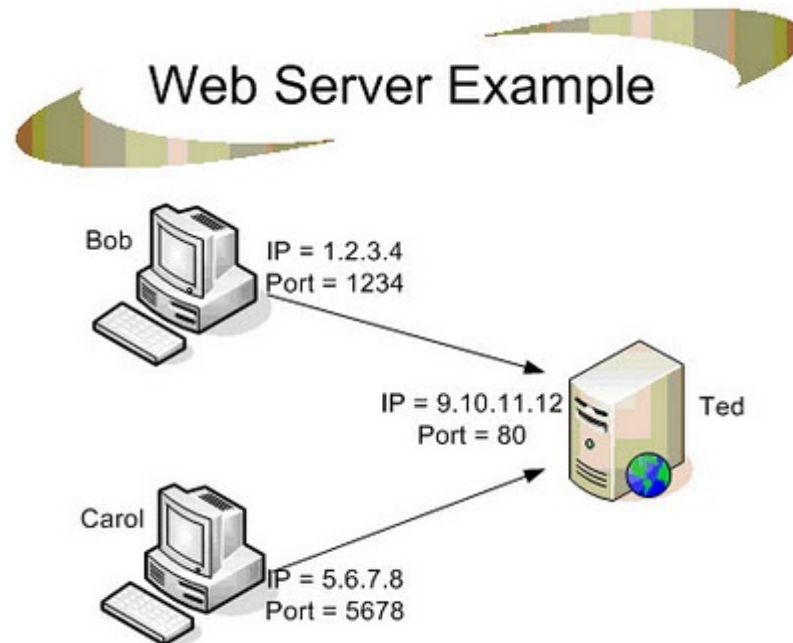


# Pemrograman Jaringan : Implementasi Network Programming (Web Server, DNS Server, FTP Server, RPC Server)

## 1. Web Server



Kata Web Server dapat dimaknai dengan :

1. Suatu Program Komputer yang mempunyai tanggung jawab/tugas menerima permintaan HTTP dari komputer klien, yang dikenal dengan nama web browser, dan melayani mereka dengan menyediakan respon HTTP berupa konten data, biasanya berupa halaman web yang terdiri dari dokumen HTML, dan objek yang terkait seperti gambar, dll.
2. Komputer yang menjalankan program diatas. Walaupun masing-masing program webserver secara detail berbeda tetapi pada umumnya program

Webserver atau server adalah komputer yang dikhususkan untuk menaruh data website, hanya saja dalam hal ini server harus 24 jam online, jika tidak maka data tak bisa diakses oleh pengunjung website. Semua komputer logikanya bisa dijadikan server, namun server yang khusus untuk website punya spesifikasi khusus. Hal ini untuk menjaga agar kecepatan server stabil dan memenuhi kriteria yang dihadapkan. Selain bergantung pada spesifikasi hardware dan software, kecepatan webserver juga bergantung pada akses internet di tempat server berada atau juga tergantung pada kecepatan Internet Service Provider (ISP) yang digunakan untuk online, dan terlebih lagi juga bergantung pada jalur lokasi negara yang bersangkutan.

Web server adalah software yang menjadi tulang belakang dari world wide web (www). Web server menunggu permintaan dari client yang menggunakan browser seperti Netscape Navigator, Internet Explorer, Mozilla, dan program browser lainnya. Jika ada permintaan dari browser, maka web server akan memproses permintaan itu kemudian memberikan hasil prosesnya berupa data yang diinginkan kembali ke browser. Data ini mempunyai format yang standar, disebut dengan format SGML (standar general markup language). Data yang berupa format ini kemudian akan ditampilkan oleh browser sesuai dengan kemampuan browser tersebut. Contohnya, bila data yang dikirim berupa gambar, browser yang hanya mampu menampilkan teks (misalnya lynx) tidak akan mampu menampilkan gambar tersebut, dan jika ada akan menampilkan alternatifnya saja.

Web server, untuk berkomunikasi dengan client-nya (web browser) mempunyai protokol sendiri, yaitu HTTP (hypertext transfer protocol). Dengan protokol ini, komunikasi antar web server dengan client-nya dapat saling dimengerti dan lebih mudah. Seperti telah dijelaskan diatas, format data pada world wide web adalah SGML. Tapi para pengguna internet saat ini lebih banyak menggunakan format HTML (hypertext markup language) karena penggunaannya lebih sederhana dan mudah dipelajari.

Kata HyperText mempunyai arti bahwa seorang pengguna internet dengan web browsernya dapat membuka dan membaca dokumen-dokumen yang ada dalam komputernya atau bahkan jauh tempatnya sekalipun. Hal ini memberikan cita rasa dari suatu proses yang tridimensional, artinya pengguna internet dapat membaca dari satu dokumen ke dokumen yang lain hanya dengan mengklik beberapa bagian dari halamanhalaman dokumen (web) itu. Proses yang dimulai dari permintaan webclient (browser), diterima web server, diproses, dan dikembalikan hasil prosesnya oleh web server ke web client lagi dilakukan secara transparan. Setiap orang dapat dengan mudah mengetahui apa yang terjadi pada tiap-tiap proses. Secara garis besarnya web server hanya memproses semua masukan yang diperolehnya dari web clientnya.

### Fungsi utama

Fungsi utama sebuah server web adalah untuk mentransfer berkas atas permintaan pengguna melalui protokol komunikasi yang telah ditentukan. Disebabkan sebuah halaman web dapat terdiri atas berkas teks, gambar, video, dan lainnya pemanfaatan server web berfungsi pula

untuk mentransfer seluruh aspek pemberkasan dalam sebuah halaman web yang terkait; termasuk di dalamnya teks, gambar, video, atau lainnya.

Pengguna, biasanya melalui aplikasi pengguna seperti peramban web, meminta layanan atas berkas ataupun halaman web yang terdapat pada sebuah server web, kemudian server sebagai manajer layanan tersebut akan merespon balik dengan mengirimkan halaman dan berkas-berkas pendukung yang dibutuhkan, atau menolak permintaan tersebut jika halaman yang diminta tidak tersedia.

Saat ini umumnya server web telah dilengkapi pula dengan mesin penerjemah bahasa skrip yang memungkinkan server web menyediakan layanan situs web dinamis dengan memanfaatkan pustaka tambahan seperti PHP, ASP.

Pemanfaatan server web saat ini tidak terbatas hanya untuk publikasi situs web dalam Waring Wera Wanua, pada prakteknya server web banyak pula digunakan dalam perangkat-perangkat keras lain seperti printer, router, kamera web yang menyediakan akses layanan http dalam jaringan lokal yang ditujukan untuk menyediakan perangkat manajemen serta mempermudah peninjauan atas perangkat keras tersebut.

#### Cara kerja web server :

1. Cara kerja Web server merupakan mesin dimana tempat aplikasi atau software beroperasi dalam mendistribusikan web page ke user, tentu saja sesuai dengan permintaan user.
2. Hubungan antara Web Server dan Browser Internet merupakan gabungan atau jaringan Komputer yg ada di seluruh dunia. Setelah terhubung secara fisik, Protocol TCP/IP (networking protocol) yg memungkinkan semua komputer dapat berkomunikasi satu dengan yg lainnya. Pada saat browser meminta data web page ke server maka instruksi permintaan data oleh browser tersebut di kemas di dalam TCP yg merupakan protocol transport dan dikirim ke alamat yg dalam hal ini merupakan protocol berikutnya yaitu Hyper Text Transfer Protocol (HTTP). HTTP ini merupakan protocol yg digunakan dalam World Wide Web (WWW) antar komputer yg terhubung dalam jaringan di dunia ini. Untuk mengenal protocol ini jelas sangat mudah sekali dimana setiap kali anda mengetik http://... anda telah menggunakannya, dan membawa anda ke dunia internet. Data yg di passing dari browser ke Web server disebut sebagai HTTP request yg meminta web page dan kemudian web server akan mencari data HTML yg ada dan di kemas

dalam TCP protocol dan di kirim kembali ke browser. Data yg dikirim dari server ke browser disebut sebagai HTTP response. Jika data yg diminta oleh browser tidak ditemukan oleh si Web server maka akan menimbulkan error yg sering anda lihat di web page yaitu Error : 404 Page Not Found.

Hal ini memberikan cita rasa dari suatu proses yang tridimensional, artinya pengguna internet dapat membaca dari satu dokumen ke dokumen yang lain hanya dengan mengklik beberapa bagian dari halaman-halaman dokumen (web) itu. Proses yang dimulai dari permintaan webclient (browser), diterima web server, diproses, dan dikembalikan hasil prosesnya oleh web server ke web client lagi dilakukan secara transparan. Setiap orang dapat dengan mudah mengetahui apa yang terjadi pada tiap-tiap proses. Secara garis besarnya web server hanya memproses semua masukan yang diperolehnya dari web clientnya.

### Aplikasi Pendukung Web Server

#### a) Text Editor

Digunakan untuk penulisan source code HTML dan Script PHP. Contoh Macromedia Dreamweaver, Notepad, Microsoft Frontpage dan lain sebagainya.

#### b) Web Browser

Digunakan sebagai media mempublikasikan halaman web. Contohnya Microsoft Internet Explorer, Mozilla FireFox dan lain-lain.

