

KEAMANAN INFORMASI PENDAHULUAN

Nur Rohman Rosyid

Dept. Teknik Elektro dan Informatika - Sekolah Vokasi UGM

SILABUS KEAMANAN INFORMASI

No.	Materi	Ket.
1.	Pendahuluan	
2.	Ancaman-ancaman Jaringan (<i>Network Threats</i>)	
3.	Pendahuluan Ethical Hacking	
4.	Footprinting & Reconnaissance	
5.	Scanning Networks	
6.	Enumeration	
7.	Vulnerability Analysis	
8.	System Hacking	
9.	Malware Threats	
10.	Sniffing	

SUMBER BACAAN

- Keamanan Jaringan
 - ✓ Network Security A Beginner's Guide, Eric Maiwald, Osborne/McGraw-Hill, 2001
 - ✓ Certified Ethical Hacker Version 8 Study Guide, Sean-Philip Oriyano, Sybex A Wiley Brand, 2014.
 - ✓ Network Security Assessment 2nd Edition, Chris McNab, O'Reilly, 2007
- CEHv8/CEHv9/CEHv10

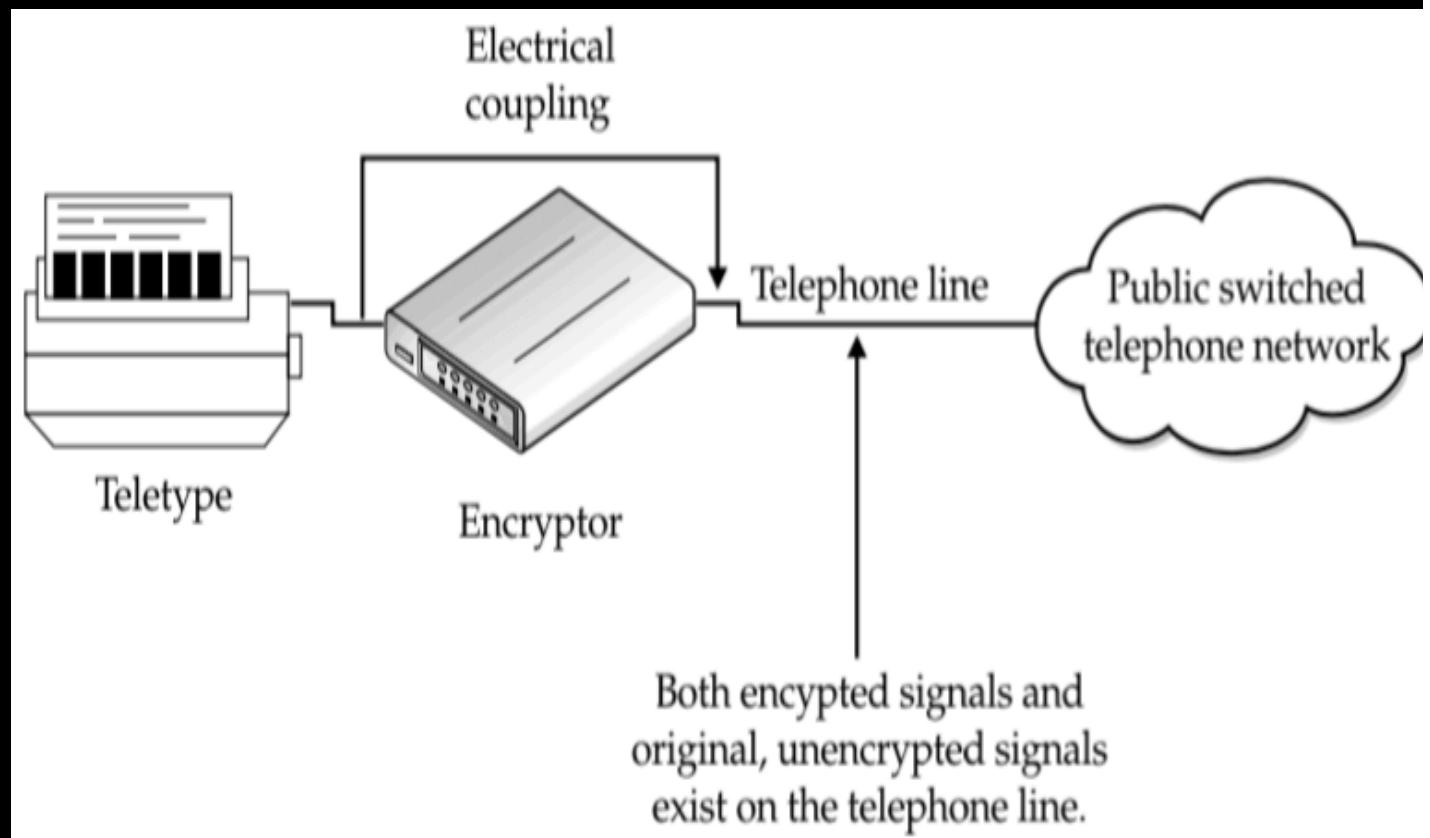
SEJARAH SINGKAT KEAMANAN

- Keamanan secara fisik (*physical security*)
 - ✓ Dahulu seluruh aset berbentuk fisik
 - pesan dipahat/ditulis pada batu atau daun
 - ✓ Dahulu aset dijaga secara fisik menggunakan tembak/benteng, parit, penjaga
- Keamanan komunikasi (*communications security*)
 - ✓ Pada saat pesan dapat dicuri/dilihat pada saat diperjalanan, maka pesan tersebut dapat dibaca oleh musuh/orang tidak berwenang
 - ✓ Solusinya adalah keamanan komunikasi
 - Dahulu Julius Caesar menciptakan Caesar Cipher
 - Saat PD-II Jerman menciptakan mesin Enigma (yang dapat dibaca juga oleh Alan Turing – Amerika)



SEJARAH SINGKAT KEAMANAN

- Keamanan pancaran (*emissions security*)
 - ✓ Encripor menerima pesan dan mengenkripsi dan meneruskan melalui jalur telephone
 - ✓ Ternyata ditemukan pula baik sinyal terenkripsi dan tidak terenkripsi ada di dalam jalur telephone





