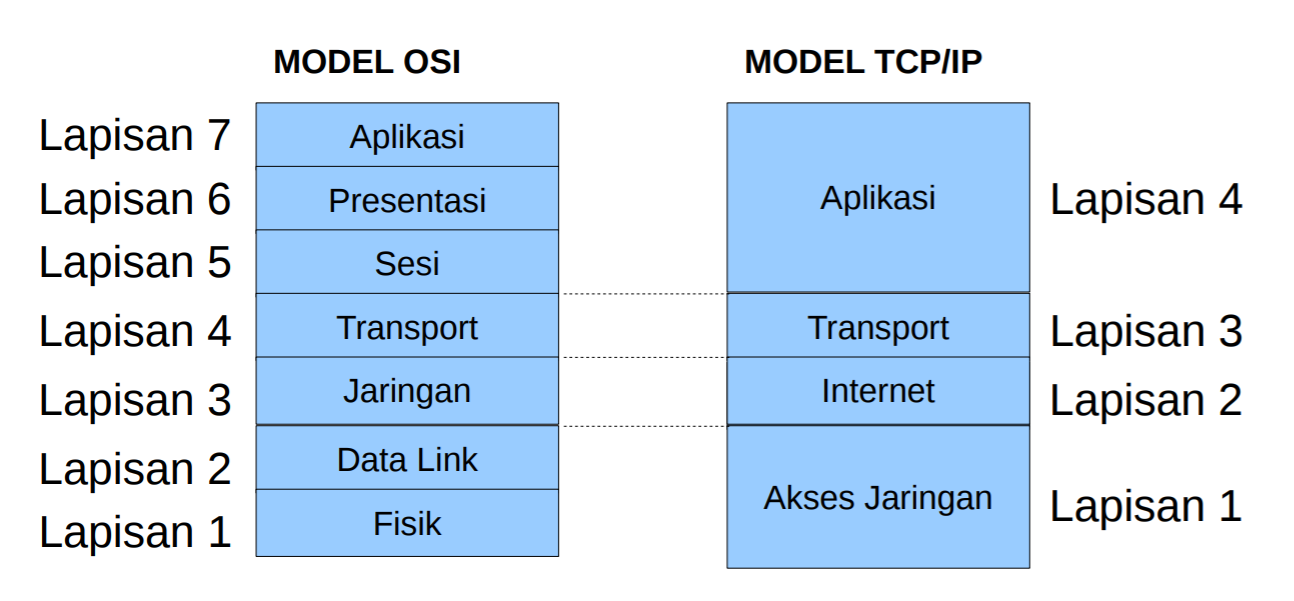
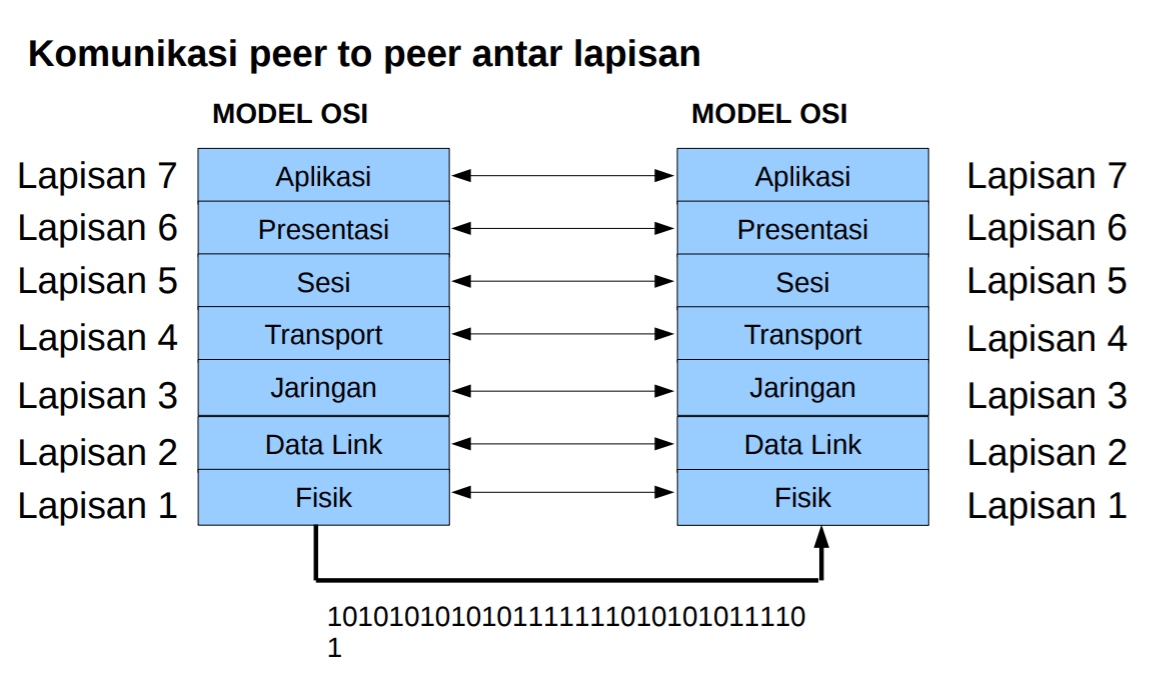
