6.1 Challenges and Risks
6.2 IPv6 Deployment Plan
6.3 IPv6 DNS(AAAA and A6 records)
6.4 IPv6 enabled Proxy, Web and Mail Servers

- ✓ As a first step towards deploying IPv6 (that will co-exist with IPv4) across the Globe, the **IPv6 Forum** was formed in July 1999. Its common mission is to educate Internet users on the advantages of the IPv6 protocol, and to promote and implement the worldwide deployment of this protocol.
- ✓ It has an impressive membership list comprising of manufacturers, leading Telecom operators, Internet service providers, and vendors of Internet solutions, Consulting companies, R&D institutions and many others.
- ✓ The current status of deployment of IPv6 in different parts of the world is very encouraging and gives an idea of what the future holds for the Internet in the coming years.
- **Korea**: KOREAv6, composed with IPv6 Trial Services and Field Test for IPv6 Equipment is the IPv6 Pilot Project launched in Korea
- **France**: IPv6 The IPv6 Task Force was created in France on September 25th 2002. The deployment of IPv6 has been done in a phased manner with the active involvement of France Telecom, the leading Telecom operator in the country
- **China**: has initiated the China's Next Generation Internet project (CNGI), which is a five-year plan with the objective of cornering a significant proportion of the Internet space by implementing IPv6 early
- **Japan**: JGN (Japan Gigabit Network) – IPv6 over ATM and Native IPv6 transport (not tunnel)
- **USA**: The US Government has issued a mandate to all vendors both civilian and defense – to make the switch to an IPv6 platform by summer of 2008
- **Canada**: Viaginie of Canada, a consulting and research and development firm specializing in advanced computer networking technologies has developed a tunnel server, the freenet6.net to allow any IPv4 node to be connected to the 6Bone. International connectivity of IPv6 has been achieved with US and other countries through native IPv6 and over IPv4 tunnels.

Major planning issues for deploying IPv6 on an existing IPv4 are platform and application support, connectivity, name resolution, security, and controlled or prioritized delivery.

6.1 Challenges and Risks

"IPv6 can be deployed just as securely as IPv4, although it should be expected that vulnerabilities within the protocol, as well as with implementation errors, will lead to an initial increase in IPv6-based vulnerabilities," the guidelines say.
Likely security challenges of IPv6 deployment include:

- The possibility that attackers might have more expertise with IPv6 than an organization in the early stages of deployment.
- Difficulty in detecting and managing unknown or unauthorized IPv6 assets on existing IPv4 production networks.
- The added complexity of operating parallel IPv4 and IPv6 networks.
- A lack of IPv6 maturity in security products.
- The proliferation of IPv6 and IPv4 tunnels can complicate defenses.

The Impact of IPv6 on Various Network Entities

1. How IPv6 affects layer 2

The layer 2 switches process packets based on MAC addresses which are independent of IPv6. Hence, implementing IPv6 over layer 2 networks should not need significant changes to the layer 2 switches. However, IPv6 support for protocol VLANs may need hardware support. Functionality such as ACL (Access Control Lists) and MLD snooping (equivalent to IPv4 IGMP snooping) will need to take into account changes for IPv6.

2. How IPv6 affects layer 3

For layer 3 support, in addition to the basic IPv6 modules, the routing and forwarding mechanism needs to be aware of IPv6. Hence, protocols such as RIPng and OSPFv3 will need to be deployed and the hardware will need to be IPv6 capable in order to do line rate processing of IPv6 packets. Thus, a significant change to hardware and software functionality will be needed in routers to support IPv6.

3. What IPv6 means to the desktop/hosts

The desktop operating system needs to support IPv6 in order to deploy IPv6 on hosts. The enterprise and consumer applications need to be ported to IPv6 so that there is an application base for IPv6. New IPv6 applications will need to be developed that support end-to-end and peerto-peer communications models on the Internet. For hosts to communicate using IPv6, the necessary infrastructure needs to be in place to support IPv6. A transition plan needs to be formulated for the network and the strategy will figure out whether the transition will need specific software support from the host or whether it will be seamless. Again, depending on the network topology plan, DHCP or DNS support for IPv6 may be needed.

