for website is also implemented to ensure authentication and authorization before website access. To implement basic website security following procedure is performed:

1. Login Web server as administrator
2. Open IIS console (Select Start→Programs→Administrative Tools→Internet Information Services Manager)
3. From the left panel expand WEB\Administrator→Click on website on which rule is required to be implemented (Figure 14)

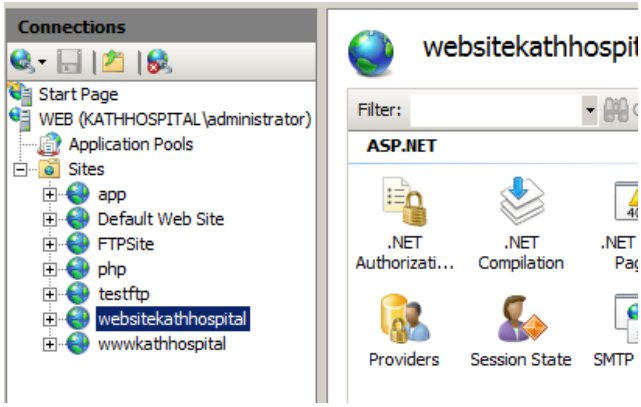


Figure 68 Website basic security

4. From feature view click on Authentication (Figure 15)

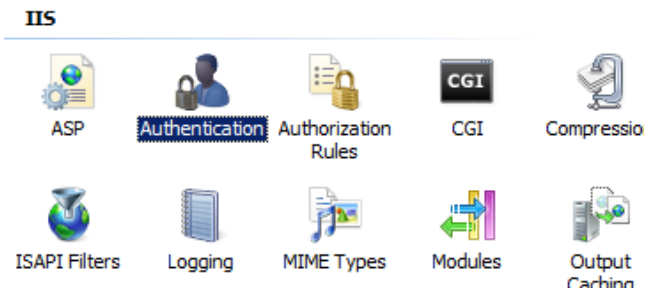
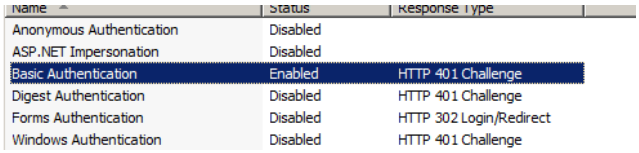


Figure 69 Website basic security

5. From list of authentication methodologies enable basic authentication and disable anonymous authentication (Figure 16)



Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Enabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

Figure 70 Website basic security

6. To verify basic windows security browse website from any member computer → instead of opening website, it should ask for authentication (provide username and password) (Figure 17)

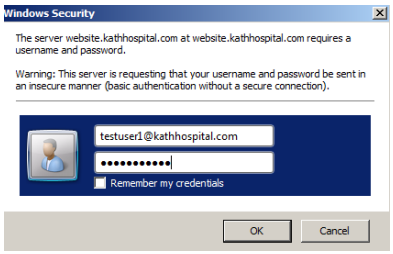


Figure 71 Website basic security

7. Once valid username and password is provided, it should open website.kathhospital.com (figure 18)

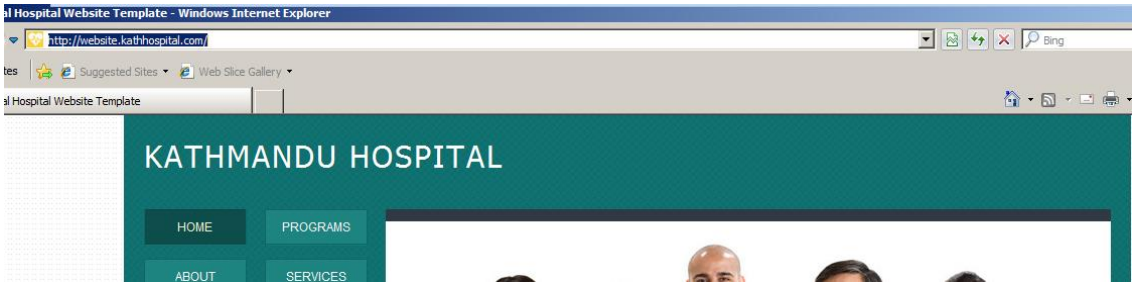


Figure 72 Website basic security

HTTPS via Self-Signed Certificate Implementation

To implement HTTPS website to provide web security, following procedure is implemented.

1. Open IIS manager (run->inetmgr)
2. Click on server node in left panel from the workspace and double click on server certificate (Figure 19)