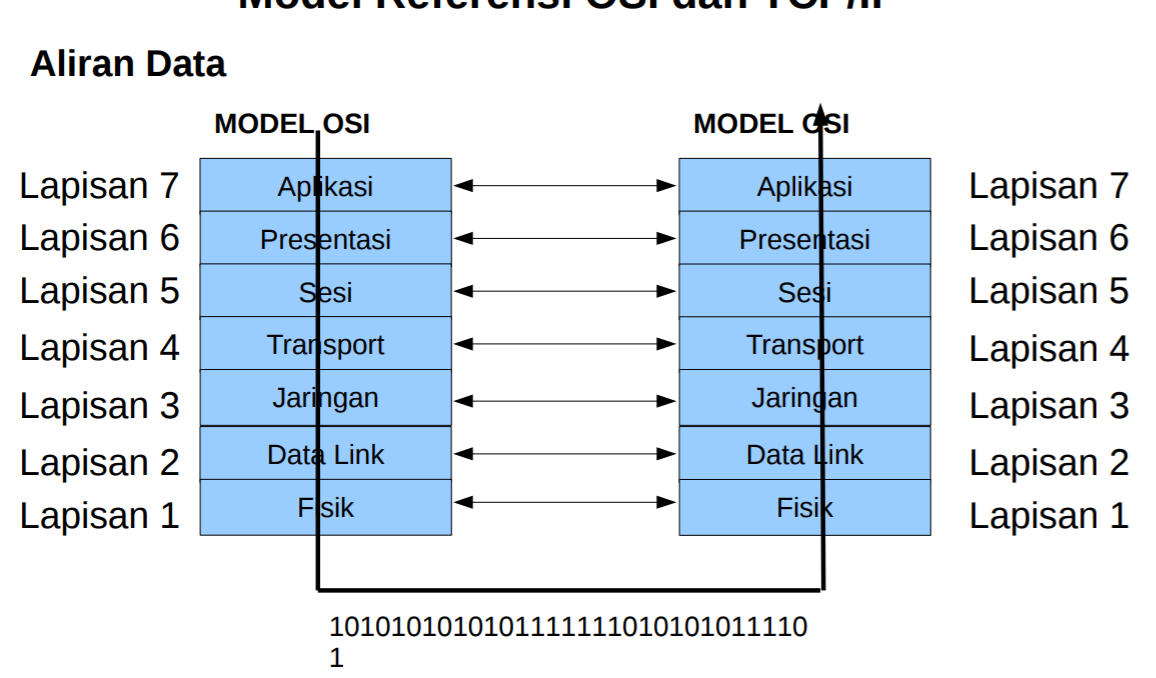