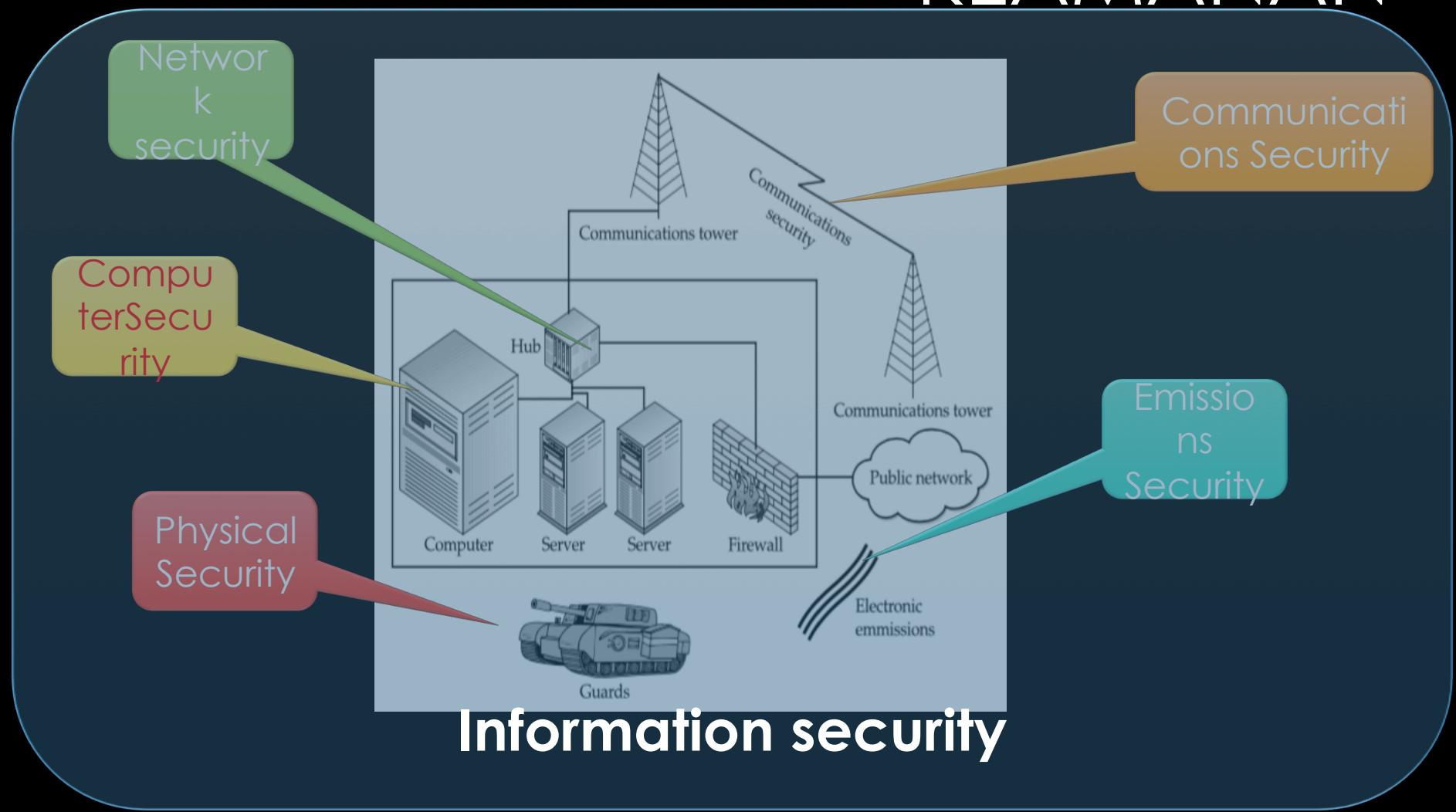
SEJARAH SINGKAT KEAMANAN

- Keamanan komputer (*computer security*)
 - ✓ Keamanan komunikasi dan pancaran mencukupi saat pesan dikirim melewati *teletype*
 - ✓ Kemudahan akses pada komputer mendorong pengembangan pengamanan pada komputer
 - ✓ Pada tahun 70-an model keamanan pengoperasian komputer diciptakan
 - Klasifikasi informasi (*unclassified, confidential, secret, dan top secret*)
 - Orang yang memiliki tingkat klasifikasinya lebih tinggi dari file (objek) maka dapat melakukan akses.

SEJARAH SINGKAT KEAMANAN

- Keamanan jaringan (*network security*)
 - ✓ Ketika komputer terhubung dengan jaringan, maka issue keamanan menjadi meningkat dan issue lama muncul kembali dengan cara yang berbeda
- Keamanan informasi (*information security*)
 - ✓ Keamanan yang bagus adalah gabungan dari semua solusi yang ada
 - ✓ Communication security (COMSEC) untuk melindungi informasi saat ditransmisikan.
 - ✓ Emissions security (EMSEC) dibutuhkan ketika musuh memiliki piranti yang mampu untuk membaca emisi elektronik dari sistem komputer.
 - ✓ Computer security (COMPUSEC) dibutuhkan untuk mengendalikan akses pada sistem komputer
 - ✓ Network security (NETSEC) diperlukan untuk mengendalikan keamanan pada LAN
 - ✓ Semua konsep tersebut menyediakan keamanan infromasi (INFOSEC)

SEJARAH SINGKAT KEAMANAN



PRODUK KEAMANAN TIDAK DAPAT MENGATASI SEGALANYA

- Anti-virus software
 - ✓ Dapat mengurangi dampak serangan malware pada organisasi
 - ✓ Tidak dapat melindungi organisasi dari penyusup (legal atau tidak legal) yang akan mengakses sistem
- Access Controls
 - ✓ Dapat mencegah pengguna legal untuk mengakses file yang bukan haknya.
 - ✓ Tidak dapat mencegah seseorang menggunakan kelemahan sistem untuk mengakses sebagai administrator
 - ✓ Dari sisi access control system seluruh serangan terlihat sebagai admin yang legal.