#### c) Server Side Scripting

Merupakan teknologi scripting atau pemrograman web dimana script dikompilasi atau diterjemahkan di server. Contohnya seperti ASP, ColdFusion, Java Server Page, Perl, Python, PHP. Yang paling umum digunakan adalah PHP.

#### d) Web Server

Digunakan untuk melayani permintaan browser client yang meminta akses ke suatu halaman web yang berada di sisi server. Web server yang umum digunakan adalah Apache.

#### e) Database

Digunakan untuk menyimpan data dalam database dan memanipulasi data yang diperlukan. Umumnya yang sering digunakan adalah MySQL.

Webserver memiliki fitur-fitur dasar yang sama seperti :

1. HTTP : Setiap program web server bekerja dengan menerima permintaan HTTP dari klien, dan memberikan respon HTTP ke klien tersebut. Respon HTTP biasanya mengandung dokumen HTML tetapi dapat juga berupa berkas raw, gambar, dan berbagai jenis dokumen lainnya. Jika terjadi kesalahan permintaan dari klien atau terjadi masalah saat melayani klien maka web server akan mengirim respon kesalahan yang dapat berupa dokumen HTML atau teks yang memberi penjelasan penyebab terjadinya kesalahan.

2. Logging : Umumnya setiap web server mempunyai kemampuan untuk melakukan pencatatan/logging terhadap informasi detil mengenai permintaan klien dan respon dari web server dan disimpan dalam berkas log, dengan adanya berkas log ini maka akan memudahkan web master untuk mendapat statistik dengan menggunakan tool log analyzer. Pada penggunaan sehari-hari banyak web server mengimplementasikan fitur-fitur berikut :

1. Otentifikasi : fitur untuk mengotorisasi suatu permintaan dari klien sebelum menggunakan sumber daya yang dimiliki oleh web server (biasanya User dan Password)
2. Penanganan konten statis (berkas tersimpan pada file sistem server) dan konten dinamis dengan mendukung satu atau lebih antara muka yang sesuai (SSI, CGI, SCGI, FastCGI, JSP, PHP, ASP, ASP.NET, Server API seperti NSAPI, ISAPI dsb).
3. Dukungan HTTPS (dengan SSL, atau TLS) yang memungkinkan koneksi yang aman (dengan enkripsi) ke server pada port 433 berbeda dengan koneksi HTTP biasa di port 80
4. Kompresi Konten (misal menggunakan encoding gzip) untuk mengurangi waktu respon server sehingga penggunaan pita data /Bandwith menjadi lebih hemat.
5. Virtual Hosting yang berguna untuk melayani banyak website hanya dengan menggunakan satu alamat IP.
6. Dukungan berkas berukuran besar, berfungsi untuk mendukung berkas yang memiliki ukuran lebih dari 2 gigabyte.
7. Pengatur Bandwith (Bandwith throttling) yang berfungsi untuk membatasi kecepatan respon dengan tujuan tidak membanjiri jaringan dan menghemat pita data (bandwith) agar dapat melayani klien lebih banyak.

Konten jawaban dari server web dibedakan menjadi :

1. Konten statis : biasanya berasal dari berkas yang telah ada pada server web
2. Konten Dinamis : dikatakan konten dinamis jika terjadi perubahan secara dinamis atas isi dari web baik dilakukan oleh program lain, script atau Application Program Interface (API) yang

dijalankan oleh server web. Server dengan konten statis biasanya lebih cepat dari yang berisi konten dinamis (2 s.d. 100 kali Lebih cepat), terutama dalam menangani pengambilan data dari database.

### Cara Memilih Web Server

Untuk membuat sebuah web server, maka kita akan menemukan berbagai macam persoalan, dimulai dari pemilihan software web browser mana yang paling sesuai kebutuhan, apa saja spesifikasi hardware yang dibutuhkan, bagaimana kondisi interkoneksi jaringan internet yang ada, dan lain sebagainya. Belum lagi termasuk bagian pembuatan halaman-halaman webnya, mau menggunakan format apa (HTML, SGML, PHP, PHP3, CGI, dan lain-lain).

Hal yang paling utama dalam proses pembuatan web server adalah memilih software mana yang akan digunakan sebagai web server kita. Untuk itu perlu adanya pertimbangan sebagai berikut :

1. Lisensi dari software yang akan digunakan (freeware, shareware atau komersial).
2. Kemudahan instalasi.
3. Kemudahan dalam mengatur konfigurasi.
4. Kemudahan untuk menambah atau mengubah periperhalnya.
5. Kemampuan Software.
6. Besar ruang yang dibutuhkan untuk menyimpan file-file minimal yang dibutuhkan agar software dapat berfungsi dengan baik.
7. Prospek software tersebut dimasa yang akan datang.
8. Performasi dan konsumsi sumber daya yang digunakan software itu.
9. Fasilitas apa yang mampu didukung oleh software itu.
10. Dukungan teknis (mempunyai site-site atau milis untuk bertanya bila terjadi masalah).
11. Dukungan platform (jenis sistem operasi apa saja yang dapat menjalankan software tersebut).
12. Dukungan terhadap third party (apakah software ini dapat ditambahkan software tambahan sebagai pelengkap).

Banyak sekali software web server yang dapat kita diambil di internet. Dengan berdasarkan pada 12 macam pertimbangan di atas, maka dapat dipilih software mana saja yang cocok dengan kebutuhan kita. Misalnya, kita memasang web server untuk keperluan suatu perusahaan jasa internet (ISP), maka pertimbangan yang harus diambil adalah apakah mereka

menginginkan software yang gratis atau komersial. Keuntungan dari software komersial adalah mereka mempunyai dukungan teknis dan dokumentasi yang lengkap.

Sedangkan pada kebanyakan software gratis mereka tidak menyertakan hal tersebut. Namun, ada juga software gratisan yang mempunyai dukungan teknis dari pembuatnya dan dengan dokumentasi yang lengkap. Salah satu software web server gratisan seperti itu adalah web server Apache.

### Penerjemahan Path (Path Translation)

Server web mengarahkan penterjemahan komponen path kedalam URL (Uniform Resource Locator) menuju :

- Sumber daya berkas sistem lokal jika permintaan bersifat statis.
- Program internal ataupun eksternal jika permintaan bersifat dinamis.

Untuk permintaan bersifat statis maka URL yang diminta oleh klien diarahkan ke root direktori webserver.

Perhatikan URL berikut yang diminta oleh klien :

`http://www.example.com/path/file.html`

Browser web pada klien akan menterjemahkan koneksi ke `www.example.com` dengan permintaan HTTP 1.1 seperti berikut :

***GET /path/file.html HTTP/1.1***

***Host: www.example.com***

Server Web `www.example.com` akan mencari path/alamat yang diberikan mulai dari root direktori. Pada mesin unix biasanya di `/var/www/htdocs`. Hasil pada sistem lokal adalah ***/var/www/htdocs/path/file.html***

Server akan mencari dan membaca berkas tersebut, jika berkas ada maka akan mengirimkan jawaban ke browser klien. Respon yang diberikan akan menggambarkan isi konten dari berkas itu sendiri.

### Load Limit (Batas Beban)

Setiap Server Web telah menentukan batas beban yang dapat ditanggung, sehingga setiap server web mempunyai batasan jumlah klien yang terhubung pada satu waktu (umumnya antara 2 s.d. 60.000, secara bawaan (default) maks 500 atau 1000). Kemampuan ini bergantung pada :

- Pengaturan Server Web itu sendiri;
- Jenis permintaan HTTP;
- Jenis Konten (Statis atau dinamis);
- Kondisi konten di server dilakukan cache atau tidak;
- Perangkat Keras, perangkat Lunak serta sistem operasi yang digunakan.

Jika server web sudah mendekati batas limit yang mampu ditangani maka server menjadi kelebihan beban sehingga lambat dalam memberikan respon. Penyebab Overload/Kelebihan beban Grafik harian beban server web, memperlihatkan adanya lonjakan beban pada awal hari. Setiap saat server web dapat saja mengalami kelebihan beban yang disebabkan :

- Terlalu banyak koneksi (misalkan ada ribuan bahkan jutaan permintaan dari klien pada jeda waktu yang singkat, seperti yang pernah terjadi pada Slashdot)
- Serangan DDOS (Distribute Denial Of Services);
- Cacing Komputer (Worm) yang dapat menyebabkan lalulintas data tidak wajar karena banyaknya komputer yang terinfeksi;
- Virus XSS dapat menyebabkan lalulintas data yang tinggi karena jutaan browser dan server web yang terinfeksi;
- Internet Web Robot, Lalu lintas data yang tidak difilter atau web server besar dengan sumber daya yang terbatas misalnya pita data yang dimiliki kecil dsb;
- I nternet (network) Lambat, hal ini menyebabkan jawaban atas permintaan klien ke server web melambat dan jumlah koneksi maksimum perwaktu jauh di bawah kemampuan server web itu sendiri;
- Sebagian Server Web dalam kondisi mati, Ini dapat terjadi jika ada keperluan yang mendadak untuk perawatan/pembaharuan, kerusakan perangkat keras atau lunak, back end (misalnya Database) gagal, dalam kondisi ini server web yang masih bertugas mengalami kelebihan lalulintas data dan menjadi kelebihan beban.