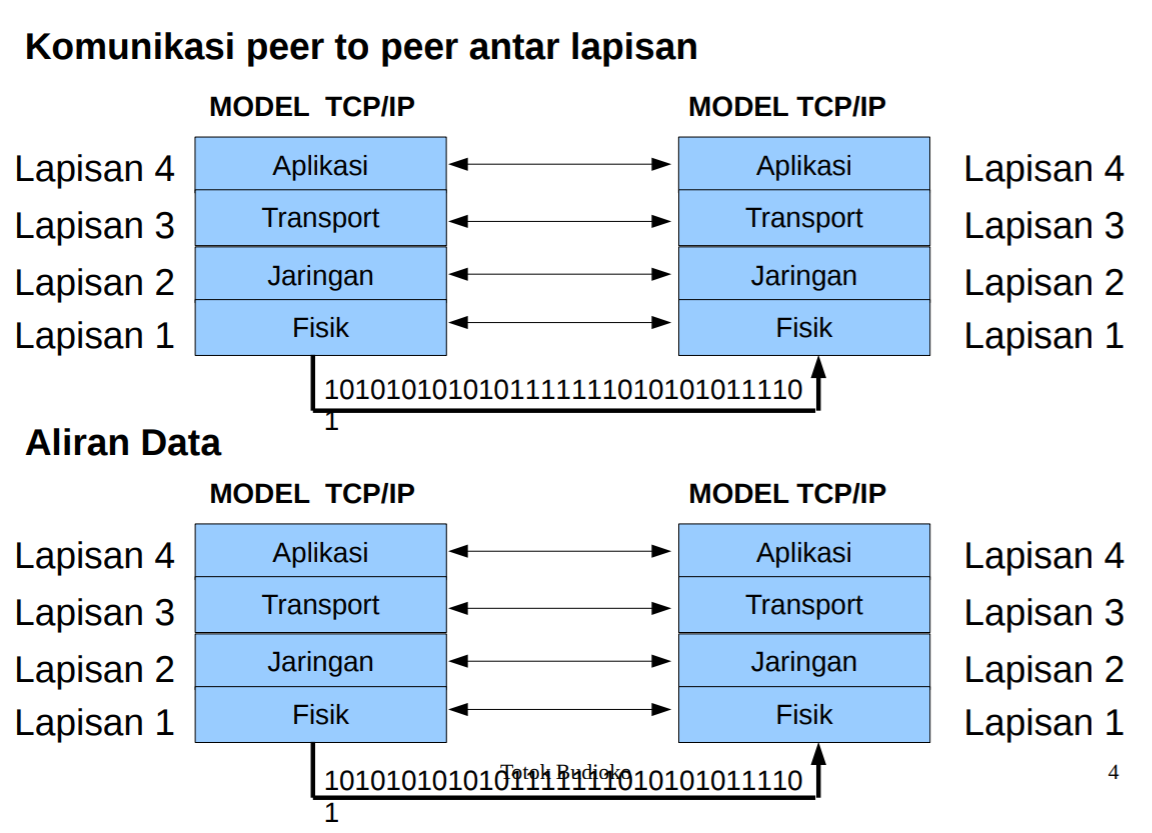
**Model Referensi TCP/IP**