PRODUK KEAMANAN TIDAK DAPAT MENGATASI SEGALANYA

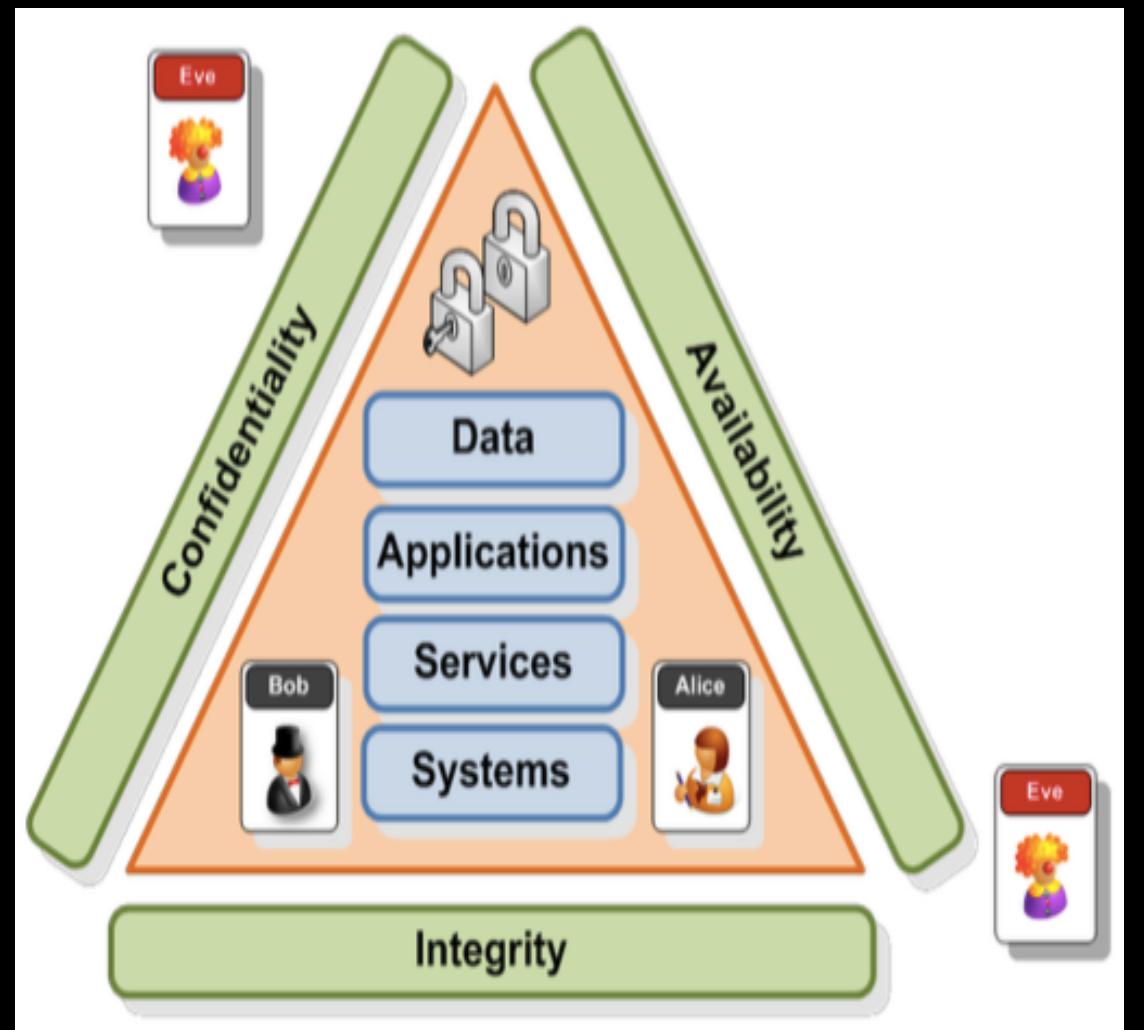
- Firewall
 - ✓ Piranti access control untuk jaringan dan membantu melindungi jaringan internal suatu organisasi dari serangan eksternal.
 - ✓ Firewall berada di batas antara jaringan internal dan eksternal, sehingga tidak dapat melindungi dari suatu serangan yang berasal dari internal
 - ✓ Firewall tidak dapat menangkal serangan dari luar yang melewati layanan umum (misal: web server, mail server, dns server, dll). Layanan tersebut diijinkan untuk diakses dari luar, namun jika layanan tersebut memiliki kelemahan dan dapat dilemahkan, maka firewall tidak dapat menangkalnya.
- Intrusion detection
 - ✓ Mencoba memberikan solusi untuk semua masalah keamanan, dengan mengidentifikasi seseorang melakukan kegiatan yang mencurigakan maka langsung dihentikan
 - ✓ Namun dapat juga mengalami kegagalan identifikasi baik positif maupun negatif

PRODUK KEAMANAN TIDAK DAPAT MENGATASI SEGALANYA

- Policy management
- Vulnerability scanning
 - ✓ Membantu mengidentifikasi potensi kelemahan sistem
 - ✓ Tidak dapat memproteksi sistem komputer, kelemahan harus segera diperbaiki
- Encryption
 - ✓ Mekanisme utama pada keamanan komunikasi
 - ✓ Encryption tidak membedakan pengguna legal maupun tidak legal, apabila mereka memiliki kunci enkripsi yang sama
- Physical security mechanism

PRINSIP UTAMA KEAMANAN

- Dapat memberikan keamanan yang maksimum, dengan minimum penurunan produktifitas, namun dengan biaya yang terjangkau ;)
- Prinsip utama → CIA
 - Confidentiality
 - Integrity
 - Availability



CONFIDENTIALITY

- Informasi hanya dapat diberikan kepada orang atau sistem yang memiliki kewenangan, sedangkan akses yang tidak sah harus dicegah
- Contoh ancaman confidentiality dari jaringan termasuk:
 - ✓ Eavesdropping on communications (menguping percakapan)
 - ✓ Pengaksesan tidak sah pada files yang sistem kendali akses nya tidak terkonfigurasi dengan benar
 - ✓ Kartu kredit yang dicuri dari server e-commerce melalui serangan cross-site scripting

INTEGRITY

- Informasi hanya dapat diubah oleh orang atau sistem yang berwenang
- Integrity memperhatikan akurasi informasi dan meproteksi dari perubahan yang tidak sah atau kecelakaan/ketaksengajaan.
- Contoh ancaman-ancaman dari jaringan meliputi:
 - Penyebaran malware antar mesin dan file-file rusak pada sistem
 - Penyergapan dan perubahan data saat ditransmisikan melintasi jaringan
 - Atau web site yang dirusak (defaced)