### Gejala Kelebihan Beban

Tanda-tanda apabila server web mengalami kelebihan beban adalah :



- Lambatnya respon terhadap permintaan dari klien (respon biasanya berkisar dari 1 s.d.Ratusan detik);
- Muncul pesan kesalahan 500, 502, 503, 504 HTTP Errors (Kadang-kadang juga muncul pesan kesalahan 404 dan 408);
- Koneksi TCP ditolak atau direset sebelum isi konten sampai ke klien;
- Hal ini jarang terjadi, hanya sebagian isi konten yang dikirim (tetapi hal ini kebanyakan disebabkan kesalahan program/bug, walaupun sumber daya yang dimiliki sistem terbatas).

### Teknik Pencegahan Kelebihan Beban

- Mengatur lalulintas data jaringan, dengan menggunakan :
  - Firewalls to menghadang data yang tidak diinginkan dari sumber IP yang tidak sesuai ataupun memiliki pola yang aneh.
  - Pengaturan lalulintas data melalui protokol HTTP, untuk memutuskan koneksi, mengarahkan, atau menulis ulang permintaan yang memiliki pola HTTP yang tidak sesuai.
  - Pengaturan Bandwith dan Traffic shaping, untuk menurunkan beban puncakpenggunaan jaringan.
    - Mengembangkan teknik cache;
    - Menggunakan domain yang berbeda, untuk melayani konten yang berbeda (Statis dan dinamis) dengan memisahkan server web, contoh :
      - http://images.example.com
      - http://www.example.com
    - Menggunakan domain yang berbeda dan atau komputer yang berbeda untuk memisahkan berkas berukuran besar dan kecil; idenya adalah untuk mengoptimalkan cache berkas yang ukuran kecil dan menengah dan secara efisien melayani berkas berukuran besar (10-1000 Mb) menggunakan pengaturan yang berbeda;
    - Menggunakan banyak server web pada tiap komputer, masing-masing program server web di arahkan ke masing-masing kartu jaringan dan alamat IP;
    - Menggunakan banyak komputer server web dan menggabungkannya kedalam satu grup bertindak seolah-olah menjadi satu server web besar;
    - Menambahkan perangkat keras seperti RAM, hdd pada tiap server web;
    - Melakukan tuning pada Sistem Operasi sehingga dapat memaksimalkan penggunaan perangkat keras terpasang;

- Menggunakan program komputer yang sesedikit mungkin pada komputer yang digunakan sebagai server web;
- Menggunakan area kerja lain untuk melayani konten-konten yang bersifat dinamis.

### Beberapa contoh Web Server yang sering digunakan di Internet

#### **Web Server Apache**

Apache merupakan web server yang paling banyak dipergunakan di Internet. Program ini pertama kali didesain untuk sistem operasi lingkungan UNIX. Namun demikian, pada beberapa versi berikutnya Apache mengeluarkan programnya yang dapat dijalankan di Windows NT. Berdasarkan sejarahnya, Apache dimulai oleh veteran developer NCSA httpd (National Center for Supercomputing Application). Saat itu pengembangan NCSA httpd sebagai web server mengalami stagnasi. ROB MC COOL meninggalkan NCSA dan memulai sebuah proyek baru bersama para webmaster lainnya, menambal bug, dan menambahkan fitur pada NCSA httpd. Mereka mengembangkan program ini lewat mailing list. Dengan berpijak pada NCSA httpd versi 1.3, Team Apache mengeluarkan rilis pertama kali secara resmi Apache versi 0.6.2. Tim inti pengembang Apache waktu itu : Web server

Apache mempunyai kelebihan dari beberapa pertimbangan di atas :

1. Apache termasuk dalam kategori freeware.
2. Apache mudah sekali proses instalasinya jika dibanding web server lainnya seperti NCSA, IIS, dan lain-lain.
3. Mampu beroperasi pada berbagai platform sistem operasi.
4. Mudah mengatur konfigurasinya. Apache mempunyai hanya empat file konfigurasi.
5. Mudah dalam menambahkan peripheral lainnya ke dalam platform web servernya.

Fasilitas atau ciri khas dari web server Apache adalah :

1. Dapat dijadikan pengganti bagi NCSA web server.
2. Perbaikan terhadap kerusakan dan error pada NCSA 1.3 dan 1.4.
3. Apache merespon web client sangat cepat jauh melebihi NCSA.
4. Mampu di kopilasi sesuai dengan spesifikasi HTTP yang sekarang.
5. Apache menyediakan feature untuk multihomed dan virtual server.

6. Kita dapat menetapkan respon error yang akan dikirim web server dengan menggunakan file atau skrip.
7. Server apache dapat otomatis berkomunikasi dengan client browsernya untuk menampilkan tampilan terbaik pada client browsernya. Misalnya, browser ingin menampilkan dalam bahasa spanyol, maka web server apache otomatis mencari dalam servicenya halaman-halaman dengan bahasa spanyol.
8. Web server Apache secara otomatis menjalankan file index.html, halaman utamanya, untuk ditampilkan secara otomatis pada clientnya.
9. Web server Apache mempunyai level-level pengamanan.
10. Apache mempunyai komponen dasar terbanyak di antara web server lain.
11. Ditinjau dari segi sejarah perkembangan dan prospeknya, Apache web server mempunyai prospek yang cerah. Apache berasal dari web server NCSA yang kemudian dikembangkan karena NCSA masih mempunyai kekurangan di bidang kompatibilitasnya dengan sistim operasi lain. Sampai saat ini, web server Apache terus dikembangkan oleh tim dari apache.org.
12. Performasi dan konsumsi sumber daya dari web server Apache tidak terlalu banyak, hanya sekitar 20 MB untuk file-file dasarnya dan setiap daemonnya hanya memerlukan sekitar 950 KB memory per child.
13. Mendukung transaksi yang aman (secure transaction) menggunakan SSL (secure socket layer).
14. Mempunyai dukungan teknis melalui web.
15. mempunyai kompatibilitas platform yang tinggi.
16. mendukung third party berupa modul-modul tambahan.

### **Web Server Litespeed**

Litespeed web server merupakan teknologi baru yang diciptakan untuk menggantikan Apache Web Server di masa mendatang. Litespeed menurut hasil riset mempunyai kelebihan yaitu 50% lebih cepat dalam memproses PHP dan lebih cepat 6x dibandingkan Apache Web Server.

Ini dia beberapa detail kelebihan Litespeed Web server:

- \* Performa PHP mampu meningkat 50%
- \* Mampu melebihi performa Apache hingga 6x lebih cepat

- \* Pembatasan validasi HTTP request
- \* Anti DDoS
- \* Pencegahan System Overloading
- \* Recover dari kegagalan secara langsung dan otomatis
- \* Kompatibel dengan Cpanel, Plesk dan direct admin
- \* Dukungan kompatibilitas dengan mod\_security request filtering
- \* Kompatibel dengan Apache .htaccess
- \* dll

### **Web Server Nginx**

Nginx dengan cepat memberikan konten statis dengan penggunaan efisien sumber daya sistem. Hal ini dapat menyebarkan dinamis HTTP konten di jaringan menggunakan FastCGI handler untuk script , dan dapat berfungsi sebagai perangkat lunak yang sangat mampu menyeimbangkan beban

Nginx menggunakan asynchronous -event pendekatan untuk menangani permintaan yang diprediksi memberikan kinerja yang lebih rendah beban, kontras dengan Apache HTTP server model yang menggunakan berulir atau proses yang berorientasi pada pendekatan-permintaan penanganan.

#### Fitur yang ada pada webserver Nginx:

1. Handling of static files, index files, and auto-indexing
2. Reverse proxy with caching
3. Load balancing
4. Fault tolerance
5. SSL support
6. FastCGI support with caching
7. Name- and IP-based virtual servers
8. FLV streaming
9. MP4 streaming, using the MP4 streaming module
10. Web page access authentication
11. gzip compression

12. Ability to handle more than 10000 simultaneous connections
13. URL rewriting
14. Custom logging
15. Server-side includes

#### Kelebihan dan Kekurangan

- 1 Performanya yang tinggi, stabil, memiliki banyak fitur
- 2 Mudah dikonfigurasi
- 3 Menggunakan hanya sedikit sumberdaya pada server
- 4 Tidak bergantung kepada thread untuk melayani klien
- 5 Belum support IPV6
- 6 Update/patchnya versi terbarunya lama keluar
- 7 Fast-CGInya tidak berfungsi maksimal
- 8 Pemakainya tidak sebanyak Apache atau IIS (komunitasnya tidak sebanyak Apache atau IIS)

### **Web Server IIS**

Internet Information Service (IIS) adalah komponen yang dapat digunakan untuk mengelola web, File Transfer Protocol (FTP), Gopher, dan NNTP. Komponen IIS terdapat pada sistem operasi Windows NT, Windows 2000, Windows XP, 7 dan Windows Server 2003.