Deployment Issues

IPv6 technology promises to bring a number of benefits to network communications. But given the complexity of the entire IPv6 protocol family and the need for a robust infrastructure supporting the protocols, it would be wise for an enterprise to give thoughtful consideration to issues concerning IPv6 deployment.

• Protecting existing investment

Vendors need to protect existing investments in switches/routers/hosts. Thus they need a strategy which will maximize the returns on current investments

• Return on investment (ROI)

IPv6 will need software and hardware upgrades on hosts, switches and routers. It may need deployment of new applications. Also, IPv6 transition needs to be carefully planned and a pilot network is typically done to evaluate the strategy. All this requires time and adds to expenses. Hence, a clear business case needs to be made to trigger migration of enterprise networks to IPv6.

• Network planning

IPv6 can be deployed in two ways: having completely independent IPv6 and IPv4 networks or overlaying IPv4 and IPv6 networks. This strategy can affect the IPv6 features required on hosts, switches and routers.

• Instability in some IPv6 features

Certain standards like mobile IPv6 are not stable yet, and this is necessary for successful deployment particularly to avoid interoperability issues.

• Service provider support

For enterprises which require IPv6 communication over the Internet, it is necessary to look into what IPv6 services and applications are offered by the service providers

6.2 IPv6 Deployment Plan

When deploying IPv6, you should consider the following in planning:

- Platform support for IPv6
- Application support for IPv6
- Network management infrastructure support for IPv6
- Unicast IPv6 addressing architecture
- Tunnel-based IPv6 connectivity
- Other IPv6 transition technologies
- Native IPv6 connectivity
- Name resolution with DNS
- Native IPv6 addressing allocation
- Host-based security and IPv6 traffic
- Controlled or prioritized delivery for IPv6 traffic

Platform support for IPv6

- Microsoft has supplied a production-quality, deployment-ready IPv6 protocol in the following versions of Windows e.g. Windows Server 2008, 2012, Windows Vista, 7,8,10 etc.

Application support for IPv6

- All the applications included with Windows Server 2012 and Windows 8 support operation over IPv6. Whether third-party applications and custom applications developed for use by your organization support operation over IPv6 depends on the application programming interfaces (APIs) that they use for network operations. For applications that use IP protocol–independent APIs, such as Windows Runtime or the .NET Framework, no modification is needed for operation over IPv6.
- Applications that use IP protocol-dependent APIs such as Windows Sockets (Winsock) might need to be updated to support operation over IPv6. For example, a Winsock application might use the older Gethostbyname() function, which is an IPv4 protocol–specific function that returns only IPv4 addresses. This application must be modified to use the new Getaddrinfo() function, which returns both IPv4 and IPv6 addresses.

Network management infrastructure support for IPv6

- Network management infrastructure components such as firewalls, network node management systems, WAN optimizers, and security systems that monitor network traffic, either enable IPv6 functionality in the existing systems that support it as needed or determine the plan to include IPv6 support in their update, upgrade, or replacement cycle.
- For example, if a WAN optimizer product does not currently support optimization of native IPv6 traffic, inquire with the vendor about their plans for such support in a future update or upgrade. If they have no plans to support IPv6 in the long term, begin investigating other WAN optimization products for a suitable replacement when your current product nears the end of its usable life cycle

Unicast IPv6 addressing architecture

Just as for your IPv4 infrastructure, you must decide on a unicast IPv6 addressing plan for your intranet. You must determine how to number the individual subnets of your organization. Subnet addressing for IPv6 is actually easier than IPv4, due to the 64-bit prefix length for all LAN subnets and the relative abundance of address space for organizations.

Tunnel-based IPv6 connectivity

- Windows includes the tunneling technologies and methods e.g. ISATAP, 6to4, Configured Tunneling etc.