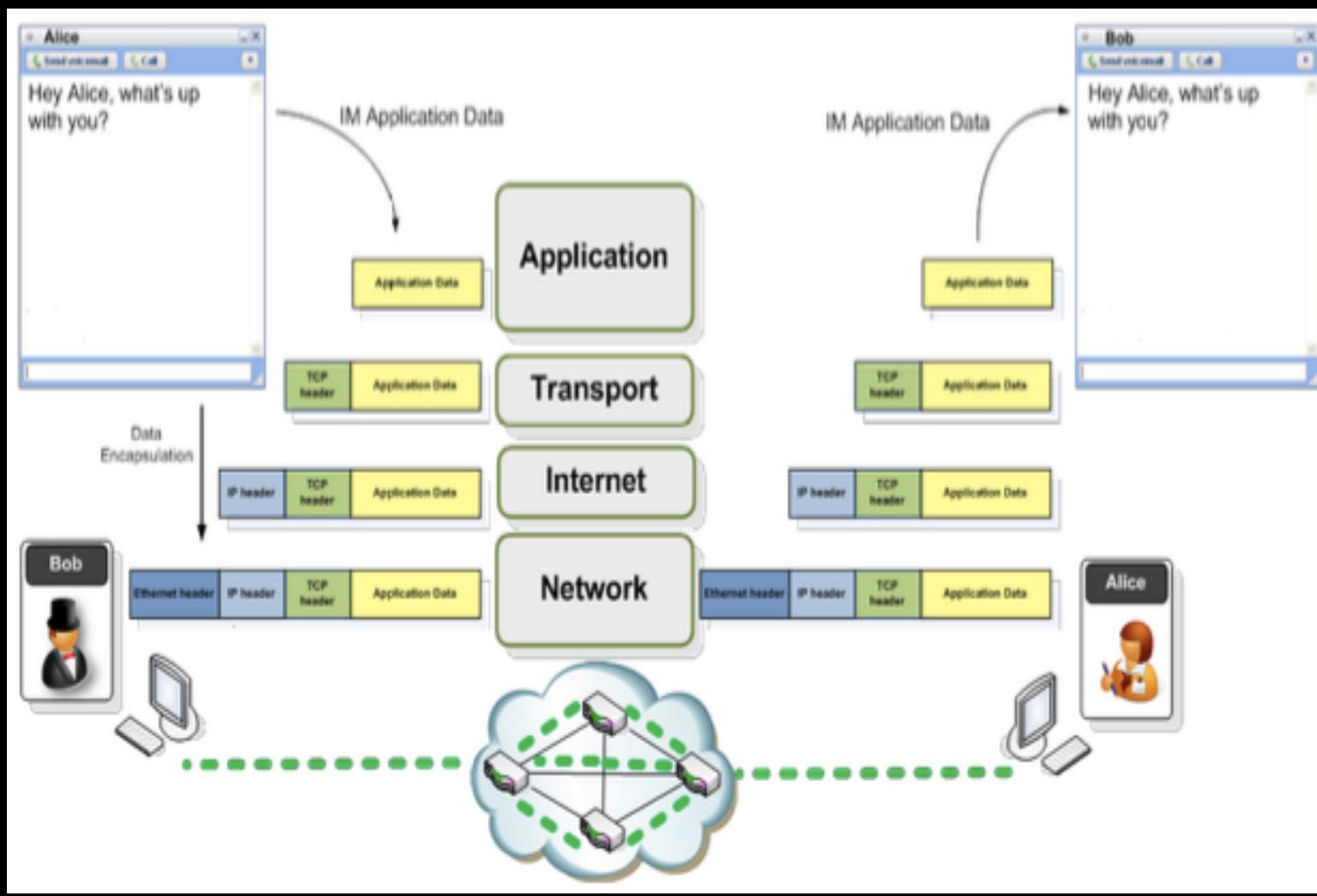
AVAILABILITY

- Kebutuhan akan informasi dan sistem untuk selalu dapat diakses oleh orang yang berwenang
- Contoh penyebab kegagalan ketersediaan meliputi:
 - Listrik mati
 - Web server tidak berfungsi karena network traffic yang berlebih
 - Adanya serangan DDoS

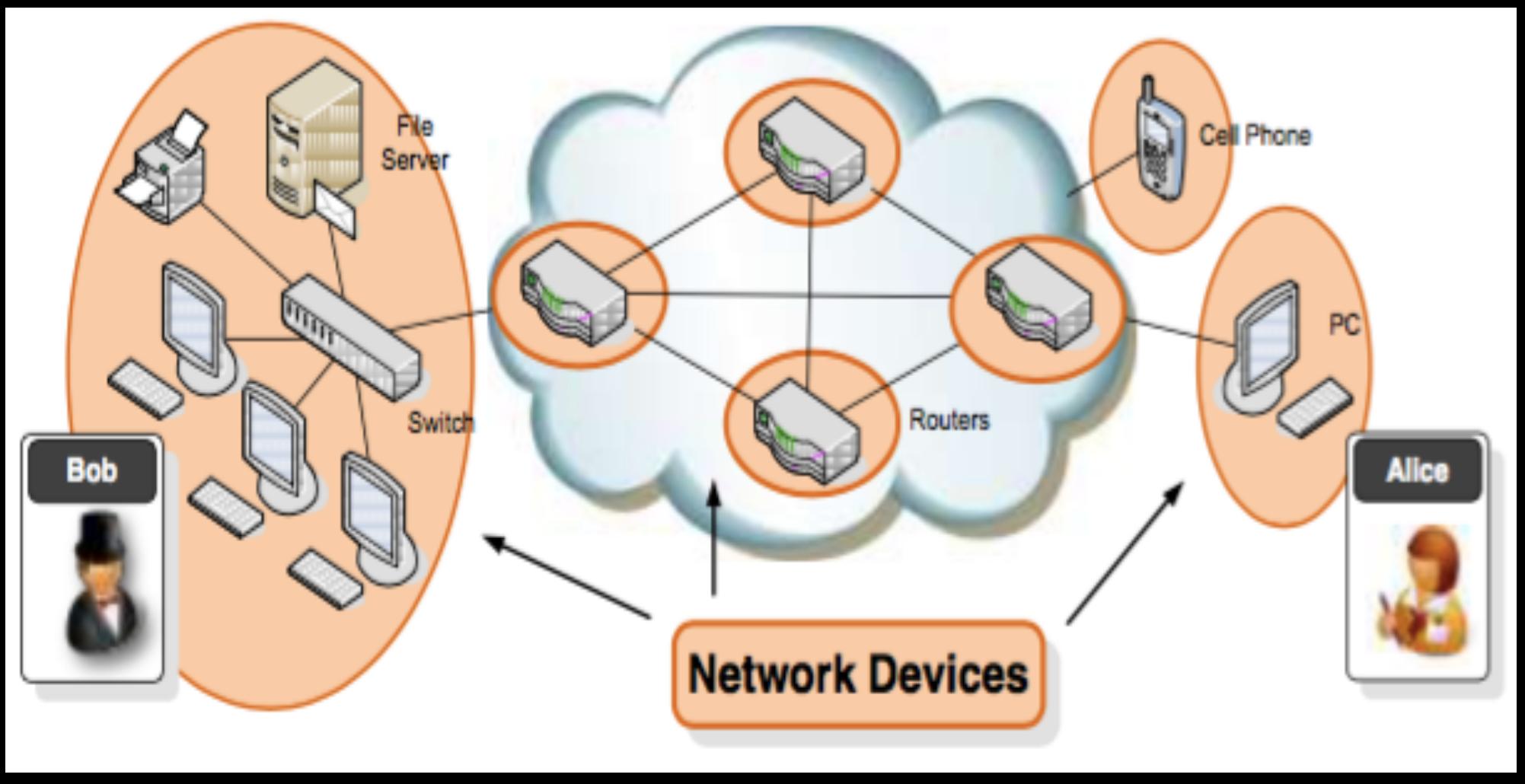
AUTHENTICATION

- Untuk membantu memproteksi suatu yang lebih kompleks
- Prinsip untuk mengetahui kepercayaan terhadap siapa dan apa.
- Konsepnya adalah konfirmasi identitas pengguna atau sistem
- Metode yang ditekankan adalah dengan memberikan
 - Username dan password
 - Biometrics
 - Autentikasi kriptografi seperti Digital Certificates