**Satuan Data Protokol (Protocol Data Unit (PDU)) dan Pengkapsulan (Encapsulation)**

Bentuk data pada setiap lapisan disebut dengan satuan data protokol (Protocol Data Unit (PDU)). Nama PDU pada setiap lapisan berbeda-beda. 1. Data : Lapisan aplikasi 2. Segment: Lapisan Transport 3. Packet: Lapisan Internetwork 4. Frame: Lapisan Akses Jaringan

Model OSI

1. Lapisan Aplikasi Lapisan aplikasi merupakan lapisan paling atas baik di OSI maupun TCP/IP. Lapisan Aplikasi menyediakan antarmuka antara aplikasi yang digunakan untuk berkomunikasi dan lapisan dibawahnya untuk mengirimkan pesan. Lapisan aplikasi digunakan untuk mengirimkan data antara program yang berjalan baik di sumber maupun tujuan.

Pada Protokol TCP/IP lapisan Aplikasi mencakup tiga lapisan atas,yaitu Aplikasi, Presentasi dan Sesi. Totok Budioko 7 Model Referensi OSI dan TCP/IP Model OSI

1. Lapisan Presentasi Fungsi utama lapisan Presentasi:

- Pengkodean dan konversi

- Kompresi dan dekompresi

- Enkripsi dan dekripsi

1. Lapisan Sesi Fungsi lapisan Sesi :

* Membuat dan memelihara dialog antara aplikasi sumber dan tujuan.
* Melakukan inisiasi dialog, mengaktifkan dan merestart sesi jika terjadi gangguan atau idlle.
* Sebagian besar aplikasi menggabungkan 3 lapisan atas semisal Web Browser dan email client.

**Lapisan Aplikasi Model TCP/IP**

Beberapa protokol pada lapisan Aplikasi:

* Domain Name Service Protocol (DNS) Menerjemahkan nama host menjadi alamat IP.
* Hypertext -Transfer Protocol (HTTP) digunakan untuk mentransfer file Web dari World Wide Web.
* Simple Mail Transfer Protocol (SMTP) digunakan untuk mentransfer pesan email.
* Telnet, a terminal emulation protocol, digunakan untuk mengakses server atau peralatan jaringan jarak jauh
* File Transfer Protocol (FTP) Digunakan untuk transfer file secara interaktif antar sistem

**Mengapa Model Referensi dibuat berlayer**

1. Membantu dalam perancangan protokol
2. Membantu dalam pengembangan
3. Mencegah perubahan kemampuan atau teknologi akibat perubahan lapisan di bawah atau atasnya
4. Menyediakan satu bahasa untuk mendeskripsikan fungsi jaringan dan kemampuannya.

**Fungsi Layer Transport**

Sesuai dengan namanya, tansport layer merupakan lapisan OSI yang memilki tugas sebagai pengantar. Fungsi utama dari transport layer pada lapisan OSI ini adalah :

* Memecah data ke dalam paket – paket data
* Mentransmisikan data dari session layer menuju network layer, maupun sebaliknya.
* Membuat penomoran pada paket – paket data, sehingga nantinya dapat disusun kembali dengan mudah
* Melakukan proses transmisi ulang pada paket data yang hilang
* Berkat adanya transport layer ini, maka setiap data bisa saling berjalan dari server menuju clientnya dengan lancar tanpa adanya gangguan.

1. **Menerima data dari session layer**

Fungsi pertama dari transport layer ini adalah menerima data yang dikirimkan melalui session layer. Seperti kita ketahui, bahwa keseluruhan model OSI ini merupakan satu kesatuan, sehingga setiap kegiatan yang berjalan di dalam Model Referensi OSI ini adalah berkesinambungan. Begitu pula dengan proses transmisi data. Data yang sdah melewati layer session, kemudian diteruskan ke transport layer, untuk kemudian diteruskan lagi menuju layer-layer berikutnya. (baca juga: [session layer jaringan komputer](https://dosenit.com/jaringan-komputer/teknologi-jaringan/session-layer-jaringan-komputer))

1. **Memecah data menjadi bagian – bagian yang lebih kecil**

Disinilah fungsi utama lainnya dari transport layer. Ya, transport layer memiliki fungsi utama untuk memecah data atau peket data ke dalam bentuk-bentuk paket yang lebih kecil. Proses ini dilakukan untuk mempermudah proses pengiriman alias transmisi data yang berjalan di dalam jaringan komputer tersebut. Dengan adanya proses pemecahan data ini, maka setiap data diyakini tidak akan mengalami corrupt , atau mengalami proses trasnmisi yang sangat lamabt akibat besarnya ukuran data yang ada.