Pada Windows 98, supaya dapat mengelola Web diperlukan komponen Personal Web Server (PWS) walaupun tidak terdapat fasilitas untuk FTP. PWS juga merupakan bagian dari IIS. Komponen PWS terdapat pada CD master Windows 98 dan terletak pada direktori \add-ons\pws. Instalasi PWS dapat dilakukan dari <Drive CD ROOM>:\ADD-ONS|PWS|SETUP.

#### Komponen pendukung IIS antara lain :

1. Protocol jaringan TCP/IP.
2. Domain Name System (DNS).
3. Direkomendasikan untuk menggunakan format NTFS demi keamanan.
4. Software untuk membuat situs web, salah satunya Microsoft FrontPage.

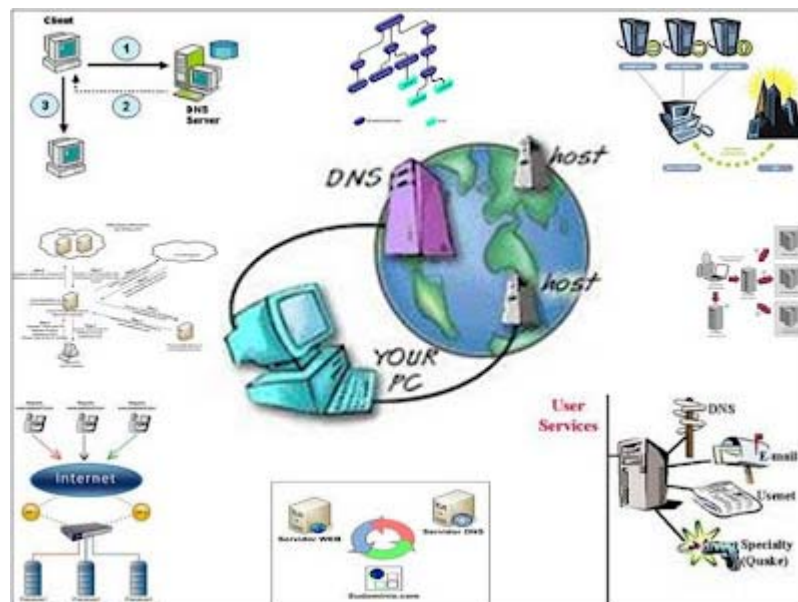
#### Kelebihan dan Kekurangan IIS :

- 1 Lebih kompatibel dengan Windows karena memang IIS adalah keluaran Microsoft
- 2 Unjuk kerja untuk PHP lebih stabil, handal, dan cepat

- 3 Adanya kemampuan diagnostik untuk pelacakan kesalahan (bisa dikustomisasi)
- 4 Untuk platform .NET, user hanya bisa menggunakan IIS
- 5 Memiliki score tertinggi dari web server lainnya untuk masalah bug
- 6 Tidak gratis (web server berbayar)
- 7 Port 80 (Port untuk layanan web) sangat mudah diserang oleh cracker
- 8 Keamanan file log juga sangat mudah ditembus sehingga system password pun akan mudah didapatkan.

Pada pembahasan Internet Information Service ini, yang banyak dibahas adalah Internet Information Service yang terdapat pada Windows 2000 Server dan hanya terbatas pada Files Transfer Protocol (FTP) dan web saja.

## 2. DNS Server



### Sejarah DNS

Pada tahun 1970an jaringan ARPAnet hanya terdiri dari beberapa ratus host saja. Pada waktu itu, sebuah file HOSTS.TXT yang berisi tentang semua informasi host-hosts tersebut masih bisa melayani setiap permintaan query dan menerjemahkan nama ke alamat IP (name-to-address-mapping). Pada sistem operasi berbasis UNIX, file /etc/hosts merupakan hasil dari

pengolahan file HOSTS.TXT tersebut. File HOSTS.TXT pada waktu itu dikelola oleh Stanford Research Institute Network Information Center (SRI-NIC) di Menlo Park, California. File tersebut tersebut didistribusikan ke semua host dan penggunaanya hanya dengan menggunakan satu buah host (mesin/komputer) saja.

Petugas administrasi dari ARPAnet biasanya mengirimkan email kepada SRI-NIC tentang perubahan (termasuk penambahan maupun pengurangan) tentang informasi suatu host, dan dalam periode tertentu, mereka melakukan transfer file HOSTS.TXT yang paling baru (biasanya diperbaharui sekali dalam seminggu) dengan menggunakan protokol ftp. Seiring dengan berkembangnya jaringan ARPAnet dan penggunaan protokol TCP/IP, ukuran dari file HOSTS.TXT menjadi besar dengan bertambahnya jumlah host yang bergabung dengan jaringan ARPAnet. Kemudian timbul beberapa masalah dengan penggunaan file HOSTS.TXT ini, misalnya :

- **Trafik dan Beban (Traffic and load):** Beban mesin dan trafik (bandwidth) di SRI-NIC dalam mendistribusikan file menjadi lebih berat dan besar
- **Penamaan yang saling bentrok (name collisions):** Pada file HOSTS.TXT tidak diperkenankan adanya dua buah nama host yang sama. Namun pada prakteknya, tidak ada cara untuk mencegah seseorang untuk menambahkan nama yang sama sehingga kemungkinan bisa menjadi bentrok dan pada akhirnya merusak skema yang telah ada
- **Keaslian (consistency):** Mengelola keaslian dan keutuhan sebuah file antar beberapa jaringan yang sedang berkembang pesat merupakan sesuatu hal yang sulit dilakukan

Berangkat dari masalah-masalah tersebut diatas, ARPAnet membentuk suatu sistem alternatif pengganti dari sistem lama yang menggunakan file HOSTS.TXT. Tujuannya adalah untuk memecahkan masalah dalam pengelolaan tabel host yang sangat beraneka ragam dan masih menggunakan metode sentralisasi. Pada sistem yang baru, seorang sistem administrator memungkinkan untuk mengelola data secara loka, namun akan selalu update secara global di internet. Sistem yang menggunakan metode desentralisasi ini diharapkan akan mengurangi beban dan trafik, serta pengelolaan data dan proses update dari sebuah informasi akan menjadi lebih mudah.

Paul Mockapertis dari University of Southern California Information Science Institute di Marina del Rey, California, dipilih sebagai orang yang bertanggung jawab terhadap rancangan, desain, arsitektur dan implementasi dari sistem pengelolaan data host yang baru. Pada tahun 1984 beliau merilis RFC (Request For Comment) 882 dan RFC 883 yang menjelaskan tentang Domain Name System (DNS). Kemudian disusul dengan RFC 1034 dan RFC 1035 yang juga menambahkan tentang masalah keamanan DNS, penerapan (implementasi), pengelolaan

(administrative), mekanisme pembaharuan data secara dinamis, serta keamanan data dalam sebuah domain dan lain-lainnya.

### Pengertian DNS

DNS (Domain Name System / Sistem Penamaan Domain) Adalah sistem berbentuk database terdistribusi yang akan memetakan/mengkonversikan nama host/mesin/domain ke alamat IP (Internet Protocol) dan sebaliknya. DNS menerjemahkan sebuah domain name ke IP address dan salah satu jenis system yang melayani permintaan pemetaan IP address ke FQDN (Fully Qualified Domain Name) dan dari FQDN ke IP address. DNS biasanya digunakan pada aplikasi yang berhubungan ke internet seperti Web Browser atau e-mail, Dimana DNS membantu memetakan host name sebuah computer ke IP address. Selain digunakan di internet DNS juga dapat di implementasikan ke private network atau internet.

DNS menyediakan servis yang cukup penting untuk Internet, bilamana perangkat keras komputer dan jaringan bekerja dengan alamat IP untuk mengerjakan tugas seperti pengalamatan dan penjaluran (routing), manusia pada umumnya lebih memilih untuk menggunakan nama host dan nama domain, contohnya adalah penunjukan sumber universal (URL) dan alamat e-mail. DNS menghubungkan kebutuhan ini. Beberapa jenis perangkat lunak DNS yang menerapkan metode DNS seperti: BIND, djbdns, MaraDNS, QIP, NSD, PowerDNS, Microsoft DNS.

### Fungsi DNS

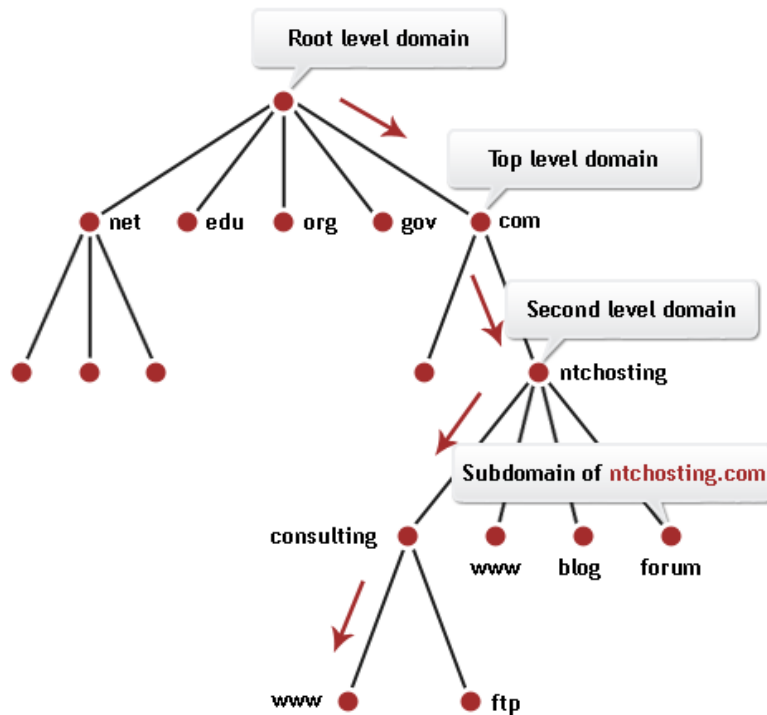
Fungsi utama dari sebuah sistem DNS adalah menerjemahkan nama-nama host (hostnames) menjadi nomor IP (IP address) ataupun sebaliknya, sehingga nama tersebut mudah diingat oleh pengguna internet. Fungsi lainnya adalah untuk memberikan suatu informasi tentang suatu host ke seluruh jaringan internet. Menyediakan keluwesan untuk kegagalan computer, Beberapa server DNS memberikan perlindungan untuk setiap domain. Tepatnya, Tiga belas server akar (root server) digunakan oleh seluruh dunia.