JARINGAN



PIRANTI JARINGAN



PIRANTI JARINGAN - CISCO

2811 Router



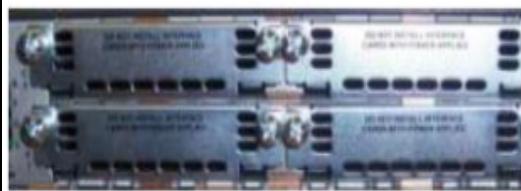
7206 Router – GNS3



PIX 515E Firewall



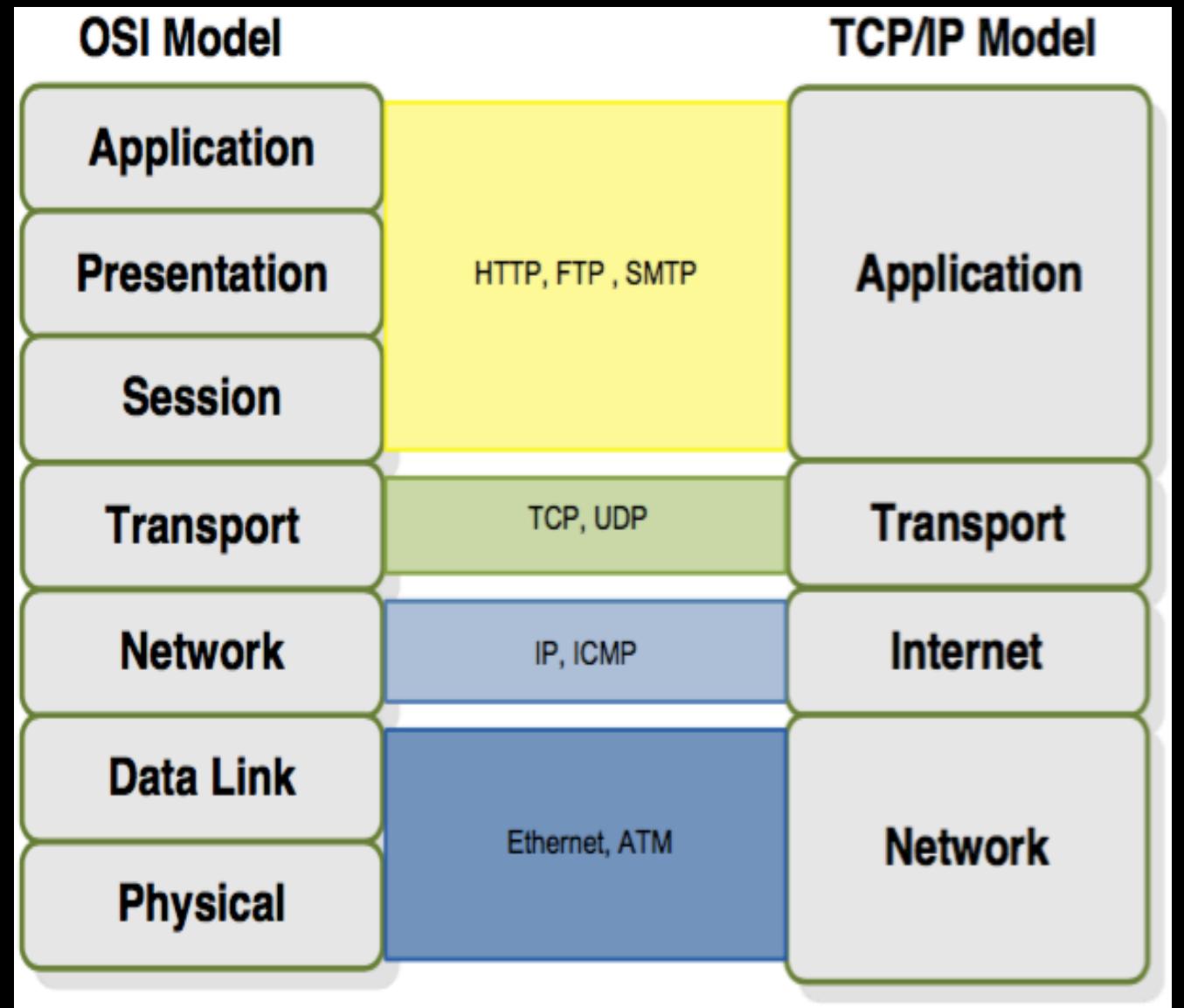
ASA 5510 Firewall



PIRANTI JARINGAN - MIKROTIK



PROTOKOL- PROTOKOL JARINGAN



PROTOKO PROTOKO JARINGAN



Application layer protocols. Typical: Web browser, Telnet, and FTP.

Defines the format of the data to be presented. Typical: ASCII, EBCDIC and ANSI.

Creating, controlling and shutting down TCP sessions. Typical: RPC and SQLNet (used in Oracle).

Flow control and end-to-end error control. Typical: TCP and UDP.

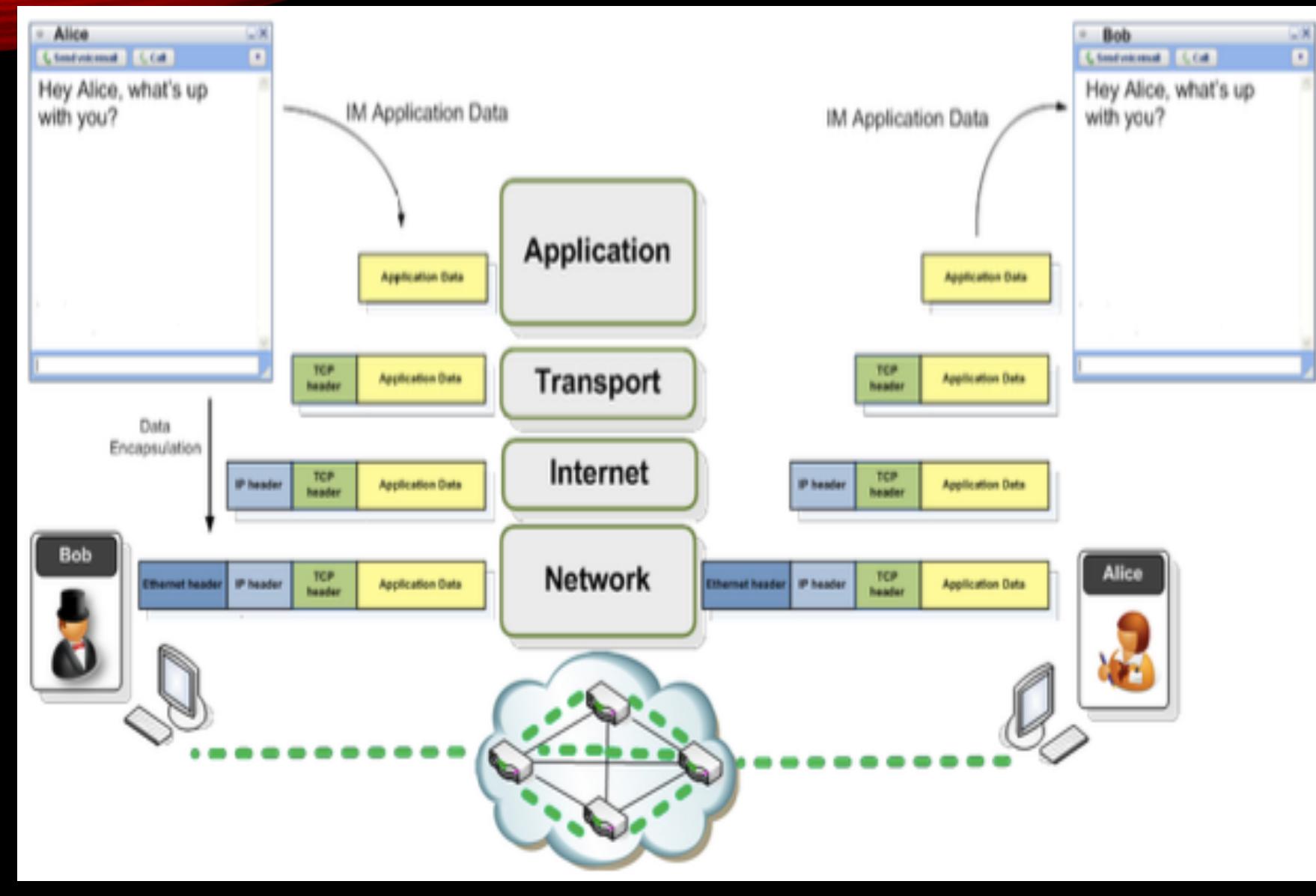
Logical and network address. Typical: IP and IPX.