Other IPv6 transition technologies

- Windows includes the additional IPv6 transition technologies are – IP-HTTPS, NAT64, DNS64
- IP over the Secure Hypertext Transfer Protocol (HTTPS) (IP-HTTPS) is a tunneling protocol that tunnels IPv6 traffic inside of an HTTPS session. IP-HTTPS is supported by Windows Server 2012, Windows Server 2008 R2, Windows 8, and Windows 7
- **NAT64** provides stateful translation between IPv6 and IPv4 traffic when that traffic is initiated by an IPv6-only node. NAT64 takes the IPv6 traffic from the IPv6-only node and converts it into IPv4 traffic for the IPv4-only node, and vice versa. **DNS64** is a method of mapping IPv6-only address record (AAAA) DNS queries to IPv4 address record (A) responses to facilitate communication between communication-initiating IPv6-only nodes and IPv4- only nodes. NAT64/DNS64 is provided in Windows Server 2012

Native IPv6 connectivity

- Native IPv6 connectivity consists of the following capabilities: Unicast routing (required) and Multicast routing (optional)

Name resolution with DNS

For your internal DNS to provide the same level of service for IPv6-related information as it does for IPv4-related information, you need to ensure that your DNS infrastructure supports the following:

- AAAA records for IPv6 addresses
- DNS dynamic updates so that IPv6 hosts can automatically register AAAA records

Native IPv6 addressing allocation

- A key decision for native IPv6 addressing allocation is whether to use stateless address autoconfiguration (the use of routers only to assign IPv6 addresses), stateful address autoconfiguration (the use of DHCPv6 only to assign IPv6 address and other configuration options), or a combination of the two.
- Because the IPv6/IPv4 hosts on your intranet, whether they are located on the IPv4-only or IPv6- capable portion, will continue to use IPv4 and DHCP to obtain configuration settings such as the IPv4 addresses of your DNS servers or the DNS name suffix for your organization, the use of DHCPv6 is optional and you can accomplish your IPv6 addressing needs on a subnet with stateless address autoconfiguration.

Host-based security and IPv6 traffic

Providing security for IPv6 traffic for IPv6 hosts running Windows consists of the following: ■ Authorization for automatically assigned addresses and configurations ■ Prevention of rogue IPv6 routers

■ Protection of IPv6 packets- cryptographic protection of IPv6 traffic, use IPsec ■ Host protection from scanning and attacks

■ Control of tunneled traffic on your intranet: To control what types of IPv6 traffic, either tunneled or native, are allowed to travel within your intranet, you can use Router-based firewalls or Host-based firewalls

■ Control of what traffic is exchanged with the Internet

Controlled or prioritized delivery for IPv6 traffic

- If you do not, as the volume of IPv6 traffic on your network grows, it will not have the same treatment as IPv4 traffic and can lead to undesirable situations that the techniques for IPv4 traffic are trying to prevent.
- A WAN optimizer can compress IPv4 traffic before sending it over a relatively small bandwidth WAN link to a remote location. The WAN optimizer helps prevent the WAN link from being overwhelmed with IPv4 traffic and lowers the transit delay between locations. If the WAN optimizer does not support compressing IPv6 traffic, when the volume of IPv6 traffic rises as it replaces IPv4 traffic, it can eventually overwhelm the WAN link.

6.3 IPv6 DNS(AAAA and A6 records)

- An AAAA record points a domain or subdomain to an IPv6 address.
- A6 and AAAA are both DNS records to represent IPv6 addresses. They differ in format (AAAA being a fixed length format while A6 is a variable length format).
- As for support in a DNS client, you can live with supporting only AAAA (as that is widely supported by DNS resolver) and would need to add support for A6 only if you stumble on a server which accepts only A6 records.

An AAAA (pronounced quad A) record is a DNS record that maps to an IPv6 address.

