Modul 10 TCP/IP Lanjutan

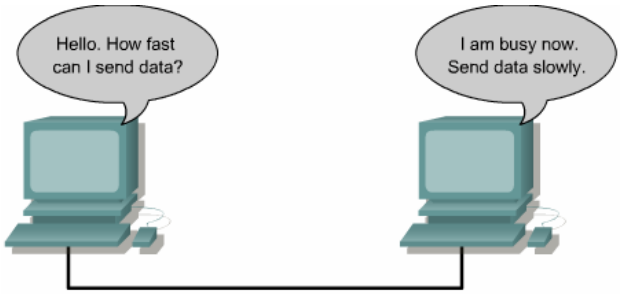
Pendahuluan
Router menggunakan informasi IP address dalam paket header IP untuk menentukan interface mana yang akan di-switch ke tujuan. Tiap-tiap layer OSI memiliki fungsi sendiri-sendiri dan tergantung dari layer lainnya. Setiap layer menerima layanan dari layer di atas dan di bawahnya. Layer application, presentation dan session pada model OSI sama dengan layer application pada model TCP/IP, sedangkan akses ke layanan layer transport melalui port. Modul ini akan menjelaskan konsep dari port dan nomor port di jaringan.

Setelah mengikuti modul ini Anda diharapkan mampu:

- Menggambarkan TCP dan fungsinya
- Menggambarkan sinkronisasi TCP dan flow control
- Menggambarkan operasi UDP
- Mengidentifikasi nomor port yang umum digunakan
- Menggambarkan komunikasi antar host
- Mengidentifikasi port yang digunakan untuk layanan dan klien
- Menggambarkan penomoran port
- Mengerti perbedaan dan hubungan antara MAC address, IP address dan port number

1. Operasi TCP
1.1 Layer 4 – Transport layer
IP address mengijinkan routing paket antar jaringan. IP menjamin pengiriman paket data. Layer transport bertanggung jawab untuk menjamin transmisi dan aliran data dari asal ke tujuan. Hal ini nanti akan berhubungan dengan sliding window dan sequencing number untuk sinkronisasi aliran data.

Untuk memahami reliability dan flow control, analoginya sama dengan mahasiswa yang belajar bahasa asing selama satu tahun. Bayangkan kalau mahasiswa ini pergi ke Negara dimana dia belajar bahasa tersebut. Mahasiswa harus bertanya ke orang-orang untuk mengulang kata-kata dan berbicara secara benar (reliability) dan pelan-pelan (sama dengan konsep flow control).



Gambar 1.1 Layer4: transport layer

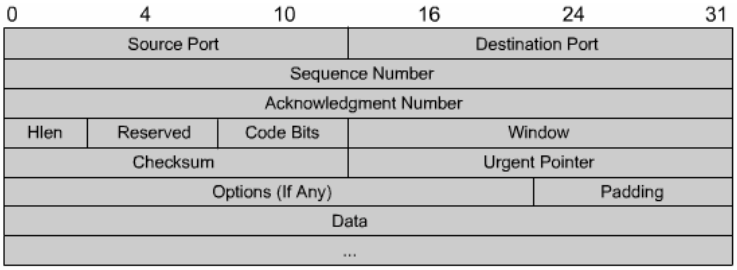
1.2 Sinkronisasi dan 3-way handshake
TCP adalah protokol connection-oriented. Komunikasi data antar host terjadi melalui proses sinkronisasi untuk membentuk virtual connection setiap

session antar host. Proses sinkronisasi ini meyakinkan kedu sisi apakah sudah siap transmisi data apa belum dan mengijinkan device untuk menentukan inisial sequence number. Proses ini disebut dengan 3-way handshake. Untuk membentuk koneksi TCP, klien harus menggunakan nomor port tertentu dari layanan yang ada di server.

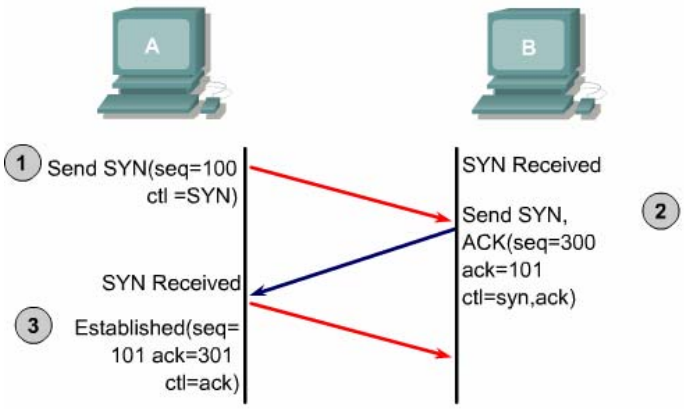
Tahap satu, klien mengirimkan paket sinkronisasi (SYN flag set) untuk inisialisasi koneksi. Paket dianggap valid kalau niali sequence numbernya misalnya x. bit SYN menunjukkan permintaan koneksi. Bit SYN panjangnya satu bit dari segmen header TCP. Dan sequence number panjangnya 32 bit.