Formatting and framing the data with a frame. Normally has a header and footer. Common ... Ethernet, with source and destination MAC addresses.

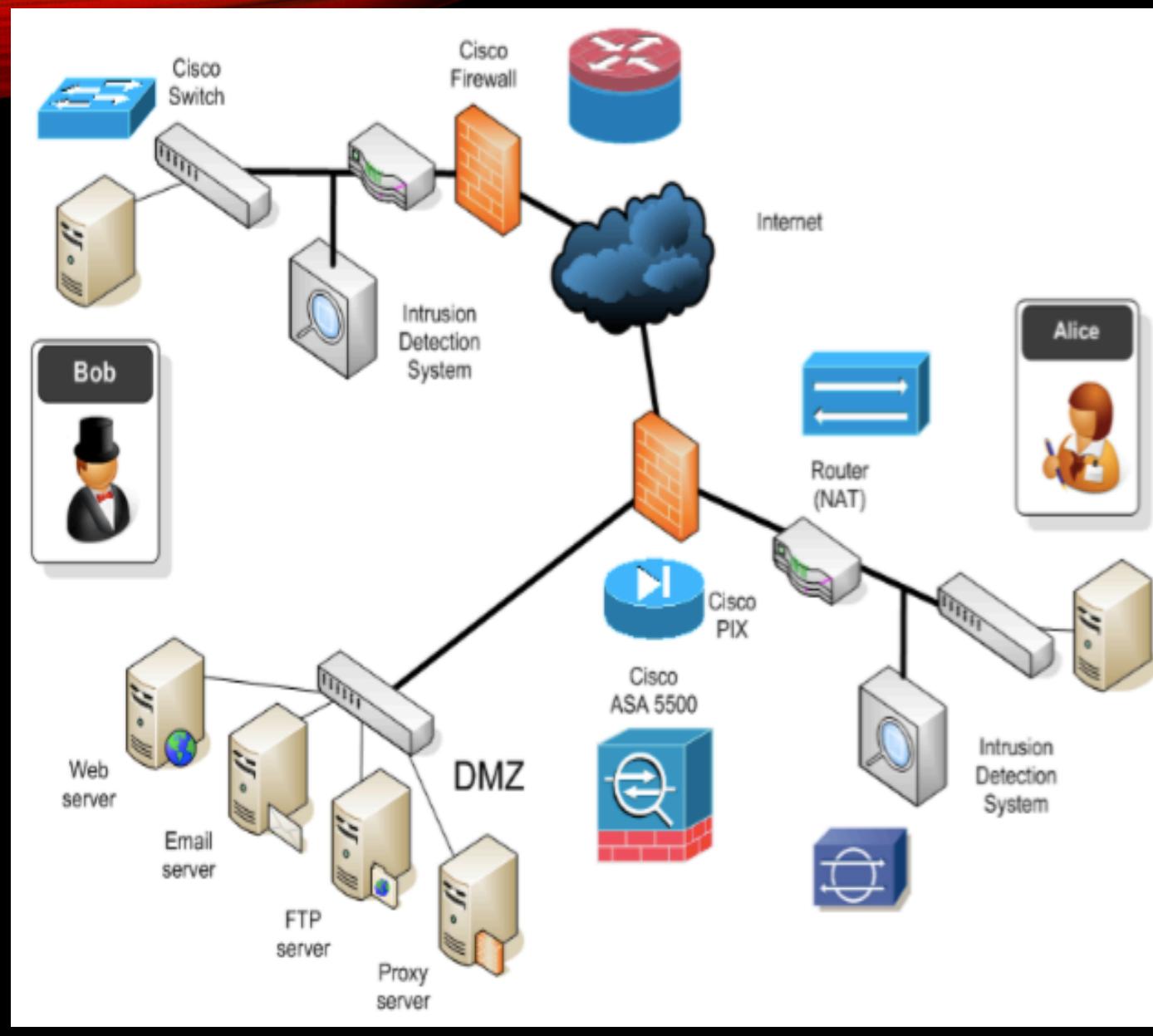
Bit-level communications ... Copper, fiber, radio.



ENKAPSULASI

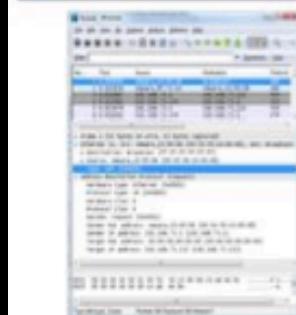
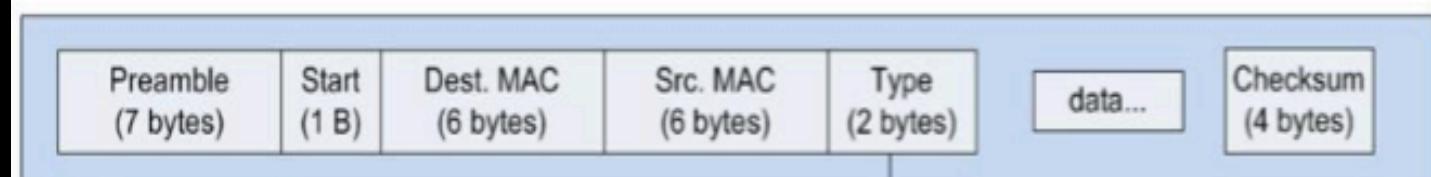
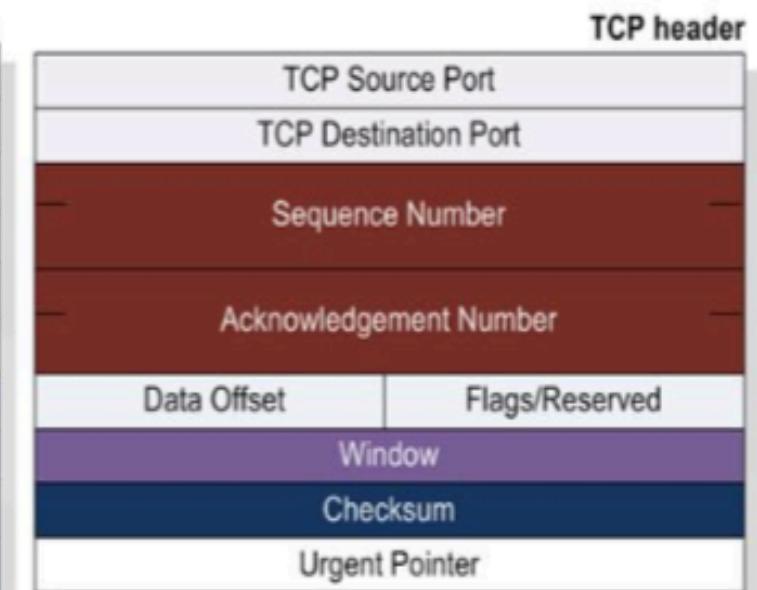
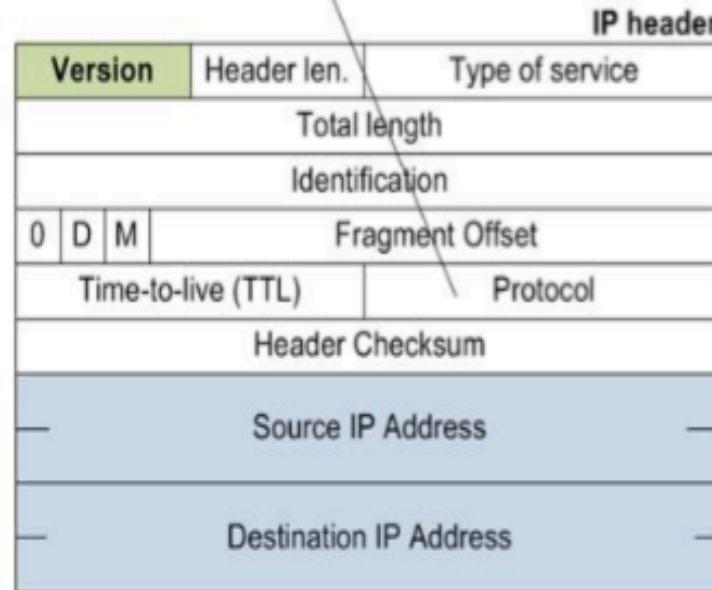