For example:

```
~: dig ns1.no-ip.com AAAA
;; ANSWER SECTION:
ns1.no-ip.com. 86400 IN AAAA 2620:0:2e60::33
```

AAAA records are available for customers using the No-IP Plus Managed DNS service. Currently, IP addresses are based on version 4 of the internet protocol, where there are 4 sets of numbers ranging from 0-255. For example (127.198.30.245).

The A6 record is used to represent a 128-bit IPv6 address. When an IPv6 aware application wants to look up the name of an IPv6 server, it will request an A6 record from the DNS server. (Just as a reminder: in IPv4, applications request the A, for "Address," record to translate names to addresses.)
The first several bits (words, actually) of the address are the Provider's prefix. In IPv4, this is analogous to the network number, which is the same for all systems on the network and gets repeated a lot. Since IPv6 addresses are so much longer, we'd rather not hardcode that prefix into the local DNS. The A6 record lets us *refer* to the Provider's DNS for those bits in the address. This gives Provider and Client more independence from each other's DNS. In addition, if the network changes ISPs, there is no need to modify the DNS---you can simply change the referral record to point to the new ISP.

```
;A6 RR format;
;NAME [TTL] TYPE BITS ADDRESS REFERRAL
; IN
; REFERRAL
linux A6 64 ::02d0:09ff:fef7:6d2c SLAnortel.v6.ilabs.interop.net.
```

In the example above, the name given in the Referral field is defined in the Provider's DNS, and would have the first 64 bits of the address being looked up.
Thus, when an application looked up the name "linux," it would get the last 64 bits of the address from the address (A6) record above, and then go to SLAnortel.v6.ilabs.interop.net to get the first 64 bits, which it would combine to get a full IPv6 address.
The AAAA record is to help transition and coexistence between IPv4 and IPv6 networks. It is here today - supported in BIND 8.1.x. With this record, an IPv4 nameserver can provide IPv6 addresses:

```
linux aaaa 3ffe:1900:4545:2:02d0:09ff:fef7:6d2c
```

The PTR record is the same as the first example above, using dotted nibbles. Most DNS servers supporting IPv6 today are doing so with AAAA records running a production version of BIND.

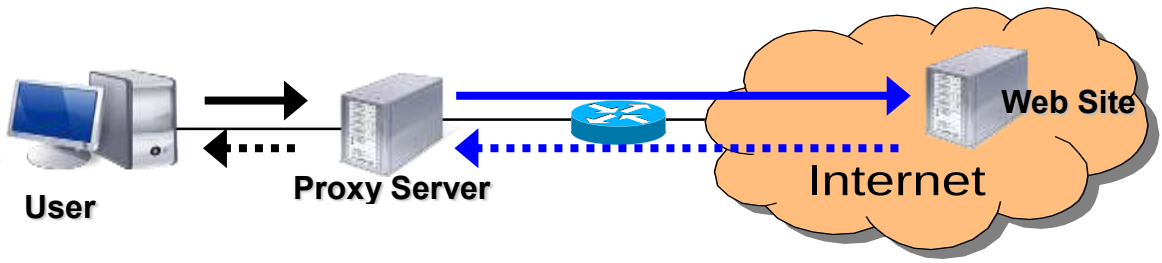
IPv6 DNS Configuration

• In an IPv4 environment, by default the DNS Client service on computers running Windows 2000, Windows XP, or Windows Server 2003 dynamically updates host (A) resource records (RRs) in DNS
• IPv6 has the additional requirement that IPv6 nodes use a new type of address resource record, known as AAAA (quad-A) resource records, to resolve a fully qualified domain name to an IPv6 address. (*Four "A"s are used for the name of these resource records because 128-bit IPv6 addresses are four times as large as 32-bit IPv4 addresses.)*
• An IPv6 host sends DNS name queries to the DNS server to resolve host names to IPv6 addresses. The AAAA resource records stored on the DNS server provide the mapping from a host name to its IPv6 address
• **Address Resource Records.** To successfully resolve names to addresses, the DNS infrastructure must contain the following resource records, populated either manually or dynamically: A resource records for the IPv4 addresses of IPv4 nodes.
• AAAA resource records for the IPv6 addresses of IPv6 nodes. The following is an example of a AAAA resource record:
host1.microsoft.com IN AAAA FEC0::2AA:FF:FE3F:2A1C