Tahap dua, host yang lain menerima paket dan mencatat sequence number x dari klien dan membalas dengan acknowledgement (ACK flag set). Bit control ACK menunjukkan bahwa acknowledgement number berisi nilai acknowledgement yang valid. ACK flag panjangnya satu bit dan Ack number 32 bit dalam segmen TCP header. Sekali koneksi terbentuk, ACK flag diset untuk semua segmen. ACK number nilainya menjadi x + 1 artinya host telah menerima semua byte termasuk x dan menambahkan penerimaan berikutnya x + 1.

Tahap tiga, klien meresponnya dengan Ack Number y + 1 yang berarti ia menerima ack sebelumnya dan mengakhiri proses koneksi untuk session ini.



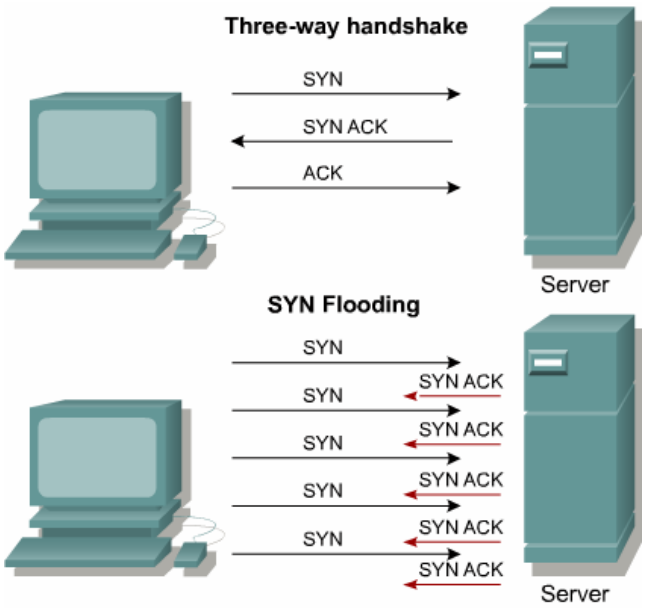
Gambar 1.2 Format segmen TCP



Gambar 1.3 Format segmen TCP

1.3 Serangan Denial of Service (DoS)

Serangan DoS didisain untuk mencegah layanan ke host yang mencoba untuk membentuk koneksi. DoS umutmnya digunakan oleh hacker untuk mematikan sistem. DoS dikenal dengan nama SYN flooding artinya membanjiri dan merusak 3-way handshake.

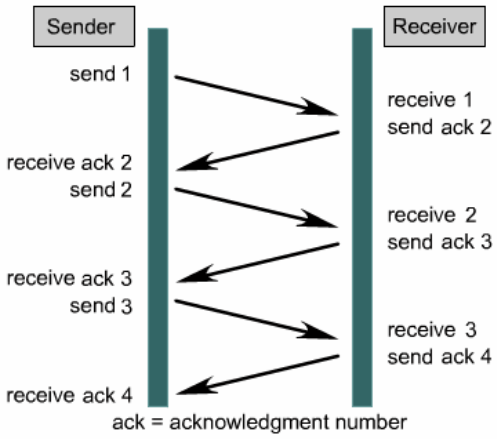


Gambar 1.4 Serangan DoS

Pada DoS, hacker meginisialisasi SYN tapi disisipi dengan alamat IP tujuan, artinya hacker memberikan permintaan SYN dengan informasi yang salah, sehingga proses koneksi akan menunggu lama dan akhirnya gagal. Untuk mengatasi hal ini, admin harus mengurangi koneksi selama peride tertentu dan menaikkan jumlah antrian koneksi.

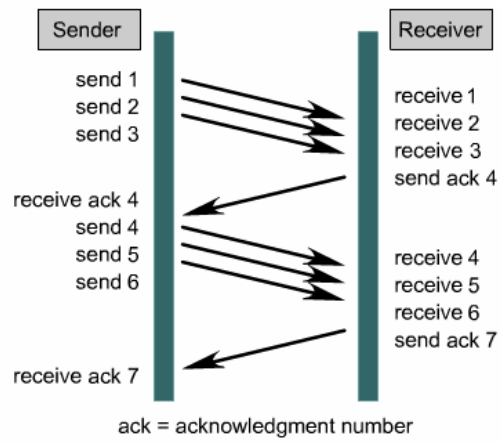
1.4 Windowing dan window size

Window size menetukan jumlah data yang dapat dikirim pada satu waktu sebelum tujuan meresponnya dengan acknowledgment. Setelah host mengirim angka window size dalam byte, hist harus menerima ack bahwa data telah doterima sebelum ia dapat mengirim data berikutnya. Sebagai contoh, jika window size 1, setiap byte harus ack sebelum byte berikutnya dikirim.