1. **Meneruskan data ke network layer**

Masih ingat mengenai network layer? Ya, [netwok layer jaringan komputer](https://dosenit.com/jaringan-komputer/teknologi-jaringan/network-layer-jaringan-komputer) merupakan salah satu lapisan yang bertugas untuk memberikan header pada paket data yang sudah dipecah. Nah, ketika paket data tersebut sudah dipecah-pecah di dalam transport layer, maka kemudian paket data tersebut akan diteruskan ke dalam network layer, untuk kemudian diproses dan diberikan header atau judul pada setiap paket data yang ditransmisikan.

1. **Memastikan bahwa semua data yang melewatinya dapat tiba di sisi lainnya dengan tepat**

Fungsi berikutnya dari transport layer adalah fungsi supervise atau pengawasan. Transport layer memiliki fungsi yang sangat penting, karena transport layer berfungsi untuk memastikan bahwa seluruh paket data yang ditransmisikan di dalam jaringan komputer tersebut dapat sampai pada komputer penerima dengan cepat, tepat, dan sesuai dengan tujuan. Hal ini untuk menghindari terjadinya kesalahan dalam proses transmisi data di dalam jaringan komputer.

1. **Mengirim segment dari satu host ke host yang lain**

Fungsi berikutnya dari transport layer adalah melakukan proses pengiriman segment dari satu host menuju host yang lain. segment sendiri merupakan bagian dari pecahan-pecahan data yang sudah diproses di dalam transport layer. Dengan begitu, setiap pecahan data tersebut nantinya akan diterima di host lain.

1. **Memastikan realibilitas data**

Reliabilitas merupakan sebuah kondisi dimana sebuah data adalah benar adanya, dan beisi sesuai dengan spesifikasinya. Tugas dar transport layer adalah memastikan hal tesebut. Jadi, transport layer nantinya akan mengecek, apakah data yang diolah dan juga diproses di dalam transport layer sudah sesuai dan sudah reliabel.

Apabila hal ini sudah selesai, maka transport layer kemudian akan mengirimkan pecahan atau pakt data tersebut menuju layer berikutnya untuk diproses lebih lanjut. Hal ini dilakukan untuk menjaga agar konektivitas di dalam jaringan ttap berjalan dengan baik.

1. **Mengatur lalu lintas dari sebuah jaringan**

Fungsi lainnya dari transport layer yang tidak kalah penting adalah fungsinya sebagai polisi lalu lintas. Ya, transport layer merupakan lapisan yang berfungsi untuk mengatur lalu lintas kecepatan data yang ditransmisikan melalui jaringan komputer tersebut. Hal ini dilakukan agar setiap perputaran dan traffic dapat berjalan dan ditransmisikan dengan lancar, dan juga diaplikasikan untuk mencegah terjadinya kemacetan apabila jaringan sedang berada pada kondisi yang sangat padat dan berpotensi mengalami kemacetan jaringan.

**Penjelasan Port Number, fungsi dan contoh proses kerjanya**

**Port jaringan adalah** proses khusus atau konstruk perangkat lunak khusus aplikasi yang berfungsi sebagai titik akhir komunikasi, yang digunakan oleh protokol Transport Layer (OSI Layer ke 4) dari paket Protokol Internet, seperti User Diagram Protocol (UDP) dan Transmission Control Protocol (TCP). **Nomor port** adalah bilangan bulat unsigned 16-bit yang **berkisar dari 0 hingga 65535**.