### Kelebihan dan Kekurangan DNS

- DNS mudah untuk di implementasikan di protocol TCP/IP
- DNS server mudah untuk di konfigurasi (Bagi admin)
- User tidak lagi di repotkan untuk mengingat IP address
- DNS tidak mudah untuk di implementasikan
- Tidak konsisten
- Tidak bias membuat banyak nama domain.



## Konsep dan hirarki DNS



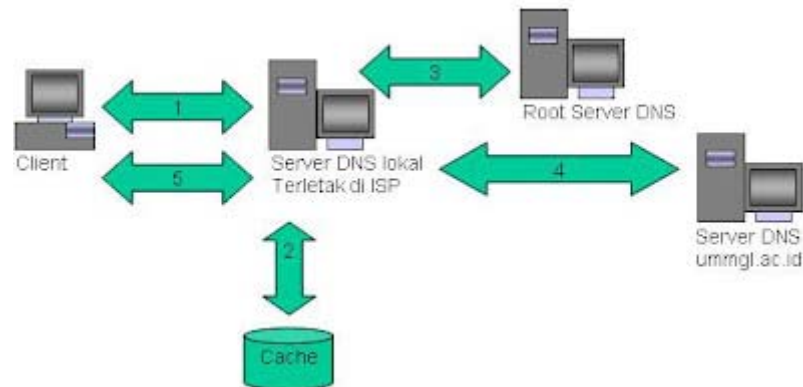
Struktur database DNS berbentuk hierarki atau pohon yang memiliki beberapa cabang. Cabang-cabang ini mewakili domain, dan dapat berupa host, subdomain, ataupun top level domain.

Struktur dari database DNS bisa diibaratkan dengan dengan struktur file dari sebuah sistem operasi UNIX. Seluruh database digambarkan sebagai sebuah struktur terbalik dari sebuah pohon (tree) dimana pada puncaknya disebut dengan root node. Pada setiap node dalam tree tersebut mempunyai keterangan (label) misalnya, .org, .com, .edu, .net, .id dan lain-lainnya, yang relatif terhadap puncaknya (parent). Ini bisa diibaratkan dengan relative pathname pada sistem file UNIX, seperti direktori bin, usr, var, etc dan lain sebagainya. Pada puncak root node dalam sebuah sistem DNS dinotasikan dengan "." atau "/" pada sistem file UNIX.

Domain teratas adalah root. Domain ini diwakili oleh titik. Selanjutnya, domain yang terletak tepat di bawah root disebut top level domain. Beberapa contoh top level domain ini antara lain com, edu, gov, dan lain-lain. Turunan dari top level domain disebut subdomain. Domain yang terletak setelah top level domain adalah second level domain, dan domain yang berada di bawah second level domain disebut third level domain, begitu seterusnya.

## Cara kerja DNS

Secara sederhana cara kerja DNS bisa dilihat pada gambar berikut ini:

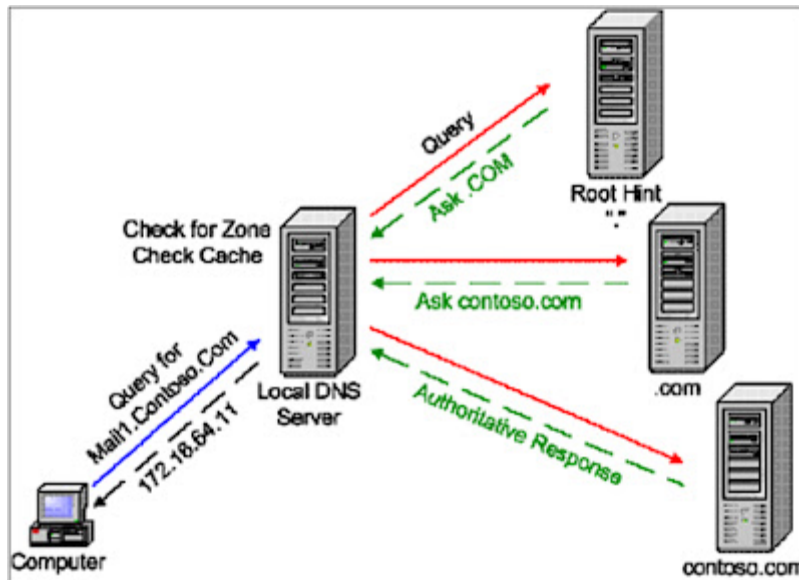


DNS menggunakan relasi client – server untuk resolusi nama. Pada saat client mencari satu host, maka ia akan mengirimkan query ke server DNS. Query adalah satu permintaan untuk resolusi nama yang dikirimkan ke server DNS.

Pada komputer Client, sebuah program aplikasi misalnya http, meminta pemetaan IP Address (forward lookup query). Sebuah program aplikasi pada host yang mengakses domain system disebut sebagai resolver, resolver menghubungi DNS server, yang biasa disebut name server.

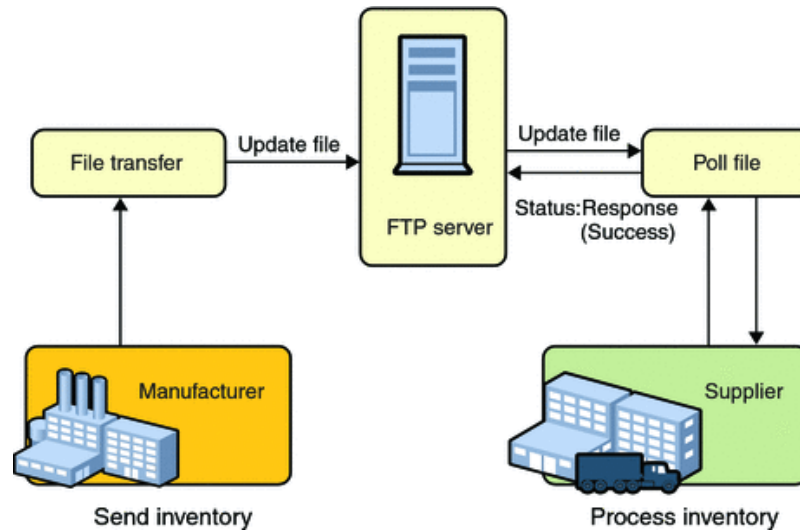
Name server meng-cek ke local database, jika ditemukan, name server mengembalikan IP Address ke resolver jika tidak ditemukan akan meneruskan query tersebut ke name server root server. Terakhir barulah si client bisa secara langsung menghubungi sebuah website / server yang diminta dengan menggunakan IP Address yang diberikan oleh DNS server. Ketika anda melakukan query (bisa berupa ping, ssh, dig, host, nslookup, email, dan lain sebagainya) ke sebuah host misalnya durmagati.ee.kurowo.edu maka name server akan memeriksa terlebih dahulu apakah ada record host tersebut di cache name server lokal. Jika tidak ada, name server lokal akan melakukan query kepada root server dan mereferensikan name server untuk TLD .edu , name server lokal kembali melakukan query kepada name server .edu dengan jenis query yang sama

Jika permintaan tidak ada pada database, name server akan menghubungi server root dan server lainnya dengan cara sebagai berikut :



1. Saat kita mengetikkan sebuah nama domain misalnya <http://www.neon.cs.virginia.edu> pada web browser, maka aplikasi http (resolver) akan mengirimkan query ke Name Server DNS Server local atau DNS Server Internet Service Provider.
2. Awalnya name server akan menghubungi server root. Server root tidak mengetahui IP Address domain tersebut, ia hanya akan memberikan IP Address server edu.
3. Selanjutnya name server akan bertanya lagi pada server edu berupa IP Address domain [neon.cs.virginia.edu](http://www.neon.cs.virginia.edu). Server edu tidak mengetahui IP Address domain tersebut, ia hanya akan memberikan IP Address server [virginia.edu](http://www.virginia.edu).
4. Selanjutnya name server akan bertanya ke server [virginia.edu](http://www.virginia.edu) tentang IP Address [neon.cs.virginia.edu](http://www.neon.cs.virginia.edu). Dan server [virginia.edu](http://www.virginia.edu) hanya mengetahui dan memberikan jawaban berupa IP Address server [cs.virginia.edu](http://www.cs.virginia.edu)
5. Selanjutnya name server akan bertanya ke server [cs.virginia.edu](http://www.cs.virginia.edu) tentang IP Address [neon.cs.virginia.edu](http://www.neon.cs.virginia.edu). Dan barulah [cs.virginia.edu](http://www.cs.virginia.edu) mengetahui dan menjawab berapa IP Address domain [neon.cs.virginia.edu](http://www.neon.cs.virginia.edu).
6. Terakhir barulah computer client bisa secara langsung menghubungi domain [neon.cs.virginia.edu](http://www.neon.cs.virginia.edu) dengan menggunakan IP Address yang diberikan oleh server [cs.virginia.edu](http://www.cs.virginia.edu).
7. IP Address milik [neon.cs.virginia.edu](http://www.neon.cs.virginia.edu) kemudian akan disimpan sementara oleh DNS server Anda untuk keperluan nanti. Proses ini disebut caching, yang berguna untuk mempercepat pencarian nama domain yang telah dikenalnya.