Gambar 1.5 TCP window size = 1

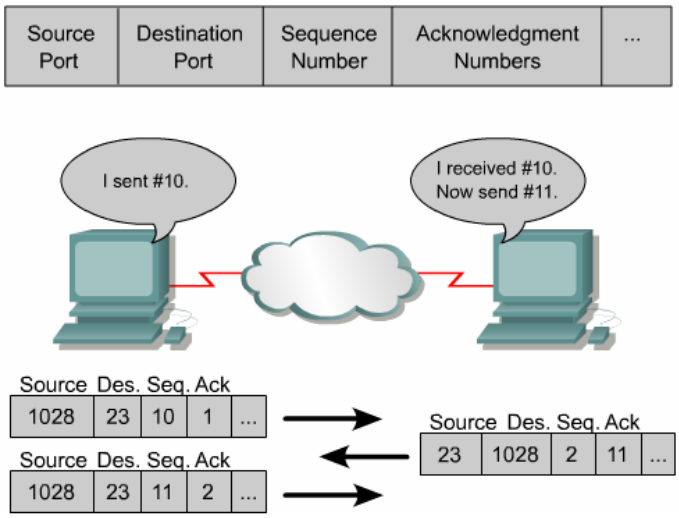
Windowing untuk menentukan ukuran transmisi secara dinamis. Device melakukan negosiasi window size untuk mengijinkan angka tertentu dalam byte yang harus dikirim sebelum ack.



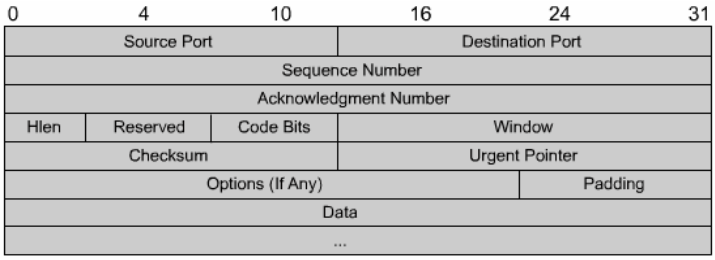
Gambar 1.6 TCP window size = 3

1.5 Sequence number dan ack number

Sequence number bertindak sebagai nomor referensi sehingga penerima akan mengetahui jika ia telah menerima semua data. Dan juga mengidentifikasi data-data yang hilang ke pengirim supaya ia mengirimnya lagi.



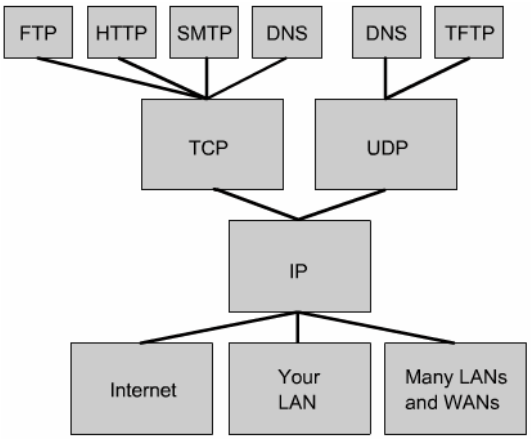
Gambar 1.7 TCP sequence number dan ack number



Gambar 1.8 Format segmen TCP

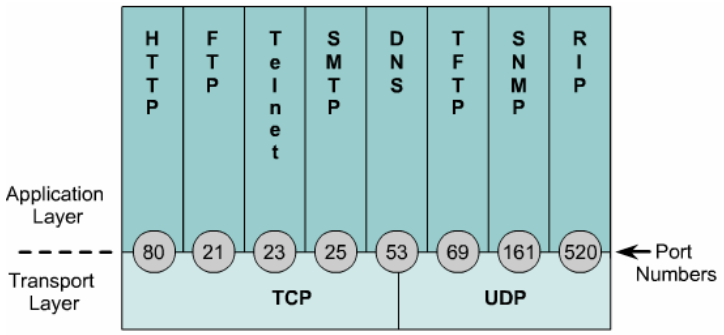
1.6 Operasi UDP

Baik TCP maupun UDP sama menggunakan IP protokol layer 3. TCP dan UDP diguanakan untuk aplikasi yang bermacam-macam. TCP melayani aplikasi seperti FTP, HTTP, SMTP dan DNS. Sedangkan UDP adalah protokol layer 4 yang digunakan oleh DNS, TFTP, SNMP dan DHCP.