* **0 hingga 1023** – port yang dikenali atau port sistem.
* **1024 hingga 49151** – port terdaftar yang ditugaskan oleh IANA ke layanan yang lebih spesifik setelah adanya *request entity*pada sebuah aplikasi.
* **49152 hingga 65535** – port dinamis (pribadi) berkisar dari 49.152 hingga 65.535. Dapat digunakan oleh layanan pribadi atau layanan khusus, sehingga Anda bisa memodifikasi fungsi dari port-nya.

**1.Port 20 & 21 (FTP)**

FTP adalah singkatan dari “File Transfer Protocol”. Tujuan FTP adalah untuk mentransfer file melalui internet. Hal ini pada dasarnya menetapkan semua aturan yang harus diikuti selama transfer data. Namun, karena masalah keamanan, FTP juga meminta otentikasi kepada pengguna sebelum melakukan transfer data. **Port 20 berfungsi untuk** untuk meneruskan dan mentransfer data. Port ini mengambil alih tugas mentransfer data FTP saat berada dalam mode aktif. **Port 21 berfungsi untuk** pensinyalan untuk FTP. Hal ini menjalankan semua perintah dan memiliki kontrol aliran untuk data, yang berarti port 21 ini lebih leluasa dalam mentransfer data karena memiliki kontrol penuh dibandingkan port 20.

**2.Port 22 (SSH)**

SSH juga disebut sebagai “Secure Shell”.  **Port ini berfungsi untuk** melakukan tugas yang bisa diakses dari jarak jauh, contohnya seperti menghubungkan ke server atau host. Hal ini juga memungkinkan Anda untuk menjalankan sejumlah perintah dan memindahkan file Anda dari jarak jauh juga.

Port ini mengirimkan data melalui jaringan dalam bentuk terenkripsi, selain itu, hanya orang yang memiliki akses yang dapat login dari jarak jauh ke sistem yang dituju menggunakan Port 22 untuk memastikan bahwa tidak ada informasi yang masuk ke tangan yang tidak sah.

Port ini beroperasi pada Application Layer (OSI Layer ke 7) Model TCP / IP dan **dianggap sebagai salah satu port paling aman** dan dapat diandalkan untuk mengakses file dari jarak jauh.

**3. Port 23 (TELNET)**

**Port 23 (TELNET) berfungsi** **untuk**membuat koneksi antara server dan komputer jarak jauh. Fungsi sebenarnya **masih sama saja seperti SSH, hanya** **yang membedakan adalah dalam hal keamanan**. Hal ini disebabkan karena port 23 tidak menggunakan enkripsi dalam koneksinya, sehingga menyebabkan telnet menjadi salah satu layanan yang kurang aman untuk digunakan.

**4. Port 25 (SMTP)**

SMTP merupakan singkatan dari Simple Mail Transfer Protocol. **Fungsi port 25 adalah** untuk memastikan bahwa pesan email dikomunikasikan melalui jaringan dengan aman. Port ini masih berada pada Application Layer (OSI Layer ke 7). Protokol ini tidak hanya melakukan tugas pengiriman pesan dalam jaringan saja, nmaun dapat mengirimkan pesan di antara berbagai jaringan yang lain. Hal Ini menjadikannya sebagai salah satu port terpenting untuk komunikasi pesan melalui jaringan karena keamanannya. Namun, Anda tidak memiliki hak  untuk mengunduh email agar bisa membacanya, karena ini hanyalah bertujuan untuk mentransfernya melalui jaringan.

**5. Port 2525 (SMTP Alternative)**

Port 2525 **masih memiliki fungsi yang sama seperti port 25**, yaitu untuk mengirimkan pesan e-mail dalam jaringan secara aman. Adapun port ini digunakan sebagai port alternatif selain port 25.

**6. Port 53 (DNS)**

DNS disebut juga sebagai “Domain Name System”, **berfungsi untuk** menerjemahkan alamat IP pada setiap host yang tadinya berupa angka menjadi huruf. Jika Anda mengunjungi sebuah situs web dengan sebuah nama, misalnya **KacaTeknologi.com**sebenarnya dibalik nama tersebut memiliki alamat IP. Hanya saja jika kita menggunakan alamat IP, maka itu cukup merumitkan. Oleh karena itu, ilmuwan komputer memiliki ide untuk mengganti alamat IP menjadi huruf agar lebih mudah dikenali dan diingat.