### 3. FTP Server



FTP server merupakan sebuah server yang memanfaatkan File Transfer Protocol (FTP) untuk keperluan transfer file antar mesin pada jaringan TCP/IP. FTP adalah sebuah protokol Internet yang berjalan di dalam lapisan aplikasi yang merupakan standar untuk pentransferan berkas komputer antar mesin-mesin dalam sebuah jaringan internet atau intranet.

FTP server, berupa sebuah komputer server yang memberikan fasilitas FTP dengan tujuan untuk menerima koneksi (hubungan) dari luar. Biasanya komputer dengan fasilitas sebagai FTP server juga berfungsi sebagai web server.

Ada dua jenis server komputer yang dapat dihubungkan dengan fasilitas FTP, yaitu :

a) Anonymous FTP Server atau dapat juga disebut Public FTP Server. Server komputer ini dapat diakses dan terbuka bagi semua pemakai internet. File-file dalam server ini dapat di-download secara gratis. Untuk menggunakan Anonymous FTP ini pengguna memasukkan login dengan username Anonymous dan password yang dipakai berupa alamat e-mail atau dapat pula menggunakan username guest tanpa password, hal ini tergantung dari server FTP yang dituju.

b) Private FTP Server, Server komputer ini hanya bisa diakses dan dipergunakan oleh user tertentu yang terdaftar secara resmi. Server ini biasanya berisi data dan informasi pribadi yang khusus digunakan untuk pemakai tertentu atau perusahaan tertentu. Pemakai khusus ini biasanya mempunyai username dan password untuk dapat terhubung dengan server jenis ini. Sebuah server yang memberikan fasilitas FTP dapat dengan mudah dikenali, biasanya sebuah server FTP

akan memiliki alamat situs dengan subdomain FTP, misalnya domain microfosft.com memberikan fasilitas FTP pada subdomain ftp.microsoft .com.

#### Keamanan FTP Server :

FTP sebenarnya tidak aman untuk melakukan tukar menukar file antar jaringan karena tidak adanya proses enkripsi terlebih dahulu. FTP dalam melakukan tranfer data menggunakan metode Clear Text yang mana user, password dan data yang anda kirim dapat dengan mudah untuk di intip (sniff) oleh sebuah progam aplikasi seperti protocol analyzer misalnya WireShark. Meskipun begitu ada cara lain yang dapat di gunakan untuk membuat proses tukar menukar file dengan menggunakan FTP menjadi aman, yaitu dengan menggunakan SFTP (SSH FTP) yaitu FTP berbasis SSH atau juga dengan FTPS yaitu FTP yang di bungkus dengan protocol SSL ( FTP Over SSL).

#### Fungsi FTP Server :

- Untuk tujuan sharing data
- Untuk menyediakan indirect atau implicit remote computer
- Untuk menyediakan tempat penyimpanan bagi user
- Untuk menyediakan transfer data yang reliable dan efisien

#### Tujuan pembangunan FTP Server

- Sharing data
- Menyediakan indirect atau implicit remote computer
- Menyediakan tempat penyimpanan bagi user
- Menyediakan transfer data yang reliable dan efisien

#### Contoh aplikasi FTP server :

- Proftpd
- Vsftpd
- Wuftpd
- IIS (didalamnya terdapat FTP Server)

## Perintah FTP Server

Perintah-perintah FTP yang dikirimkan terdiri atas string teks sederhana. Sebagai contoh, untuk mendapatkan kembali file, client mengirimkan “RETR filename” di koneksi kendali ke FTP server. Untuk mentransfer file, client mengirimkan “STOR filename”. FTP server mengetahui setiap perintah pada setiap balasan FTP, dimana terdiri atas tiga digit. Digit pertama menandai adanya tanggapan yang baik, tidak baik, atau yang tidak sempurna. Jika satu kesalahan terjadi, maka digit kedua digunakan untuk mendeteksi kesalahan yang terjadi. Dengan cara yang sama, digit ketiga digunakan untuk lebih menspesifikasikan kesalahan yang terjadi. Digit pertama merupakan digit yang paling utama, dan kemungkinan nilai yang muncul adalah sebagai berikut :

1. *1yz Positive Preliminary reply*. Permintaan diketahui, namun balasan lain dari client tetap diharapkan
2. *2yz Positive Completion reply*. Permintaan sukses dilakukan, sehingga client dapat mengirim permintaan lain
3. *3yz Positive Intermediate reply*. Perintah telah diterima, namun masih membutuhkan informasi yang lain. Client diharuskan untuk mengirimkan balasan perintah lainnya
4. *4yz Transient Negative reply*. Perintah gagal, namun masih ada kesempatan untuk mencobanya lagi
5. *5yz Permanent Negative Completion reply*. Perintah gagal, namun tidak harus diulangi lagi

Contoh perintah FTP :

- Untuk mengubah direktori yang dikirimkan oleh client :

*CWD namadirektori*

Server akan merespon dengan :

*250 CDW command successful*

Sebagai balasan, dimulai dengan a '2', dimana urutan perintah diselesaikan.

- Bila ingin merubah salah satu direktori dan itu tidak ada, maka perintahnya :

*CWD namadirektoriyanghilang*

Server akan merespon dengan :

*550 namadirektoriyanghilang : The system cannot find the file spesified*

Balasannya ialah a '5', berarti gagal dan tetap gagal jika diulangi (kecuali direktori hilang diciptakan di server).

- Sesi Perintah (Session Commands)

Untuk memulai sesi perintah FTP, maka perintah dari USER yang dikirimkan ke server adalah :

*USER chafid*

Server akan memberikan balasan :

*331 Password required for javaftp*

Client harus memberikan balasan dengan mengisi password :

*PASS 123456*

Server akan memberikan balasan :

*230 User chafid logged in*

Setelah login user dapat menggunakan perintah yang berhubungan dengan direktori dan file.

Untuk mengakhiri, client mengirimkan perintah sebagai berikut :

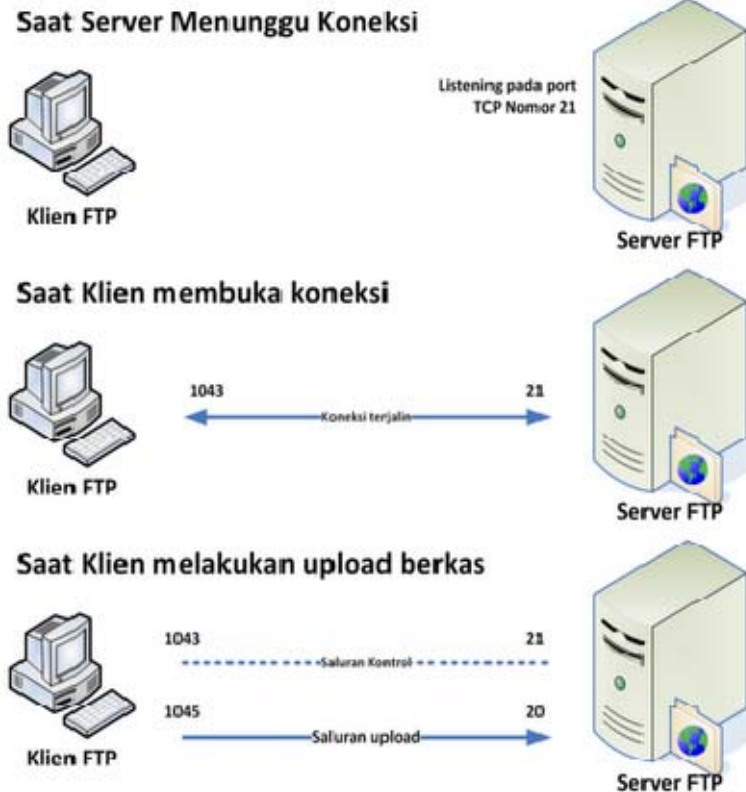
*QUIT*

Server akan memberikan balasan :

*221*

Sesi akhirnya ditutup, sehingga perintah apapun yang dikirimkan sudah tidak diterima lagi.