Gambar 1.9 Protokol TCP/IP

Gambar 1.10 Format segmen UDP

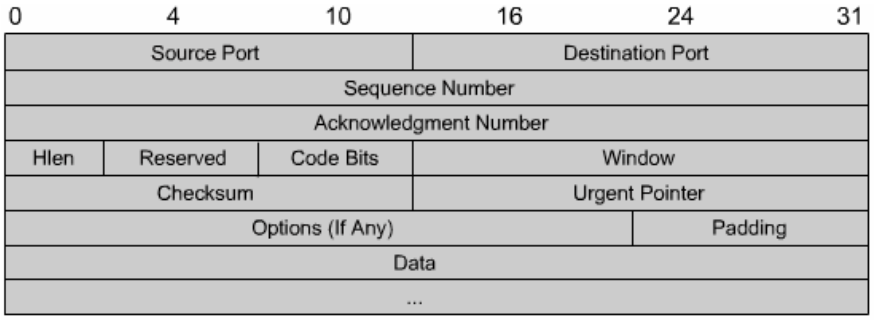


Gambar 1.11 Nomor port

2. Transport layer port

2.1 Port dan klien

Kapanpun klien terhubung ke layanan suatu server. Port asal dan tujuan pasti digunakan. Segmen TCP dan UDP berisi field port asal dan tujuan. Port tujuan, port layanan harus diketahui oleh klien. Secara umum nomor port secara acak dibangkitkan sendiri oleh klien dengan nomor di atas 1023. sebagai contoh, klien yang akan konek ke web server menggunakan TCP ke port tujuan 80 dan port asal 1045. Pada saat paket sampai di server, ia masuk ke layer transport dan masuk ke layanan HTTP yang beroperasi di port 80. server HTTP membalas ke klien dengan segmen yang menggunakan port 80 dan asal ke 1045 sebagai tujuannya.



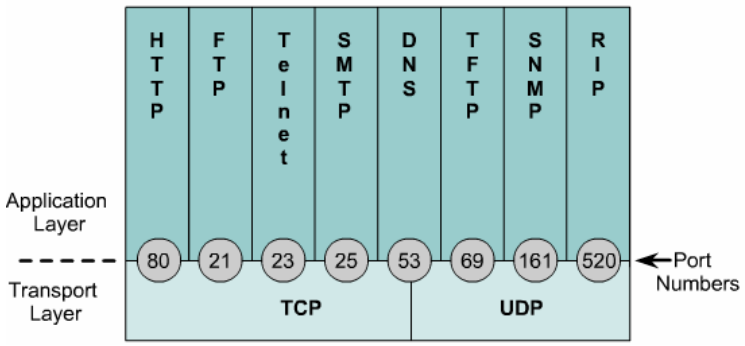
Gambar 2.1 Format segmen TCP

Gambar 2.2 Format segmen UDP

2.2 Nomor Port

Nomor port diwakili oleh 2 byte dalam header segmen TCP atau UDP. Nilai 16-bit dapat menghasilkan nomor port antara 0 sampai 65535. tiga kategori nomor port adalah well-known port, registered port dan dynamic atau private port. Nomor port 1023 ke bawah adalah well-known port, yang digunakan untuk layanan-layanan umu misalnya FTP, Telnet atau DNS.

Registered port rangenya dari 1024 – 49151. sedangkan port antara 49152 – 65535 untuk dynamic atau private port.



Gambar 2.3 Nomor port

2.3 MAC address, IP address dan port number

Sebagai analogi, pada saat kita membuat surat. Alamat pada surat berisi nama, jalan, kota dan provinsi. Data-data ini analoginya sama dengan port, MAC dan IP address untuk jaringan data. Nama di surat sama dengan nomor port, alamat surat sama dengan MAC address, dan kota serta provinsi sama dengan IP address. Banyak surat yang ditujukan ke alamat yang sama. Sebagai contoh ada dua surat yang dialamatkan ke alamat yang sama katakanlah “John Doe” dan lainnya “Jane Doe”. Hal ini analoginya sama dengan session banyak tapi nomor portnya lain.

Kesimpulan

- TCP adalah protokol connection-oriented. Dua host yang berkomunikasi terlebih dulu harus melakukan proses sinkronisasi untuk membentuk virtual koneksi.
- UDP adalah protokol connectionless, transmisi paket data tidak dijamin sampai ke tujuan
- Port number digunakan untuk melayani komunikasi yang berbeda dalam jaringan pada saat yang bersamaan. Port number diperlukan pada saat host komunikasi dengan server yang menjalankan bermacam-macam service.