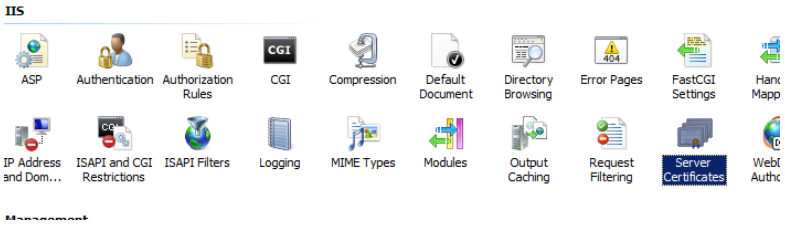


Figure 73 Self Signed Certificate Implementation

3. Click on create self-signed certificate(A box will open) (Figure 20)

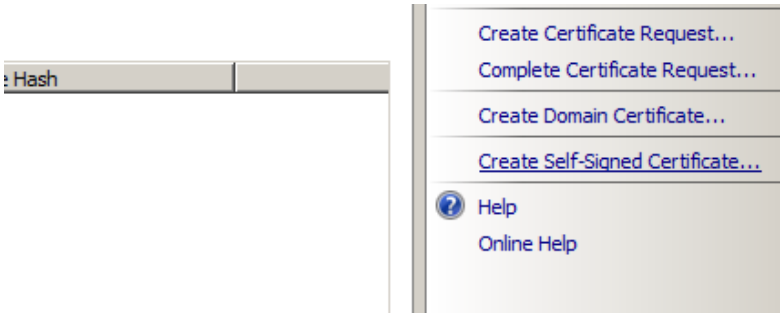


Figure 74 Self Signed Certificate Implementation

4. Type the name of certificate authority e.g. SELFSIGNEDCERTIFICATE, Click on ok (Figure 21)

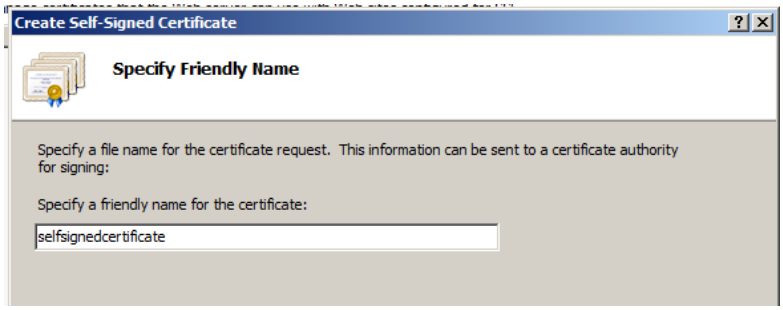


Figure 75 Self Signed Certificate Implementation

5. Select the website that one has published from website node → right click edit bindings by right cl(Figure 22)

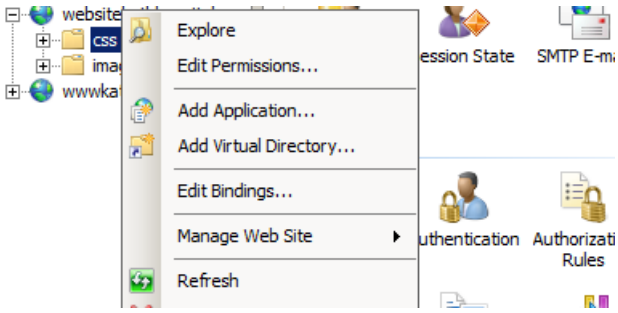


Figure 76 Self Signed Certificate Implementation

6. Click on add, select HTTPS type, select IP address, port no(443) → Select SSL certificate just created (Figure 23)

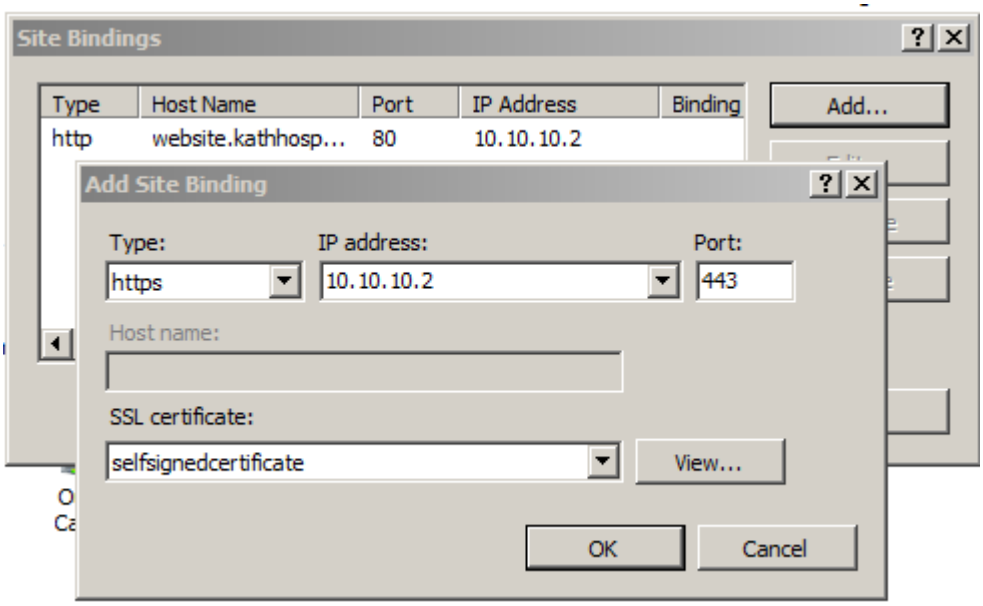


Figure 77 Self Signed Certificate Implementation

7. Now, browse website with https protocol (There might be certificate error of certificate trust, that is ok continue) (Figure 24)

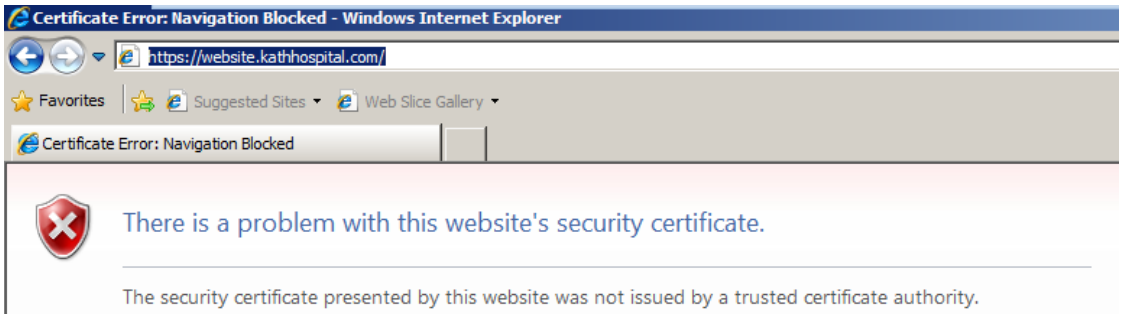


Figure 78 Self Signed Certificate Implementation

8. Click on certificate error icon, click on view certificate and ensure the identity on a remote computer (Figure 25,26)

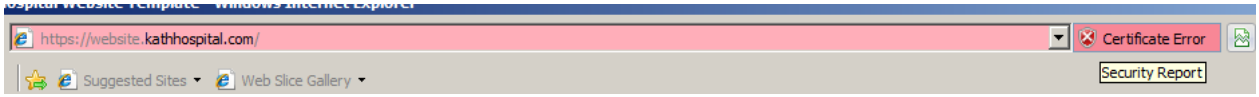


Figure 79 Self Signed Certificate Implementation

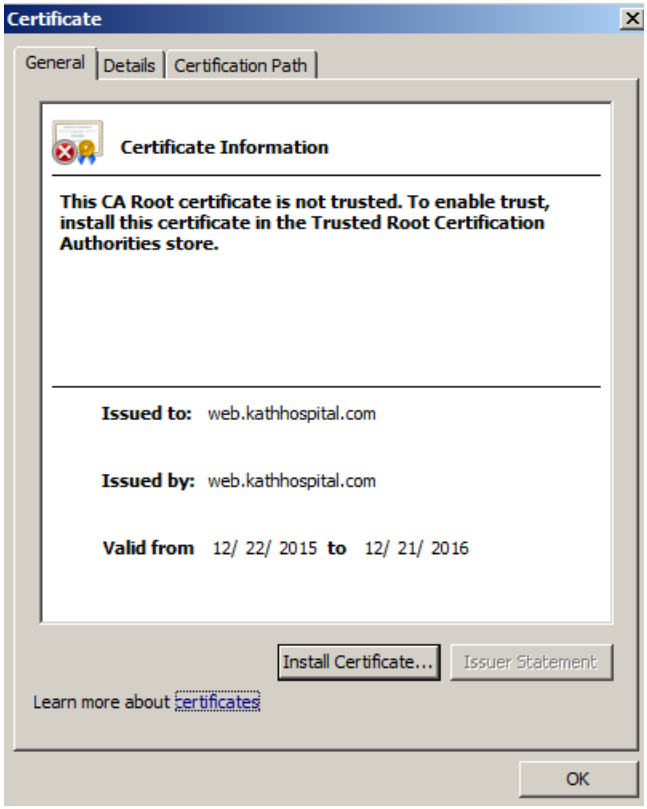


Figure 80 Self Signed Certificate Implementation

9. Click on Install Certificates and place certificates in trusted Root folder (Figure 27)

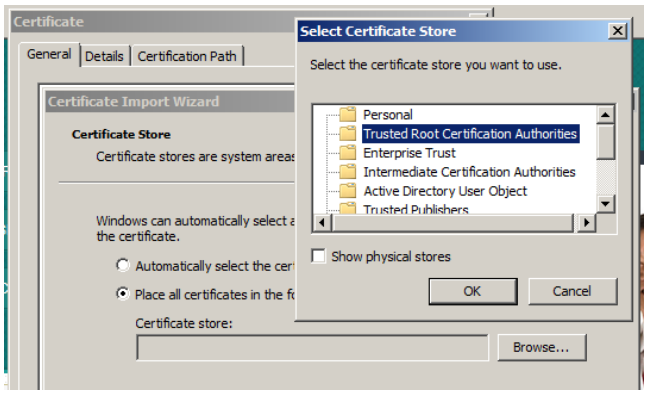


Figure 81 Self Signed Certificate Implementation

10. Finally, install certificate by clicking yes (Figure 28)

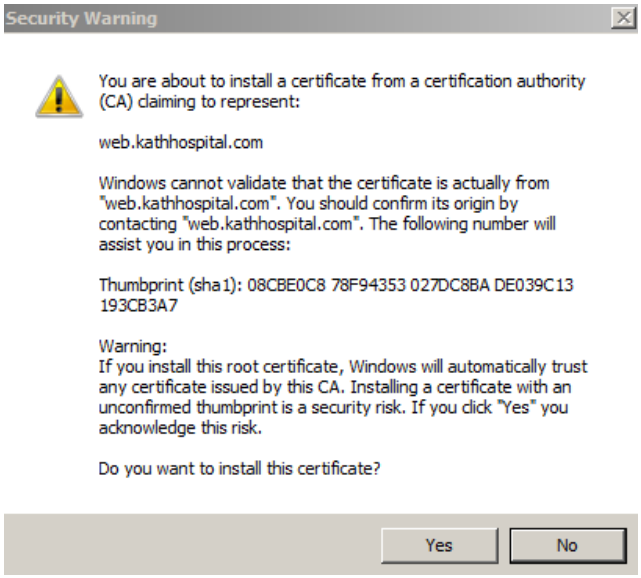


Figure 82 Self Signed Certificate Implementation

Anti-virus

Anti-virus helps to prevent attack on server from viruses, adware etc. It also has firewall system to provide added layer of firewall protection on already available windows and FTP firewall support. Avira Anti-virus server is utilized for developed Internet server environment. To implement Avira Anti-virus server following procedures are performed:

1. Visit Avira's official website and purchase Avira anti-virus for windows server. (figure 29)

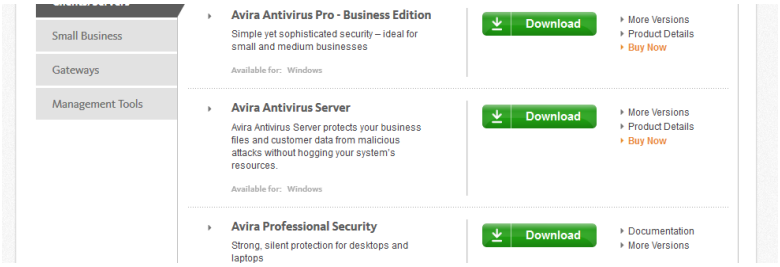


Figure 83 Anti-virus installation and management

2. Locate and double click on downloaded anti-virus (Figure 30)

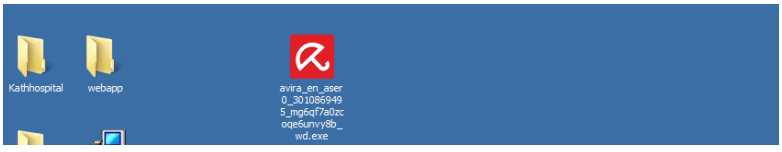


Figure 84 Anti-virus installation and management

3. Let the installation finish. (figure 31), (Figure 32)

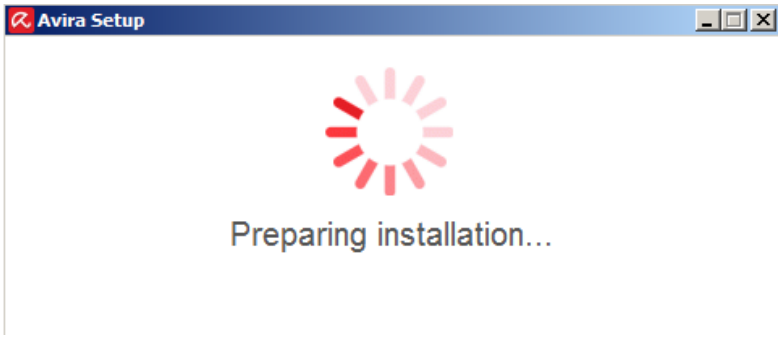


Figure 85 Anti-virus installation and management

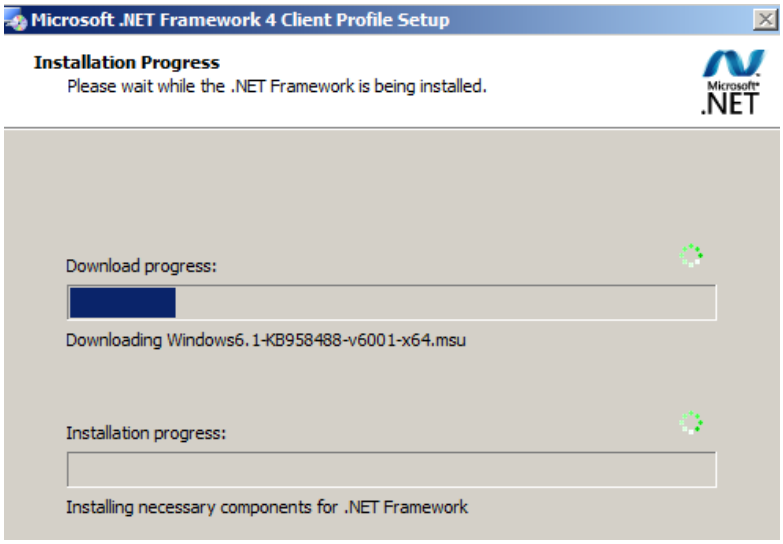


Figure 86 Anti-virus installation and management

4. Download anti-virus server package and browser safety package (Figure 33)

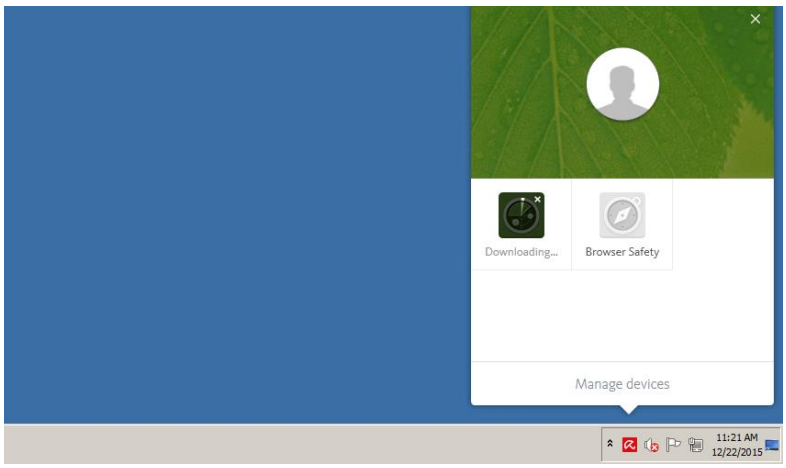


Figure 87 Anti-virus installation and management

5. Once download finish load anti-virus (Figure 34)

6. Update the definition file
7. Scan the system→ Done

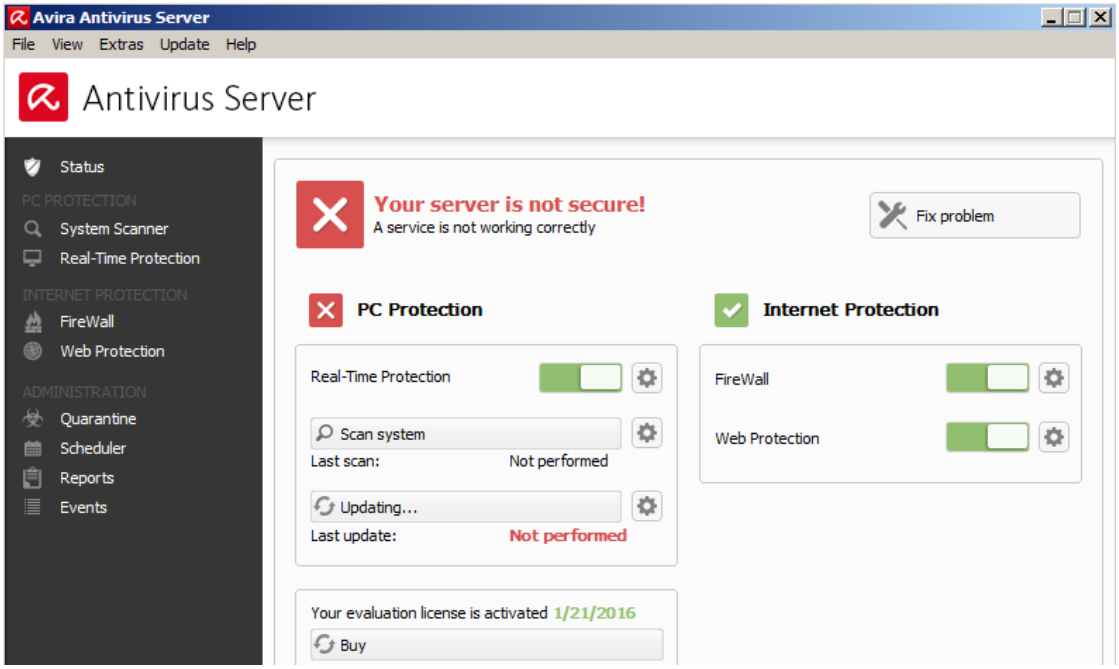


Figure 88 Anti-virus installation and management

Secure communication: Windows Firewall

Windows firewall is utilized to filter incoming and outgoing packets. In current inter-networking environment windows firewall is utilized for opening and closing ports as per requirements. Firewall is also utilized to secure connection between client and server. Following procedure is implemented.