CONTOH INFRASTRUKTUR



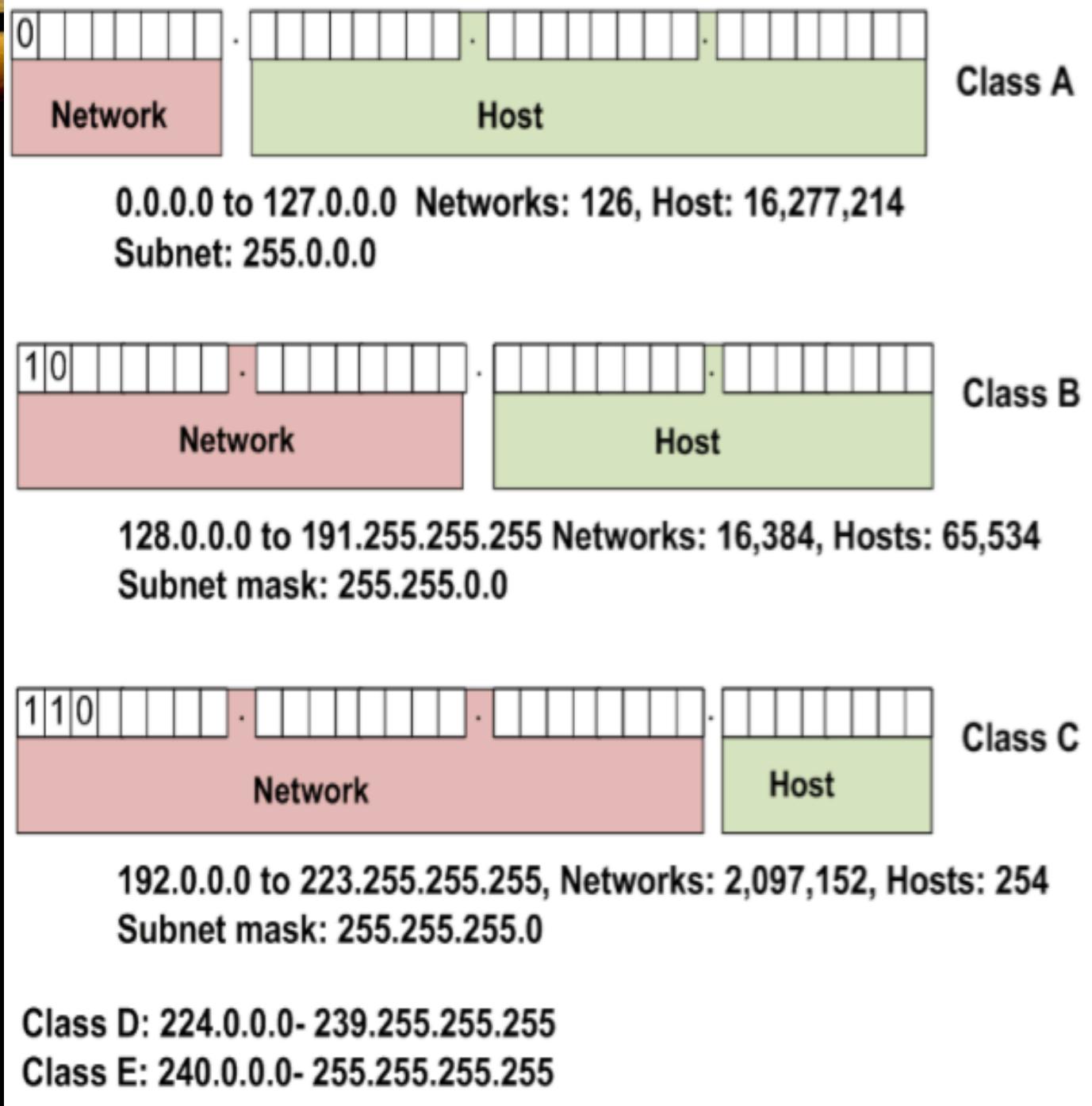
ETHERNET, IP, DAN TCP

Protocol:
 1 – ICMP
 6 – TCP
 8 – EGP
 17 - UDP

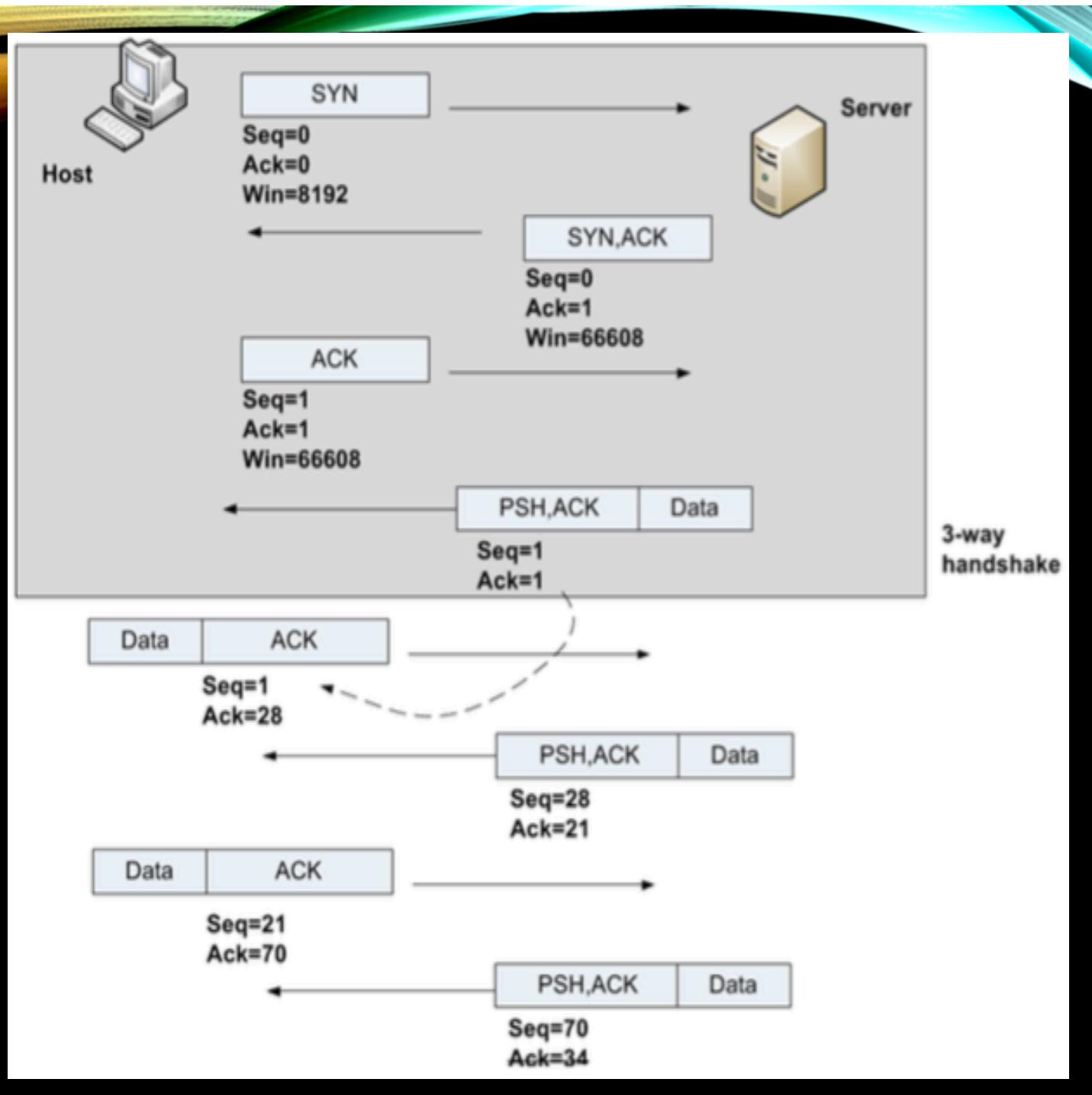


Ethernet frame
Type:
 0x800 – IP