6.4 IPv6 enabled Proxy, Web and Mail Servers

* Proxy Server

- A proxy server is a server placed between the client site and the main server. Also known as Intermediate server.
- When users request for a data from web browser which was configured to use proxy server
  - Traffic goes from web browser to a proxy server
  - On behalf of user, proxy will do the job for requesting the data from internet.
  - Proxy will transmit back the information to user



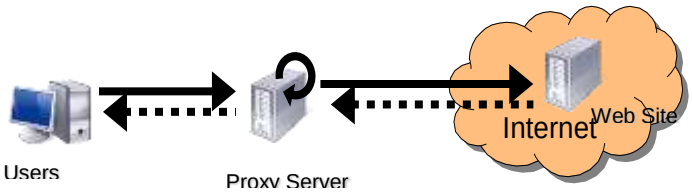
- Advantages of using proxy servers
  - Improve performance
  - Ensure security
- **Improve performance:** Faster operation, because using cache service.

- Ensure security
  - Rules and policies regulation can be added into proxy configuration makes proxy server can serve the users by filtering their requests.
  - It make the network easier to be controlled because only traffic that passes the filtering requirements will be served or reply

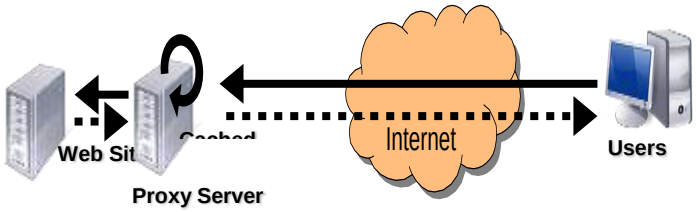
Types of Proxy

There are many different types of Proxy Servers . It depends on the purpose of network administrator to setup a proxy servers. Mainly, proxy servers can be categorized into 3 types:

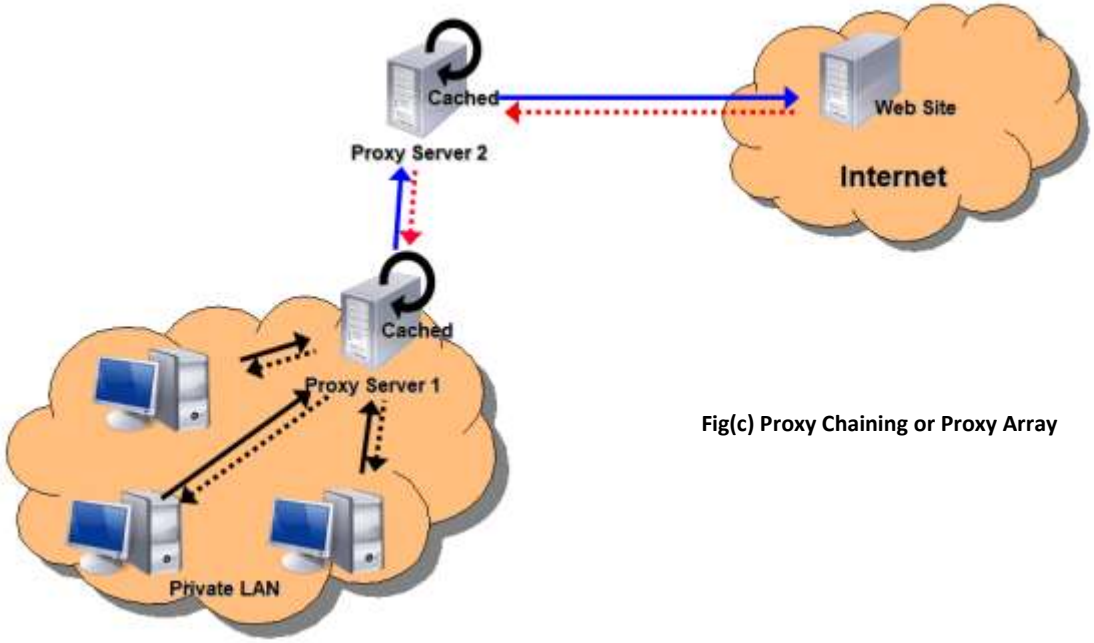
1) **Forward Proxy**: Generally used to accept or reject request from users based on the policies that defined.
2) **Reverse Proxy:** The reverse proxy is generally used to pass the request from the Internet to local network.
3) **Proxy Chaining or Proxy Array:** Proxy chain involved 2 or more proxy server in a network in order to enhance the performance and the security control of a network.