1. Log onto the server as administrator
2. Start→ Administrative tools→ Windows Firewall and avenge security
3. Connection Security rule→ Right click→ New rule (Figure 35)

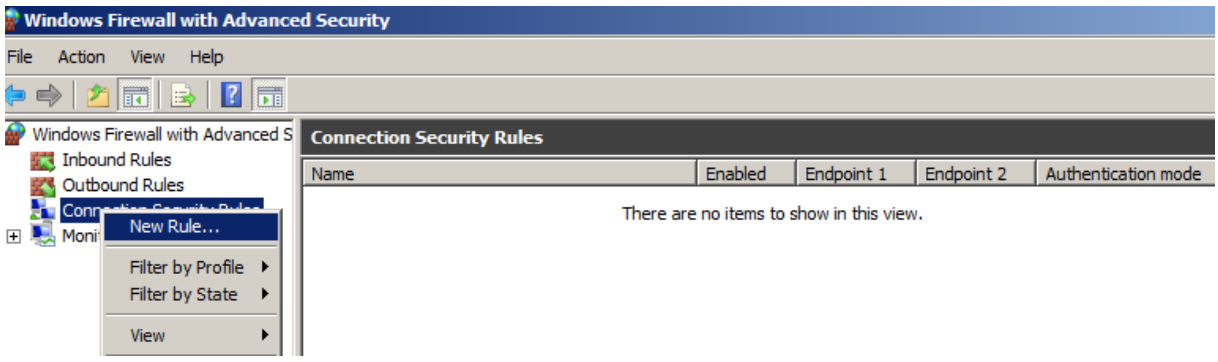


Figure 89 Secure connection configuration

4. Select Custom→ Next(Figure 36)

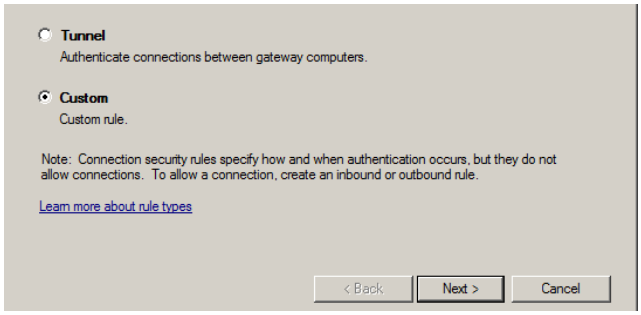


Figure 90 Secure connection configuration

5. Add end point 1 and 2 IP addresses→ Next (Figure 37)

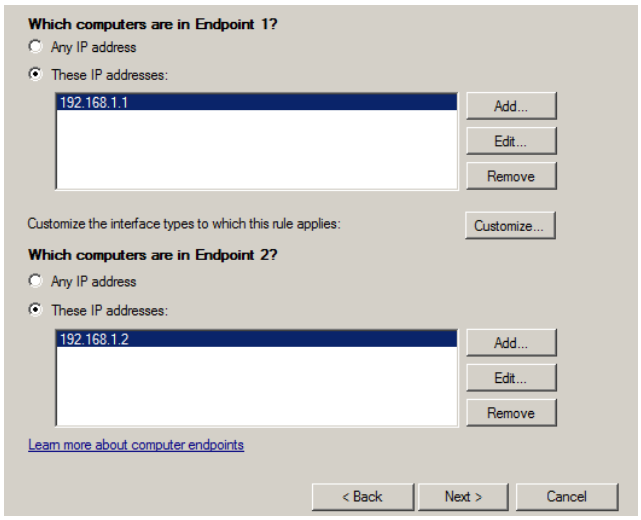


Figure 91 Secure connection configuration

6. Check on Require authentication for inbound and outbound connection→ Next (Figure 38)

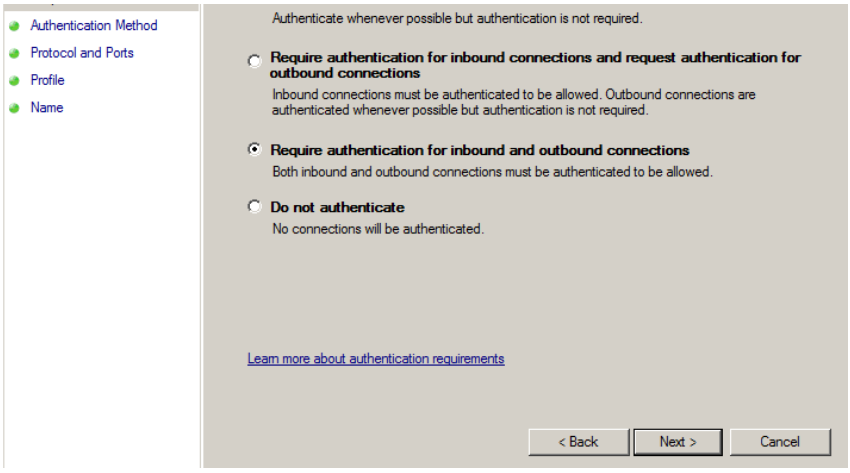


Figure 92 Secure connection configuration

7. In the Authentication Method box, select Advanced, and then click Customize → Next (Figure 39)

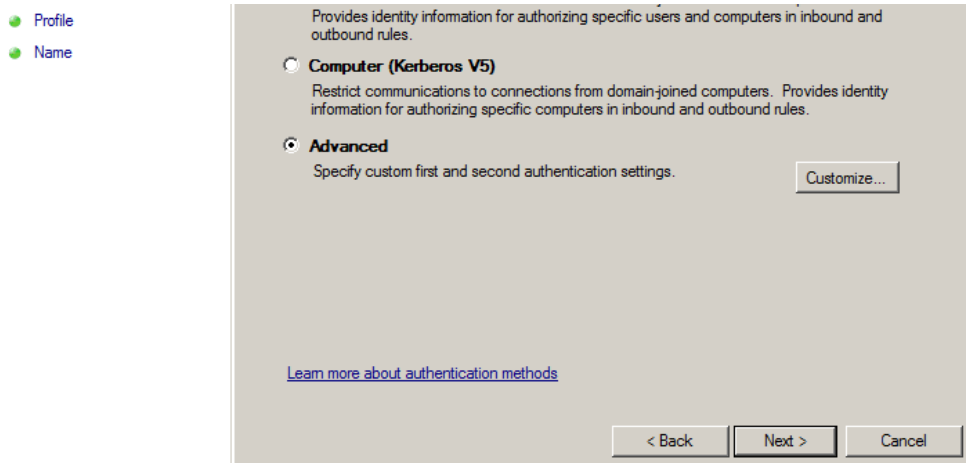


Figure 93 Secure connection configuration

8. In First Authentication Method, click Add.
9. select Computer certificate from this certificate authority→ brows certificate→ Click ok until method is selected→ Next (Figure 40)