**7. Port 67 & 68 (DHCP)**

DHCP juga dikenal sebagai “Dynamic Host Configuration Protocol”, port ini berjalan pada protokol UDP. **Port 67 dan 68 berfungsi untuk** menetapkan informasi terkait Alamat IP ke klien di jaringan secara otomatis. Informasi ini dapat terdiri dari subnet mask, Alamat IP dll.

Port UDP 67 melakukan tugas menerima permintaan alamat dari DHCP dan mengirim data ke server. Di sisi lain, UDP Port 68 melakukan tugas menanggapi semua permintaan DHCP dan meneruskan data ke klien.

**8. Port 80 (HTTP / Webserver)**

HTTP adalah singkatan dari Hypertext Transfer Protocol. **Fungsi port 80 adalah**memungkinkan peramban / browser terhubung ke halaman web di internet. Port 80 pada dasarnya menunggu klien web untuk meminta koneksi. Setelah koneksi berhasil dibuat, Anda akan terhubung ke World Wide Web (WWW) dan mendapatkan akses ke berbagai halaman web di internet.

Adapun port alternatif dari http / webserver adalah port 8080 dan 81.

**9. Port 443 (HTTPS)**

**Port HTTPS 443 berfungsi untuk** menghubungkan Anda ke internet dengan membuat koneksi antara halaman web dan browser yang terhubung ke World Wide Web (WWW). Namun, port ini memiliki fitur keamanan tambahan, yang tidak dimiliki port HTTP 80.

Port ini dibuat untuk membuat koneksi yang lebih terjaga untuk memastikan bahwa data ditransmisikan melalui jaringan yang aman. Port Ini pada dasarnya mengenkripsi dan mengotentikasi paket jaringan sebelum mentransfernya melalui jaringan untuk meningkatkan keamanan. Fitur keamanan ini diperkenalkan oleh penggunaan SSL, yang juga bisa disebut sebagai Secure Socket Layer.

**10. Port 110 (POP-3)**

POP3 juga disebut sebagai Post Office Protocol Version 3 yang beroperasi pada port 110 dari Protokol TCP. **Port 110 ini memungkinkan** pesan email untuk diambil dari server SMTP. Menggunakan port ini, Anda dapat mengunduh pesan dari server dan kemudian membacanya. Selain itu, pesan juga akan dihapus dari server setelah diunduh. Namun, port ini memiliki masalah keamanan. Otentikasi yang ditransfer melalui jaringan tidak dienkripsi dan dikirim dalam teks biasa. Hal Ini memungkinkan para *hacker* dapat dengan mudah mendapatkan informasi di dalamnya dan menyalahgunakan informasi tersebut.

**11. Port 119 (NNTP Server)**

NNTP Server atau dikenal dengan Network News Tranfer Protocol menggunakan port 119. **Port ini berfungsi untuk** menampung server-server dari dunia USENET newsgroup (berita).

**12. Port 143 (IMAP)**

IMAP adalah singkatan dari  “Internet Message Access Protocol”. **Port IMAP -143 berfungsi untuk** mengambil email dari server jauh tanpa harus mengunduh email. Berarti Anda memiliki kebebasan untuk mengakses email dari mana saja dengan asalkan terhubung dengan server. Namun, Anda juga dapat mengunduh e-mail jika mau. Hal Ini juga memberi Anda kemudahan untuk mencari pesan-pesan Anda dari banyaknya pesan yang ada. Selain itu, port ini juga memastikan bahwa data tetap aman selama koneksi berlangsung.