Fig(1) Forward Proxy



Fig(2) Reverse Proxy



Fig(c) Proxy Chaining or Proxy Array

*** Mail Server**

A mail server (sometimes also referred to an e-mail server) is a server that handles and delivers e-mail over a network, usually over the Internet. A mail server can receive e-mails from client computers and deliver them to other mail servers. A mail server can also deliver e-mails to client computers. A client computer is normally the computer where you read your e-mails, for example your computer at home or in your office. Also an advanced mobile phone or Smartphone, with e-mail capabilities, can be regarded as a client computer in these circumstances.

SMTP and POP3 server

When you press the "Send" button in your e-mail program (e-mail client) the program will connect to a server on the network / Internet that is called an SMTP server. **SMTP** is an acronym for **Simple Mail Transfer Protocol** and it is a protocol that is used when e-mails are delivered from clients to servers and from servers to other servers.
When you download e-mails to your e-mail program the program will connect to a server on the net that is known as a POP3 server. A POP3 server uses a protocol named POP3 for its communication. That is the reason why it is called a POP3 server and **POP3** is an acronym for **Post Office Protocol** version **3**

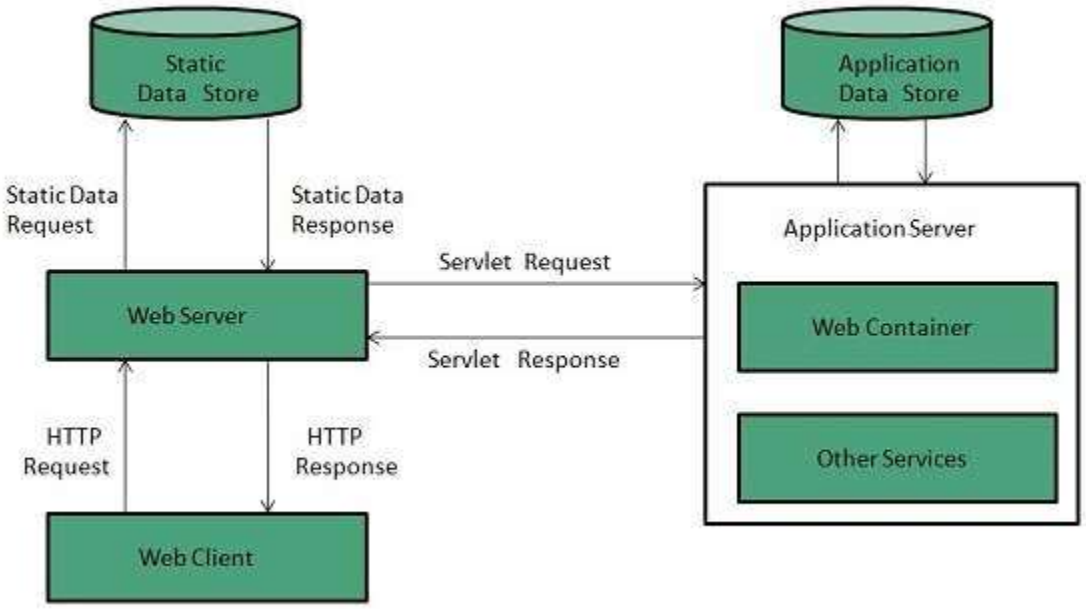
* Web Server

Web server is a computer where the web content is stored. Basically web server is used to host the web sites but there exists other web servers also such as gaming, storage, FTP, email etc.
Web site is collection of web pages whileweb server is a software that respond to the request for web resources.