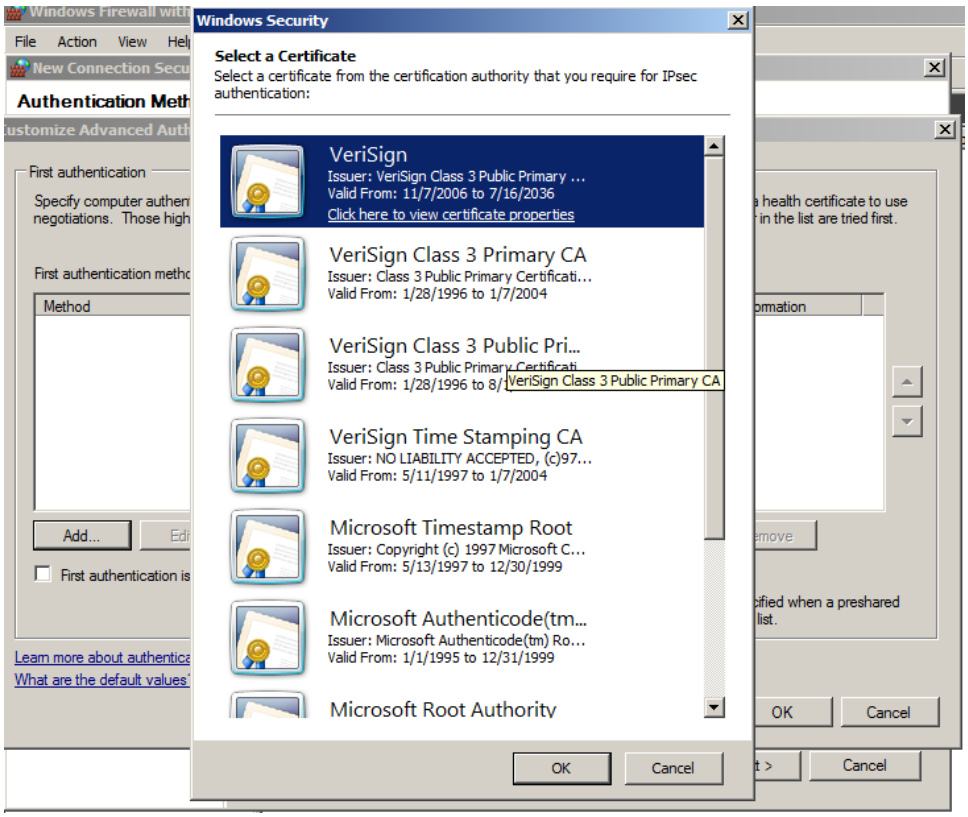


Figure 94 Secure connection configuration

10. Select ports and protocols to apply the rule→ Next (Figure 41)

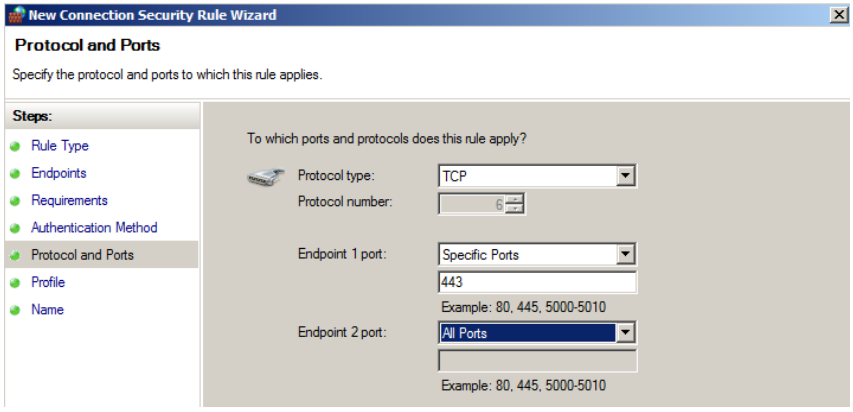


Figure 95 Secure connection configuration

11. Leave the all box checked→ Next (Figure 42)

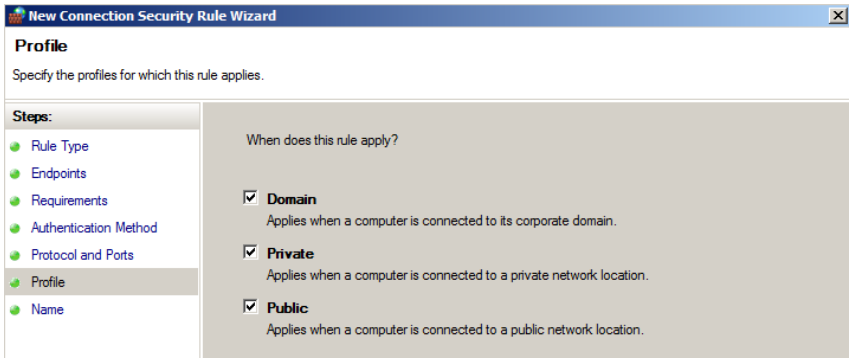


Figure 96 Secure connection configuration

12. Name your rule, and then click Finish.

13. Repeat same procedure in client PC to secure the connection.

Task11

Monitor and troubleshoot an internet server services and critically evaluate the performance of internet server. [4.3, 4.4, M3]

Introduction

Planning, implementation and testing of Internet server and supporting server components to provide required Internet services has already been completed. Now it is essential for administrator to perform continuous monitoring of Internet server. Internet server monitoring describes keeping track of every possible Internet server components including hardware and software and also keeping track of Internet services. For example, monitoring allows to ensure status of DNS server and report if there is any issue. Server monitoring also enables administrator to analyze load status, memory usage, analyze traffic and check disk space status.

Some top monitoring tools are reliable option to ensure server security and performance. They include additional tools such as altering capabilities, performance benchmarking etc. which helps administrator to analyze the state of implemented intern-networking environment. Benchmarking of internet server components such as processor, memory and network will assist analyzing the decision of managing the system. Benchmarking is widely used technology to compare and analyze performance of the system and improve them. Key factors that may affect the performance of Internet server such as hardware configuration and software configurations are evaluated using performance benchmarking. This paper documents monitoring and identifying possible problems and the server while also providing troubleshooting for the identified problem. This paper also utilizes tools and technology to prepare benchmarking of various components and provide recommendation for performance improvement.

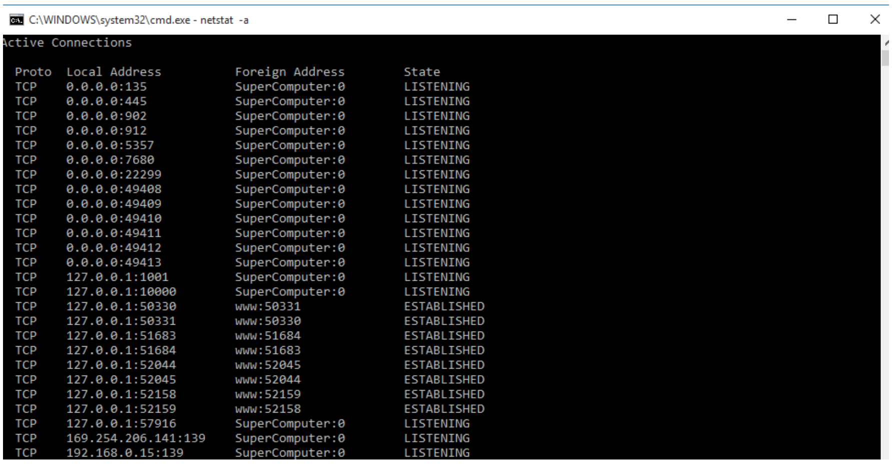
Basic Monitoring Techniques

ICMP tool

ICMP (Internet Control Message Protocol) is great tool for diagnosing problem and reporting error. It is essential mechanism for any network environment implementation. It is fast, easy and free tool to monitor health of Internet service. ICMP can be useful for:

- Availability of host computers/resources
- Probable reason for the communication problem