Untuk prosesnya dapat dilihat dari gambar berikut ini :



Sebelum membuat koneksi, port TCP nomor 21 di sisi server akan “mendengarkan” percobaan koneksi dari sebuah klien FTP dan kemudian akan digunakan sebagai port pengatur (control port) untuk (1) membuat sebuah koneksi antara klien dan server, (2) untuk mengizinkan klien untuk mengirimkan sebuah perintah FTP kepada server dan juga (3) mengembalikan respons server ke perintah tersebut. Sekali koneksi kontrol telah dibuat, maka server akan mulai membuka port TCP nomor 20 untuk membentuk sebuah koneksi baru dengan klien untuk mentransfer data aktual yang sedang dipertukarkan saat melakukan pengunduhan dan pengunggahan.

FTP hanya menggunakan metode autentikasi standar, yakni menggunakan username dan password yang dikirim dalam bentuk tidak terenkripsi. Pengguna terdaftar dapat menggunakan username dan password-nya untuk mengakses, men-download, dan meng-upload berkas-berkas yang ia kehendaki. Umumnya, para pengguna terdaftar memiliki akses penuh terhadap beberapa direktori, sehingga mereka dapat membuat berkas, membuat direktori, dan bahkan menghapus berkas. Pengguna yang belum terdaftar dapat juga menggunakan metode anonymous login, yakni dengan menggunakan nama pengguna anonymous dan password yang diisi dengan menggunakan alamat e-mail.



## 4. RPC

RPC adalah suatu protokol yang menyediakan suatu mekanisme komunikasi antar proses yang memungkinkan suatu program untuk berjalan pada suatu komputer tanpa terasa adanya eksekusi kode pada sistem yang jauh ( remote system ). RPC mengasumsikan keberadaan dari low-level protokol transportasi seperti TCP atau UDP untuk membawa pesan data dalam komunikasi suatu program. Protokol RPC dibangun diatas protokol eXternal Data

Representation (XDR), yang merupakan standar dari representasi data dalam komunikasi remote. Protokol XDR mengubah parameter dan hasil dari tiap servis RPC yang disediakan. Protokol RPC memungkinkan pengguna (users) untuk bekerja dengan prosedur remote sebagaimana bekerja dengan prosedur lokal. Prosedur panggilan remote (remote procedure calls) didefinisikan melalui rutin yang terkandung didalam protokol RPC. Tiap message dari panggilan akan disesuaikan dengan message balikan. Protokol RPC sendiri sebenarnya adalah suatu protokol untuk ”meneruskan pesan” yang mengimplementasikan protokol non-RPC lain seperti panggilan remote batching dan broadcasting. Protokol ini juga mendukung adanya prosedur callback dan select subroutine pada sisi server.

Namun demikian sebenarnya RPC dikembangkan dari pemanggilan prosedur lokal/konvensional pada satu sistem komputer yang biasa disebut sebagai *Procedure Call* saja. *Procedure Call* sendiri adalah suatu mekanisme pemanggilan/penanganan antar proses dalam satu sistem komputer.

Jadi diperlukan ruang pengalamatan yang sama (*the same address space*) agar dimungkinkan pemanggilan suatu prosedur. Dua proses mungkin saja berjalan dalam satu sistem yang sama namun bisa juga berada pada sistem yang berbeda yang terhubung melalui *network* seperti asumsi diatas.

Dengan RPC, para *programmer* aplikasi terdistribusi dapat menghindarkan diri dari kerumitan antar muka/*interface* pada *network*. Kebebasan *transport* dari suatu RPC dapat melindungi aplikasi dari elemen-elemen fisik dan logik atas mekanisme komunikasi dan memungkinkan aplikasi menggunakan variasi sistem *transport*. RPC membuat model *client/server* menjadi *powerful* dan mudah diprogram.

Adapun tujuan akhirnya adalah membuat program yang bisa menerapkan sistem komputasi *client-server* dengan *Remote Procedure Call* dimana data yang dipertukarkan terformat sebagai dokumen XML. Hal inilah yang dikenal sebagai XMLRPC.

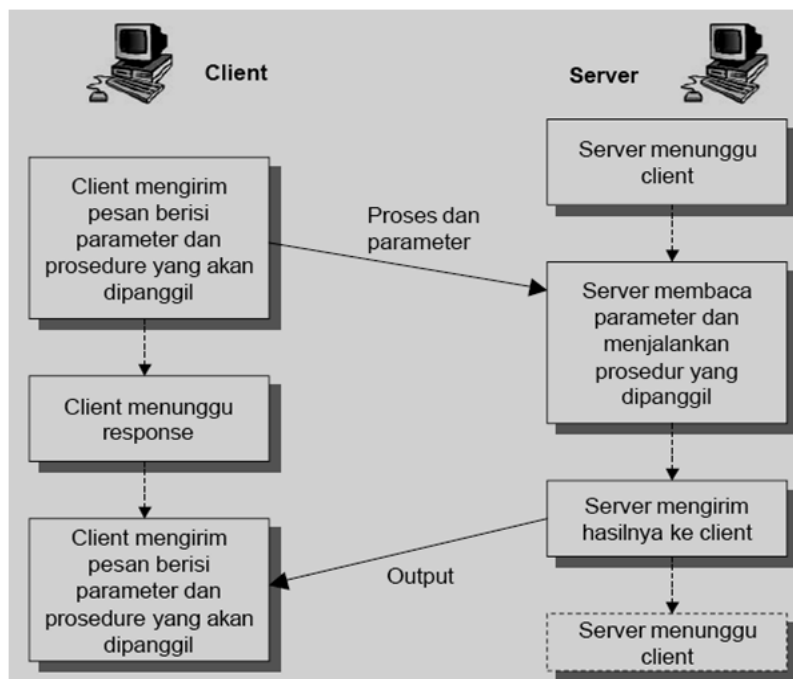
### Kelebihan RPC

- Pemanggilan remote procedure tidak jauh berbeda dibandingkan pemanggilan local procedure. Sehingga pemrogram dapat berkonsentrasi pada software logic, tidak perlu memikirkan low level details seperti socket, marshalling & unmarshalling. Robust (Sempurna): Sejak th 1980-an RPC telah banyak digunakan dlm pengembangan mission-critical application yg memerlukan scalability, fault tolerance, & reliability.

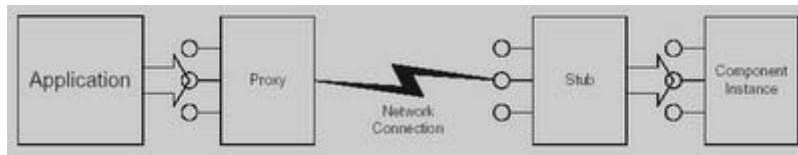
### Kekurangan RPC

- Tidak fleksibel terhadap perubahan:
  - Static relationship between client & server at run-time.
- Berdasarkan prosedural/structured programming yang sudah ketinggalan jaman dibandingkan OOP.

### Prinsip RPC dalam program Client-Server

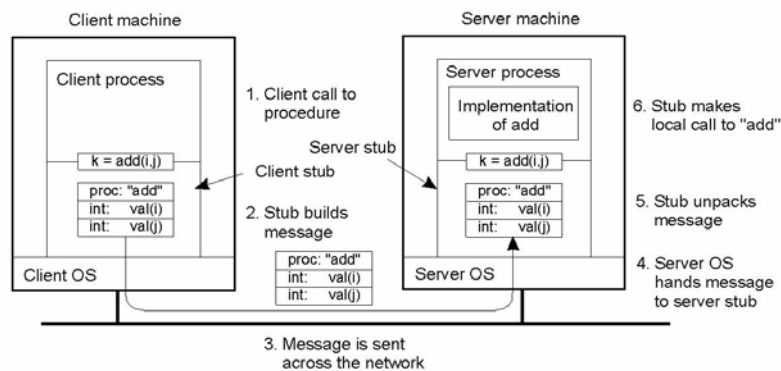


Skema RPC ini dilakukan juga pada proses-proses yang running di komputer berlainan



- Sebelum mekanisme RPC digunakan, data harus di-packaging ke dalam format transmisi. Langkah ini dinamakan marshalling.
- Proxy bertanggung jawab untuk marshalling data, kemudian mengirimkan data dan meminta instans dari komponen (remote)
- Stub menerima request, unmarshall data, dan memanggil method yang diminta. Kemudian proses mengembalikan nilai yang diinginkan

### Langkah-langkah dalam RPC



1. Prosedur client memanggil client stub
2. Client stub membuat pesan dan memanggil OS client
3. OS client mengirim pesan ke OS server
4. OS server memberikan pesan ke server stub
5. Server stub meng-unpack parameter-parameter untuk memanggil server
6. Server mengerjakan operasi, dan mengembalikan hasilnya ke server stub
7. Server stub mem-pack hasil tsb dan memanggil OS server
8. OS server mengirim pesan (hasil) ke OS client
9. OS client memberikan pesan tersebut ke client stub
10. Client stub meng-unpack hasil dan mengembalikan hasil tersebut ke client

## Object Remote

Meskipun teknologi RPC ini relatif sudah memberikan kenyamanan bagi developer, tapi perkembangan yang terjadi di bidang pemrograman berorientasi objek akhirnya menuntut kehadiran teknologi baru. Sederet teknologi akhirnya benar-benar muncul, antara lain; RMI (Remote Method Invocation), CORBA (Common Object Request Broker Architecture), dan SOAP (Simple Object Access Protocol).