Web Server Functions

Web server respond to the client request in either of the following two ways:

- Sending the file to the client associated with the requested URL.
- Generating response by invoking a script and communicating with database



Key Points

- When client sends request for a web page, the web server search for the requested page if requested page is found then it will send it to client with an HTTP response.
- If the requested web page is not found, web server will the send an **HTTP response:Error 404 Not found.**
- If client has requested for some other resources then the web server will contact to the application server and data store to construct the HTTP response.

Architecture

Web Server Architecture follows the following two approaches:

1. Concurrent Approach
2. Single-Process-Event-Driven Approach.

Concurrent Approach: Concurrent approach allows the web server to handle multiple client requests at the same time. It can be achieved by following methods:

- Multi-process
- Multi-threaded
- Hybrid method.

Multi-processing

In this a single process (parent process) initiates several single-threaded child processes and distribute incoming requests to these child processes. Each of the child processes are responsible for handling single request.
It is the responsibility of parent process to monitor the load and decide if processes should be killed or forked.

Multi-threaded

Unlike Multi-process, it creates multiple single-threaded process. Multithreading is an execution model that allows a single process to have multiple code segments (i.e., *threads*) run concurrently within the "context" of that process. You can think of threads as child processes that share the parent process resources but execute independently.

FEATURES	MULTI-PROCESSING	MULTI-THREADING
Basic	Multiprocessing adds CPUs to increase computing power.	Multithreading creates multiple threads of a single process to increase computing power.
Execution	Multiple processes are executed concurrently.	Multiple threads of a single process are executed concurrently.
Creation	Creation of a process is time-consuming and resource intensive.	Creation of a thread is economical in both sense time and resource.
Classification	Multiprocessing can be symmetric or asymmetric.	Multithreading is not classified.

Hybrid

It is combination of above two approaches. In this approach multiple process are created and each process initiates multiple threads. Each of the threads handles one connection. Using multiple threads in single process results in less load on system resources.

Examples

Following table describes the most leading web servers available today:

S.N.	Web Server Descriptino
1	**Apache HTTP Server:** This is the most popular web server in the world developed by the Apache Software Foundation. Apache web server is an open source software and can be installed on almost all operating systems including Linux, UNIX, Windows, FreeBSD, Mac OS X and more. About 60% of the web server machines run the Apache Web Server.
2.	**Internet Information Services (IIS):** The Internet Information Server (IIS) is a high performance Web Server from Microsoft. This web server runs on Windows NT/2000 and 2003 platforms (and may be on upcoming new Windows version also). IIS comes bundled with Windows NT/2000 and 2003; Because IIS is tightly integrated with the operating system so it is relatively easy to administer it.
3.	**Lighttpd** The lighttpd, pronounced lighty is also a free web server that is distributed with the FreeBSD operating system. This open source web server is fast, secure and consumes much less CPU power. Lighttpd can also run on Windows, Mac OS X, Linux and Solaris operating systems.
4.	**Sun Java System Web Server:** This web server from Sun Microsystems is suited for medium and large web sites. Though the server is free it is not open source. It however, runs on Windows, Linux and UNIX platforms. The Sun Java System web server supports various languages, scripts and technologies required for Web 2.0 such as JSP, Java Servlets, PHP, Perl, Python, and Ruby on Rails, ASP and Coldfusion etc.
5.	**Jigsaw Server:** Jigsaw (W3C's Server) comes from the World Wide Web Consortium. It is open source and free and can run on various platforms like Linux, UNIX, Windows, and Mac OS X Free BSD etc. Jigsaw has been written in Java and can run CGI scripts and PHP programs.