Tracing route using ICMP allows to identify hops between destination and source. This allows to analyze probable problem. It also allows to monitor active connections (Figure 1) to identify any suspicious connection.




```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            SuperComputer:0        LISTENING
  TCP    0.0.0.0:445            SuperComputer:0        LISTENING
  TCP    0.0.0.0:902            SuperComputer:0        LISTENING
  TCP    0.0.0.0:912            SuperComputer:0        LISTENING
  TCP    0.0.0.0:5357           SuperComputer:0        LISTENING
  TCP    0.0.0.0:7680           SuperComputer:0        LISTENING
  TCP    0.0.0.0:22299          SuperComputer:0        LISTENING
  TCP    0.0.0.0:49408          SuperComputer:0        LISTENING
  TCP    0.0.0.0:49409          SuperComputer:0        LISTENING
  TCP    0.0.0.0:49410          SuperComputer:0        LISTENING
  TCP    0.0.0.0:49411          SuperComputer:0        LISTENING
  TCP    0.0.0.0:49412          SuperComputer:0        LISTENING
  TCP    0.0.0.0:49413          SuperComputer:0        LISTENING
  TCP    127.0.0.1:1001         SuperComputer:0        LISTENING
  TCP    127.0.0.1:10000        SuperComputer:0        LISTENING
  TCP    127.0.0.1:50330        www:50331              ESTABLISHED
  TCP    127.0.0.1:50331        www:50330              ESTABLISHED
  TCP    127.0.0.1:51683        www:51684              ESTABLISHED
  TCP    127.0.0.1:51684        www:51683              ESTABLISHED
  TCP    127.0.0.1:52044        www:52045              ESTABLISHED
  TCP    127.0.0.1:52045        www:52044              ESTABLISHED
  TCP    127.0.0.1:52158        www:52159              ESTABLISHED
  TCP    127.0.0.1:52159        www:52158              ESTABLISHED
  TCP    127.0.0.1:57916        SuperComputer:0        LISTENING
  TCP    169.254.206.141:139    SuperComputer:0        LISTENING
  TCP    192.168.0.15:139       SuperComputer:0        LISTENING
```

Figure 97 Using ICMP for monitoring

FTP Session monitoring

IIS allows to monitor FTP current sessions. Administrator can keep track of active FTP session and analyze state of FTP sites (Figure 2).

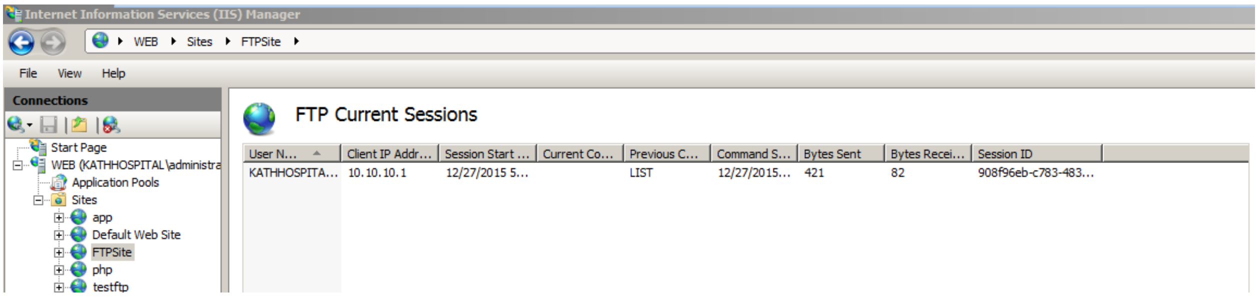
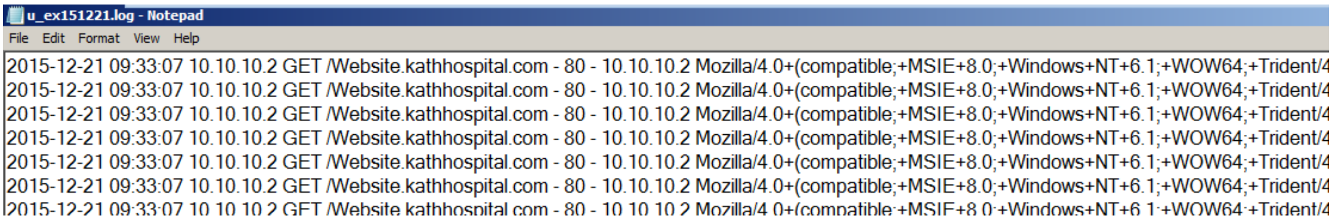


Figure 98 FTP active session monitoring

Log file review

Log files are great tools to analyze problem and troubleshooting them. Any website activity in webserver is logged into log file which administrator can study.




```
2015-12-21 09:33:07 10.10.10.2 GET /Website.kathhospital.com - 80 - 10.10.10.2 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+6.1;+WOW64;+Trident/4
2015-12-21 09:33:07 10.10.10.2 GET /Website.kathhospital.com - 80 - 10.10.10.2 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+6.1;+WOW64;+Trident/4
2015-12-21 09:33:07 10.10.10.2 GET /Website.kathhospital.com - 80 - 10.10.10.2 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+6.1;+WOW64;+Trident/4
2015-12-21 09:33:07 10.10.10.2 GET /Website.kathhospital.com - 80 - 10.10.10.2 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+6.1;+WOW64;+Trident/4
2015-12-21 09:33:07 10.10.10.2 GET /Website.kathhospital.com - 80 - 10.10.10.2 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+6.1;+WOW64;+Trident/4
2015-12-21 09:33:07 10.10.10.2 GET /Website.kathhospital.com - 80 - 10.10.10.2 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+6.1;+WOW64;+Trident/4
2015-12-21 09:33:07 10.10.10.2 GET /Website.kathhospital.com - 80 - 10.10.10.2 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+6.1;+WOW64;+Trident/4
```

Figure 99 Log File study

Network Monitoring Tools

Microsoft Network Monitor

It is free packet analyzer from Microsoft which enables administrator to capture, analyze, and study network traffics as shown in figure 4. MNM is useful tool for identifying problems and troubleshooting them. Its main benefit is it supports around 300 Microsoft proprietary protocols and public protocols. It allows to study session, wireless monitor etc. When two computers cannot communication, this tools helps to analyze the problem.

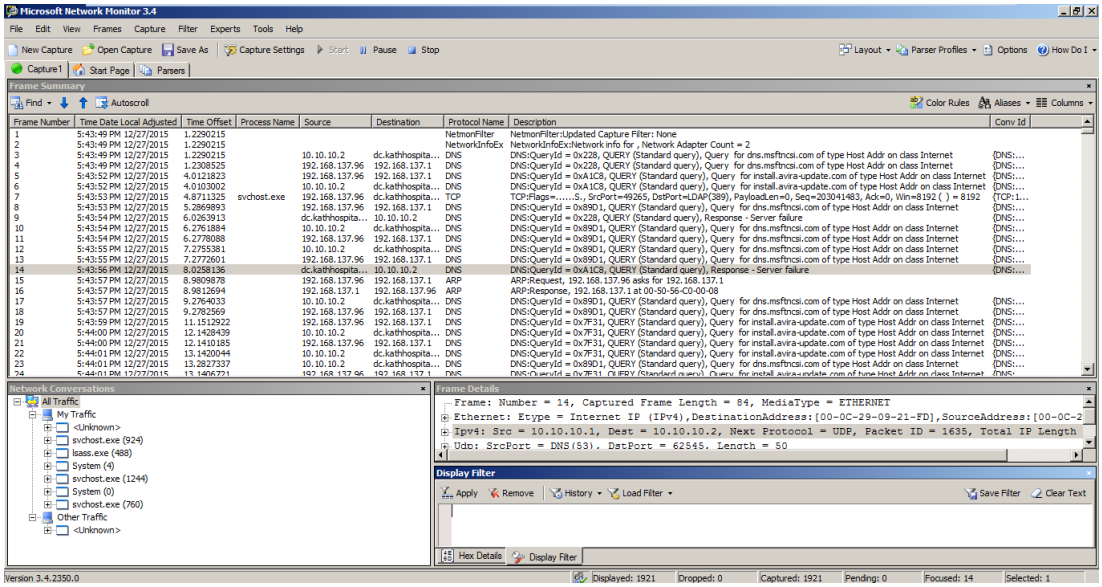


Figure 100Capturing and analyzing using MNM

Syslog Junction

It is a tool to view system logs with capabilities of graphical interface. It gains syslog messages form server and administrator can browse them in graphical interface. It allows to monitor live connections, understand volume of traffic, inbound and outbound traffics etc.