**13. Port 389 (LDAP)**

LDAP merupakan singkatan dari “Lightweight Directory Access Protocol” menggunakan port 389. Port 389 berfungsi untuk menangani permintaan otentikasi dari komputer klien yang bertujuan untuk memberikan akses terhadap direktori, telepon, alamat dll.

**14. Port 3389 (RDP)**

TCP Port 3389 digunakan untuk Windows Remote Desktop Protocol (RDP) dan kadang-kadang juga digunakan oleh Windows Terminal Server. Port ini seringkali digunakan para *hacker*untuk melakukan serangan Distributed Denial of Service Attack atau lebih dikenal dengan sebutan DDOS.

**15. Port 445 (SMB)**

Port 445 digunakan untuk Server Message Block (SMB). SMB melayani berbagi File dan Printer Windows (*file sharing*). Pada Windows 2000, Microsoft telah menciptakan transportasi baru untuk SMB melalui TCP dan UDP pada port 445, yang menggantikan implementasi yang lebih lama yaitu di atas port 137, 138, 139.

**16. Port 1503 & 1720**

Port 1503 dan 1720 digunakan oleh aplikasi kolaboratif multimedia seperti NetMeeting untuk membangun dan mengontrol sesi kolaboratif. Selain itu, contohnya adalah VOIP (Voice Over Internet Protocol) yang berfungsi untuk melakukan panggilan melalui internet seperti Voice Call di WhatsApp.

**17. Port 3306 (MySQL)**

Port 3306 adalah port default untuk Protokol MySQL, yang digunakan oleh klien mysql, MySQL Connector, dan *utility* seperti mysqldump dan mysqlpump. Port 33060 adalah port default untuk Database Extended Interface (Protokol MySQL X).

**18. Port 5631**

Port 5631 adalah port *default*pada jaringan komputer yang berfungsi untuk mengkoneksikan jaringan komputer dengan pcAnywhere. pcAnywhere adalah aplikasi yang dibuat oleh perusahaan jaringan yang bernama Symantec untuk menyediakan fungsionalitas kendali jarak jauh. Tidak berbeda jauh dengan SSH dan telnet hanya saja pcAnywhere ini berbentuk grafis / GUI.

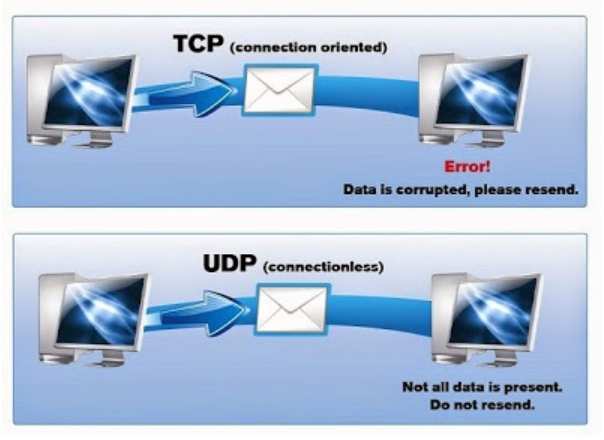
**19. Port 5900 (VNC)**

VNC adalah singkatan dari “Virtual Network Computing” menggunakan port 5900 dalam layanannya. Port ini berfungsi untuk menjalankan aplikasi *sharing* desktop dan platform remote control yang independen. VNC sangat populer dan juga digunakan untuk dukungan jarak jauh di banyak organisasi besar. Cara kerjanya tidak berbeda jauh dengan pcAnywhere.

**20. Port 8080 & 3128 (Proxy)**

Selain HTTP, Proxy juga menggunakan port yang sama dengan HTTP karena masih berjalan pada layanan yang sama hanya saja memiliki fungsi berbeda. Selain port 8080, ada juga port alternatif untuk proxy yaitu port 3128.

**Penjelasan tentang UDP dan prinsip kerjanya**

****

**Prinsip kerja Checksum Checking dan contohnya**