## Protokol Message RPC

Protokol Message RPC didefinisikan dengan menggunakan deskripsi data eXternal Data Representation ( XDR ) yang meliputi struktur, enumerasi dan union. Pembahasan lebih lanjut akan diterangkan pada bab berikutnya mengenai implementasi RPC.

Protokol Message ini membutuhkan faktor-faktor pendukung sebagai berikut :

1. Spesifikasi yang unik untuk tiap prosedur call
2. Respon message yang sesuai untuk tiap message yang diminta
3. Otentifikasi klien untuk tiap layanan dan sebaliknya Protokol Message RPC memiliki dua ( 2 ) struktur yang berbeda, yaitu call message dan reply message. Tiap klien yang akan melakukan RPC pada suatu server di jaringan akan menerima balasan (reply) berupa hasil dari eksekusi prosedur tersebut. Dengan menggunakan spesifikasi yang unik untuk tiap prosedur remote, maka RPC dapat mencocokkan message balasan untuk tiap call message yang diminta klien.

## Call Message

Tiap call message pada RPC mengandung nilai-nilai unsigned integer yang digunakan untuk mengidentifikasi prosedur remote yang diminta. Nilai-nilai ini adalah :

1. Nomor Program
2. Nomor Versi dari Program
3. Nomor Prosedur

## Reply Message

Reply message yang dikirimkan oleh server jaringan bervariasi tergantung apakah call messages yang diminta klien diterima atau ditolak. Reply message mengandung informasi yang

digunakan untuk membedakan kondisi-kondisi yang diminta sesuai dengan call messages. Informasi ini antara lain :

1. RPM mengeksekusi call message dengan sukses
2. Implementasi remote tidak sesuai dengan protokol yang digunakan. Versi yang lebih rendah atau tinggi akan ditolak.
3. Program remote tidak tersedia pada sistem remote
4. Program remote tidak mendukung versi yang diminta klien
5. Nomor prosedur yang diminta tidak ada.

### Fitur dalam RPC

RPC memiliki fitur - fitur sebagai berikut :

- batching calls
- broadcasting calls
- callback procedures
- using the select subroutine

### **Batching Calls**

Fitur Batching calls memungkinkan klien untuk mengirim message calls ke server dalam jumlah besar secara sequence ( berurutan ). Batching menggunakan protokol streaming byte seperti TCP / IP sebagai mediumnya. Pada saat melakukan batching, klien tidak menunggu server untuk memberikan reply terhadap tiap messages yang dikirim, begitu pula dengan server yang tidak pernah mengirimkan messages reply. Fitur inilah yang banyak digunakan klien, karena arsitektur RPC didesain agar pada tiap call message yang dikirimkan oleh klien harus ada proses menunggu balasan dari server. Oleh karena itu maka pihak klien harus dapat mengatasi error yang kemungkinan terjadi karena pihak klien tidak akan menerima peringatan apabila terjadi error pada message yang dikirim.

### **Broadcasting Calls**

Fitur Broadcasting memungkinkan klien untuk mengirimkan paket data ke jaringan dan menunggu balasan dari network. Fitur ini menggunakan protokol yang berbasiskan paket data

seperti UDP/IP sebagai mediumnya. Broadcast RPC membutuhkan layanan port mapper RPC untuk mengimplementasikan fungsinya.

### **Callback Procedures**

Fitur Callback Procedures memungkinkan server untuk bertindak sebagai klien dan melakukan RPC callback ke proses yang dijalankan oleh klien.

### **Using the select subroutine**

Fitur ini akan memeriksa deskripsi dari suatu file dan messages dalam antrian untuk melihat apakah mereka siap untuk dibaca (diterima) atau ditulis (dikirim), atau mereka dalam kondisi ditahan sementara. Prosedur ini memungkinkan server untuk menginterupsi suatu aktivitas, memeriksa datanya, dan kemudian melanjutkan proses aktivitas tersebut.

### Otentifikasi RPC

Proses otentifikasi adalah proses yang digunakan untuk mengidentifikasi server dan klien pada RPC. Untuk setiap prosedur remote yang dilakukan protokol RPC menyediakan slot yang dipakai sebagai parameter otentifikasi yang berfungsi agar pemanggil (caller) dapat, memberikan identitasnya kepada server. Parameter otentifikasi ini dibuat di paket klien.

Otentifikasi RPC terdiri atas beberapa bagian. Berikut ini adalah bagian-bagian pada otentifikasi RPC :

#### 1. Protokol Otentifikasi RPC

Protokol Otentifikasi RPC disediakan sebagai bagian dari protokol RPC. Untuk setiap prosedur remote, semuanya diotentifikasi oleh paket RPC pada server. Parameter yang digunakan adalah respon verifier. Sedangkan pada pihak klien, setiap paket RPC diberikan parameter otentifikasi dan parameter yang digunakan adalah credential dan verifier.

#### 2. Otentifikasi NULL

Otentifikasi NULL digunakan pada sistem dimana pemanggil (caller) RPC tidak mengetahui identitasnya sendiri dan server tidak membutuhkan identitas pemanggil.

### 3. Otentifikasi UNIX

Otentifikasi Unix digunakan pada prosedur remote di sistem UNIX. Jenis otentifikasi ini dibagi dua (2) yaitu otentifikasi pada sisi klien dan otentifikasi pada sisi server. Pada sisi klien, otentifikasi ini akan membuat otentifikasi handle dengan AIX permissions agar dapat berasosiasi dengan parameter credentials pada sistem UNIX. Sedangkan pada sisi server, server harus dapat menentukan tipe otentifikasi yang diberikan oleh pemanggil RPC. Penentuan dukungan terhadap tipe otentifikasi akan memberikan reply yang berbeda.

### 4. Otentifikasi Data Encryption Standard ( DES )

Otentifikasi DES membutuhkan keyserv daemon yang harus berjalan baik di sisi server maupun klien. Tiap pengguna pada sistem ini harus memiliki kunci public ( public key yang disahkan pada database kunci publik oleh Administrator jaringan tersebut.

### 5. Protokol Otentifikasi DES

Protokol Otentifikasi DES meliputi protokol penanganan DES pada proses otentifikasi RPC. Protokol ini mencakup 64-bit blok data DES yang terenkripsi dan menentukan panjang maksimum untuk user name pada jaringan yang digunakan.

### 6. Enkripsi Diffie-Hellman

Enkripsi Diffie-Hellman digunakan pada pembuatan kunci public pada otentifikasi DES dengan menggunakan 192-bit kunci. Enkripsi ini memiliki dua buah variable onstan, yaitu BASE dan MODULUS yang digunakan pada protokol otentifikasi DES. PC berhubungan hanya dengan proses otentifikasi, tidak dengan kontrol akses terhadap erVICES/layanan individual yang diberikan. Tiap layanan mengimplementasikan eraturan mengenai kontrol akses masing-masing.

Sumber :

Web Server

<http://radensomad.com/pengertian-web-server-hosting-domain-name-server-dns-dan-domain.html>

<http://amif.wordpress.com/2008/07/25/pengertian-dan-kelebihan-web-server/>

<http://naughtyric.blogspot.com/2011/10/konsep-dasar-pemrograman-web-server.html>

<http://radensomad.com/pengertian-web-server-hosting-domain-name-server-dns-dan-domain.html>

## DNS Server

<http://trimawati.wordpress.com/2008/07/25/pengertianfungsikeunggulan-dan-kekurangn-dns-server/>

<http://hanyaingin.1sthost.org/index.php/menu-artikel/artikel-linux-hanya-ingin/69-pengertian-dns-server>

[http://gcoz.blogspot.com/2011/03/konfigurasi-dns-domain-name-server\\_27.html](http://gcoz.blogspot.com/2011/03/konfigurasi-dns-domain-name-server_27.html)

<http://aquaer.wordpress.com/2011/02/14/dns-domain-name-server/>

<http://www.catatanteknisi.com/2011/01/pengertian-prinsip-cara-kerja-dns.html>

## FTP Server

<http://adhit.web.id/cara-kerja-ftp-server-instalasi-dan-konfigurasi-vsftpd/>

<http://piyan32.wordpress.com/2008/05/29/definisi-ftp-server/>

<http://opensuse.or.id/panduan/server-setup/opensuse-sebagai-ftp-server/setup-ftp-server-pada-opensuse-menggunakan-yast/>

<http://agus08.wordpress.com/tutorial/instalasi-win-2000-server/ftp-server/>

<http://shofiutami.blogspot.com/2009/06/pengertian-ftp-server-pengertian-ftp.html>

## RPC

<http://handaru.blogsome.com/category/xmlrpc/>

<http://blog.uad.ac.id/erwan/2010/10/09/rpc-dan-rmi/>

<http://blog.uad.ac.id/andex/2010/10/07/rpc-dan-rmi-2/>

<http://sobatbaru.blogspot.com/2010/12/pengertian-remote-procedure-calls-rpc.html>