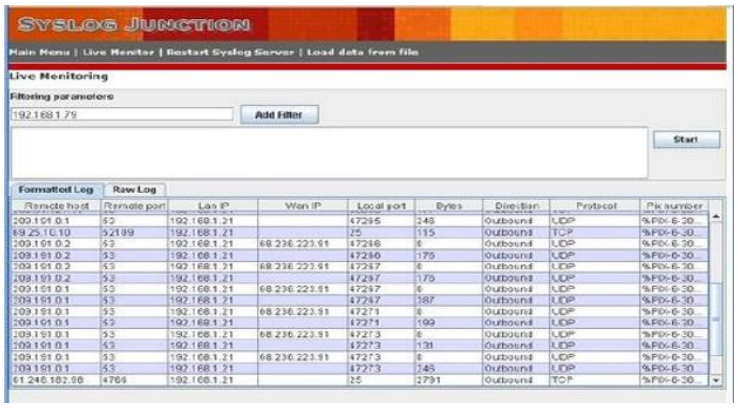


Figure 101 Live Session Monitoring using Syslog Junction

Identified Issues and Troubleshooting

Packet Loss

Traffic monitoring shows packet drop in traffic.

Possible cause	Solution and Recommendation
Link congestion	Probable reason for this issue can be trying to pass large traffic from smaller capacity line. To address this issue ensure network lines can support all potential traffic size.
Firewall misconfiguration	Firewall misconfiguration is another probable cause of the data packet loss. Administrator has to ensure required ports are not blocked by Firewall.
Broken or loose cable	Another usual cause for packet loss is damaged cable and loose connection, administrator has to ensure cable is in correct condition and there is no loose connection.

Internet server Performance

Nova bench

To perform benchmarking of Internet server, free third party tool Nova Bench is utilized. It enables to benchmark GPU, CUP, disk speed, and RAM. It is comprehensive tool for all in one benchmarking. It process faster than many other benchmark suits and helps to study the performance of the system. Benchmark report of the implemented Internet server is provided below.

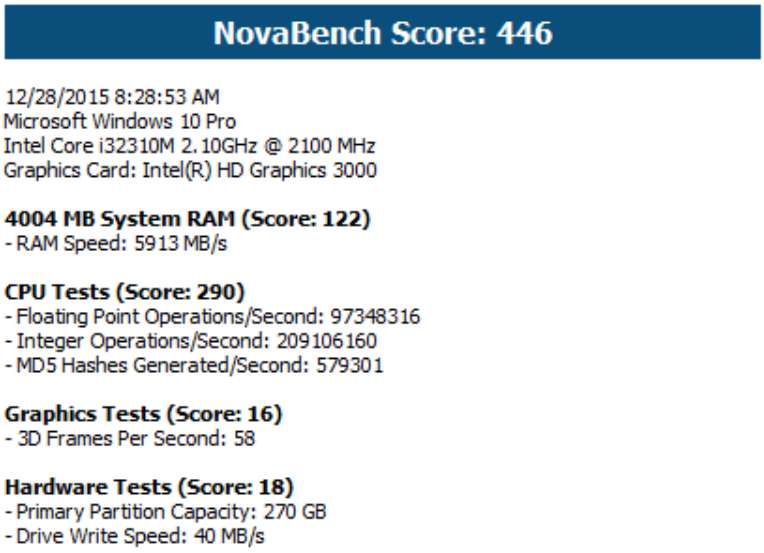


Figure 102 Nova Benchmarking

Resource monitoring

Windows based server allows to monitor various system components such as CPU, memory, Disk and Network. It allows to analyze state of such components and find any problematic application, need of system upgrade, study disk usage etc. Resource monitoring report of Implemented Internet server is provided below.

Overview Report

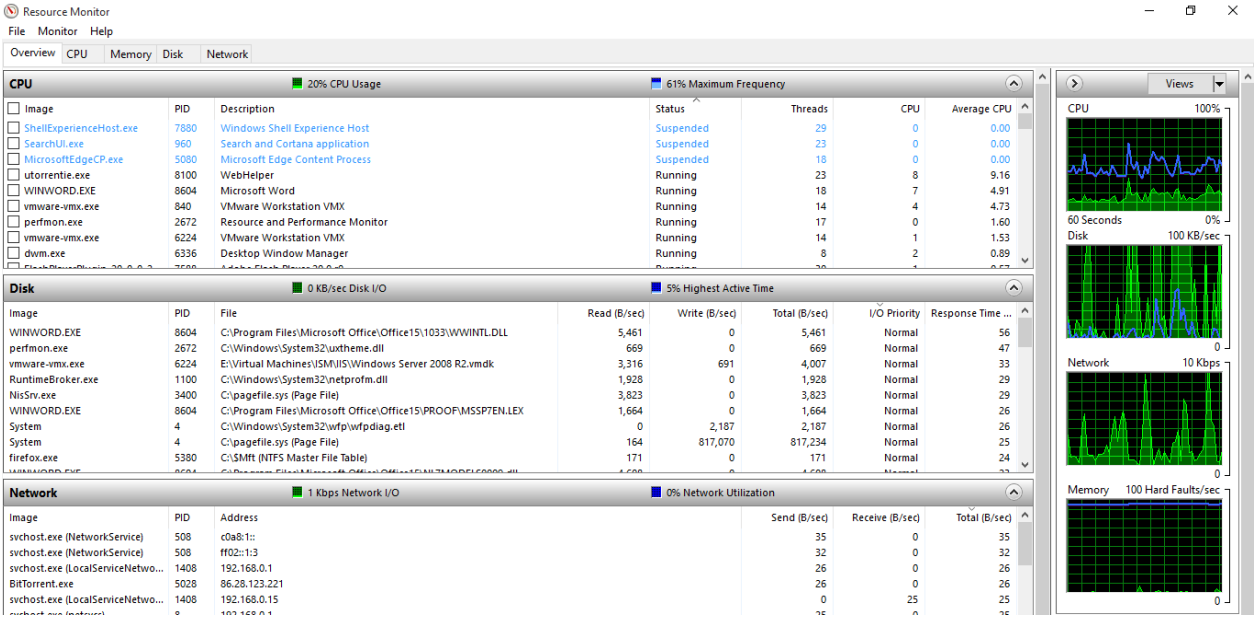


Figure 103 Resource Monitor Overview Report

CPU Report

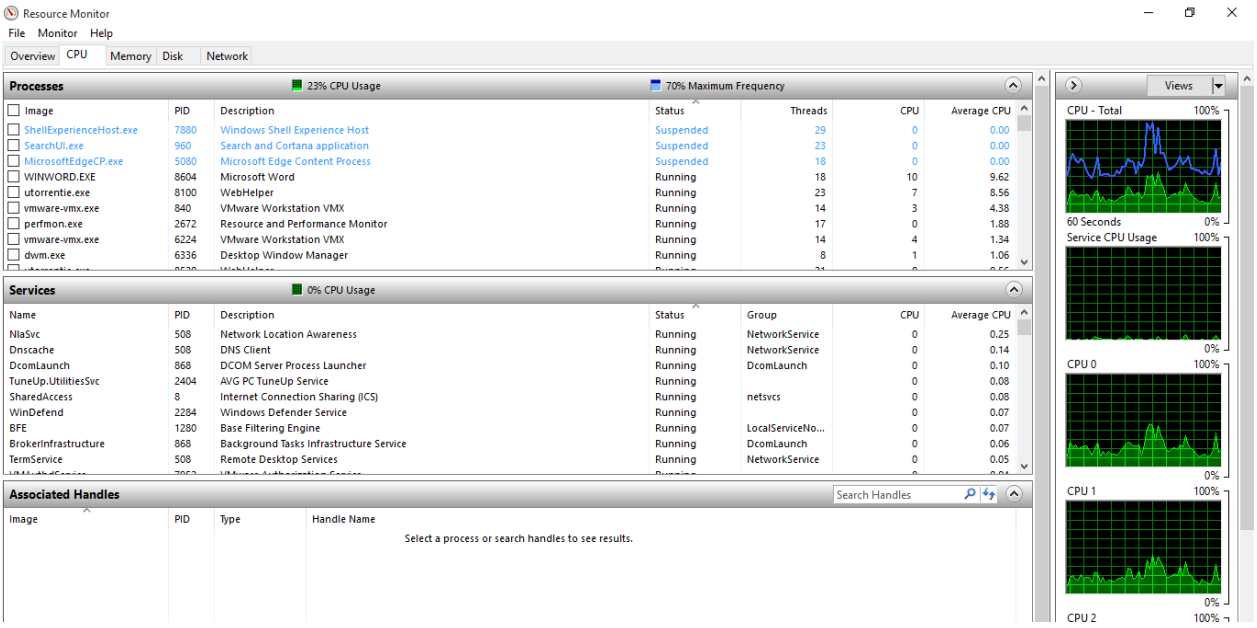


Figure 104 Resource Monitor CPU Report

Memory Report

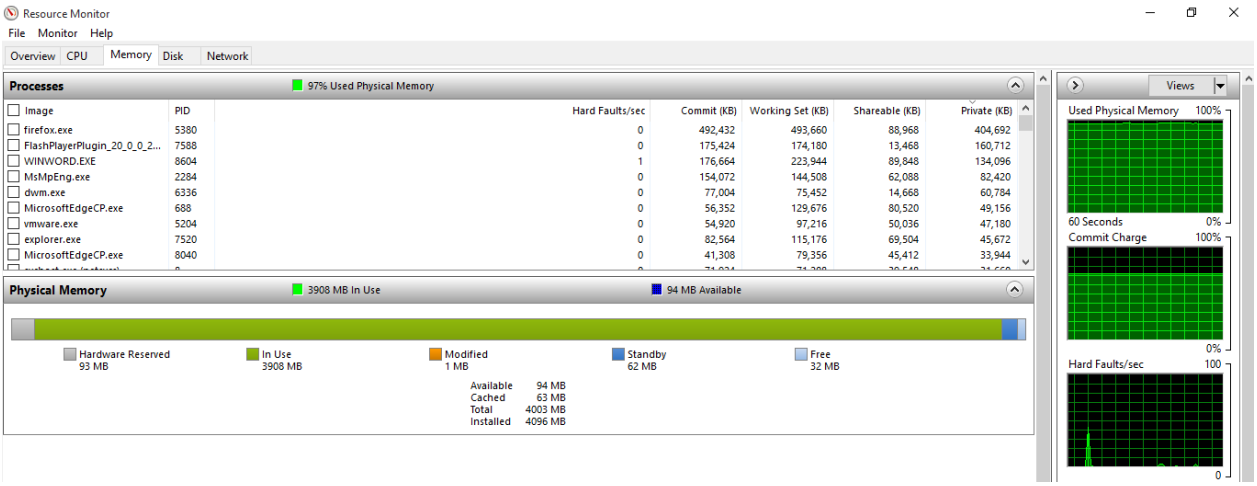


Figure 105 Resource Monitor Memory Report

Disk Usage Report

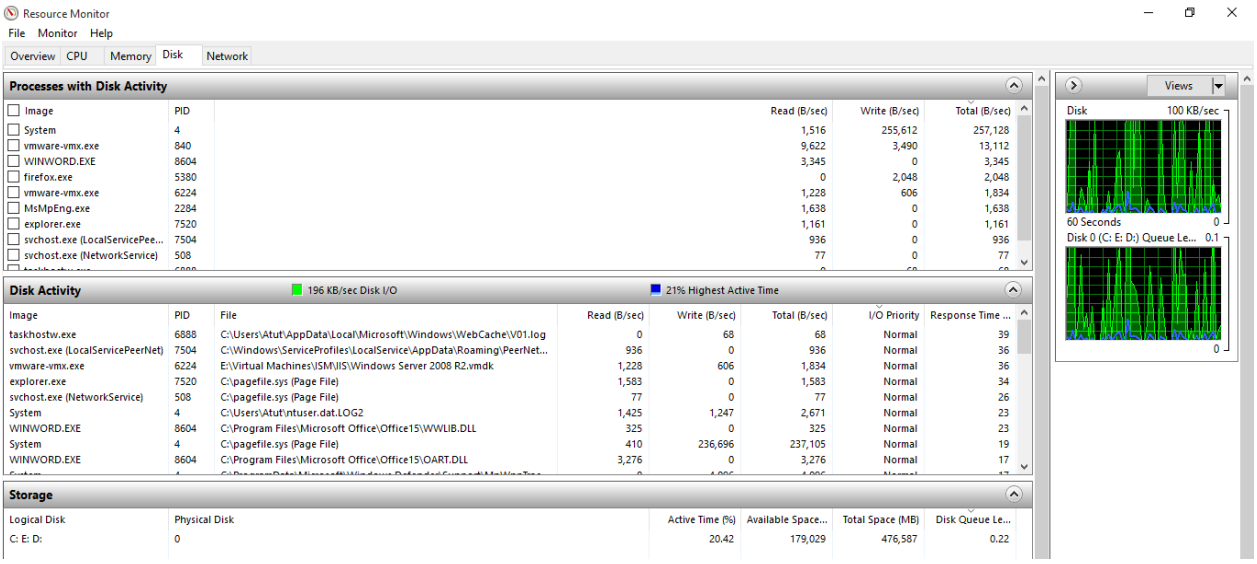


Figure 106 Resource Monitor Disk usage Report

Network Report

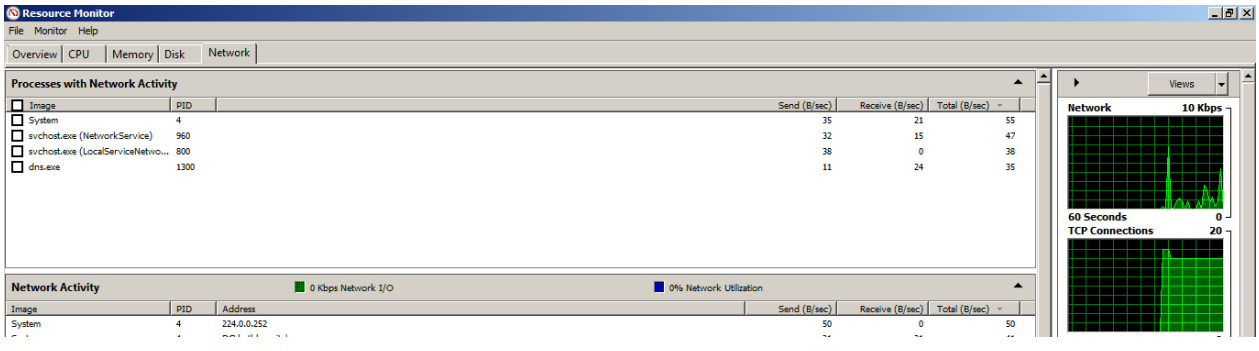


Figure 107 Resource Monitor Network Report

Conclusion

This paper has utilized various monitoring tools and keep track of system activities while identifying problems and troubleshooting them. Monitoring of system shows packet loss in communication. Troubleshooting for such problem is provided in this report. Furthermore, benchmarking tools like Nova bench is utilized to benchmark the system and resource monitor is utilized to monitor the state of resources in in system. Monitoring shows absence of free RAM, this can be address via identifying application that is eating RAM and closing them or upgrading the size of RAM in the system. Other than that every other report shows satisfying results.