 0x806 – ARP

ALAMAT NETWORK IP



TCP CLIENT/ SERVER



DNS OPERATION

DNS (UDP)

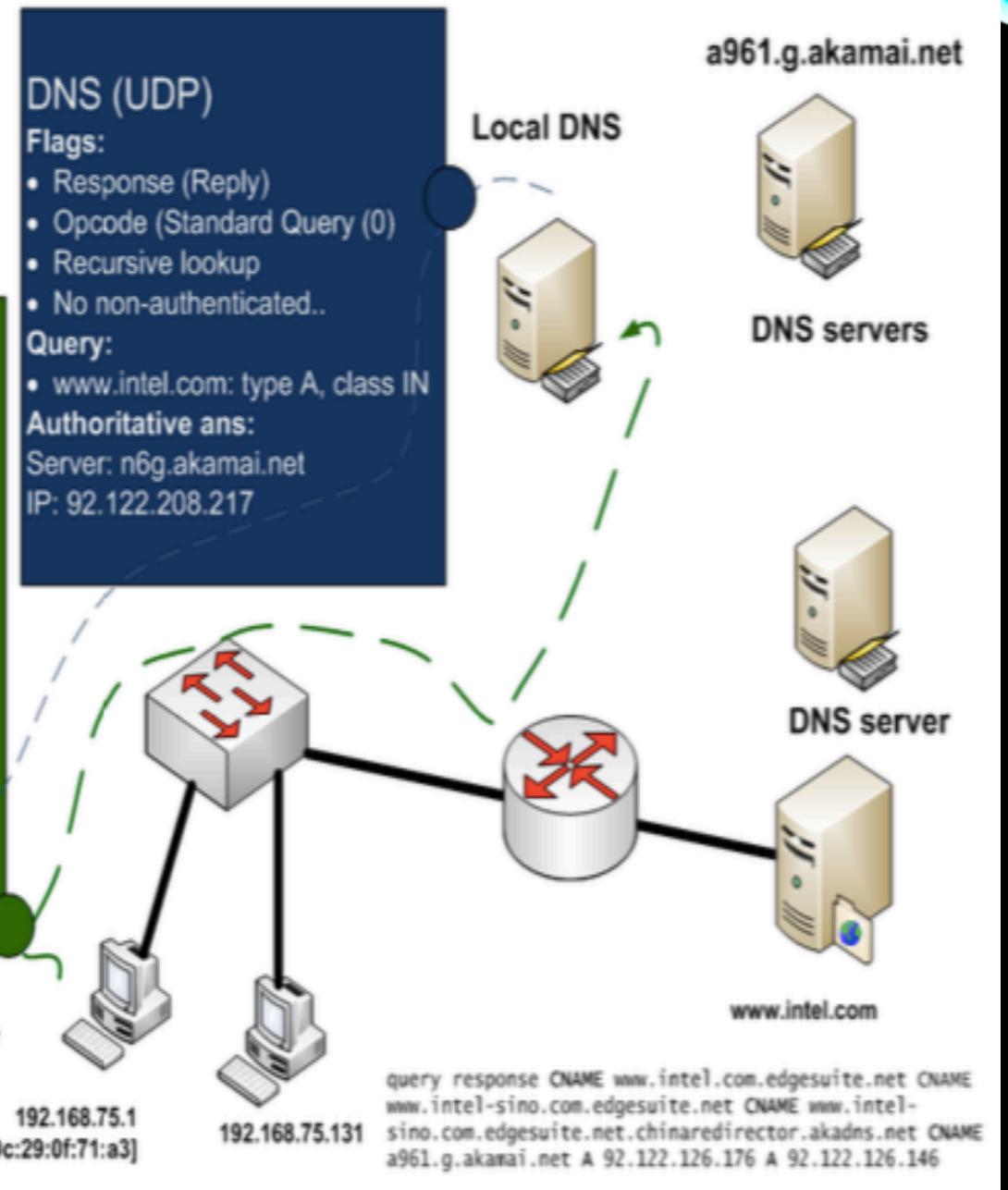
Flags:

- Response (Query)
- Opcode (Standard Query (0))
- Recursive lookup
- No non-authenticated..

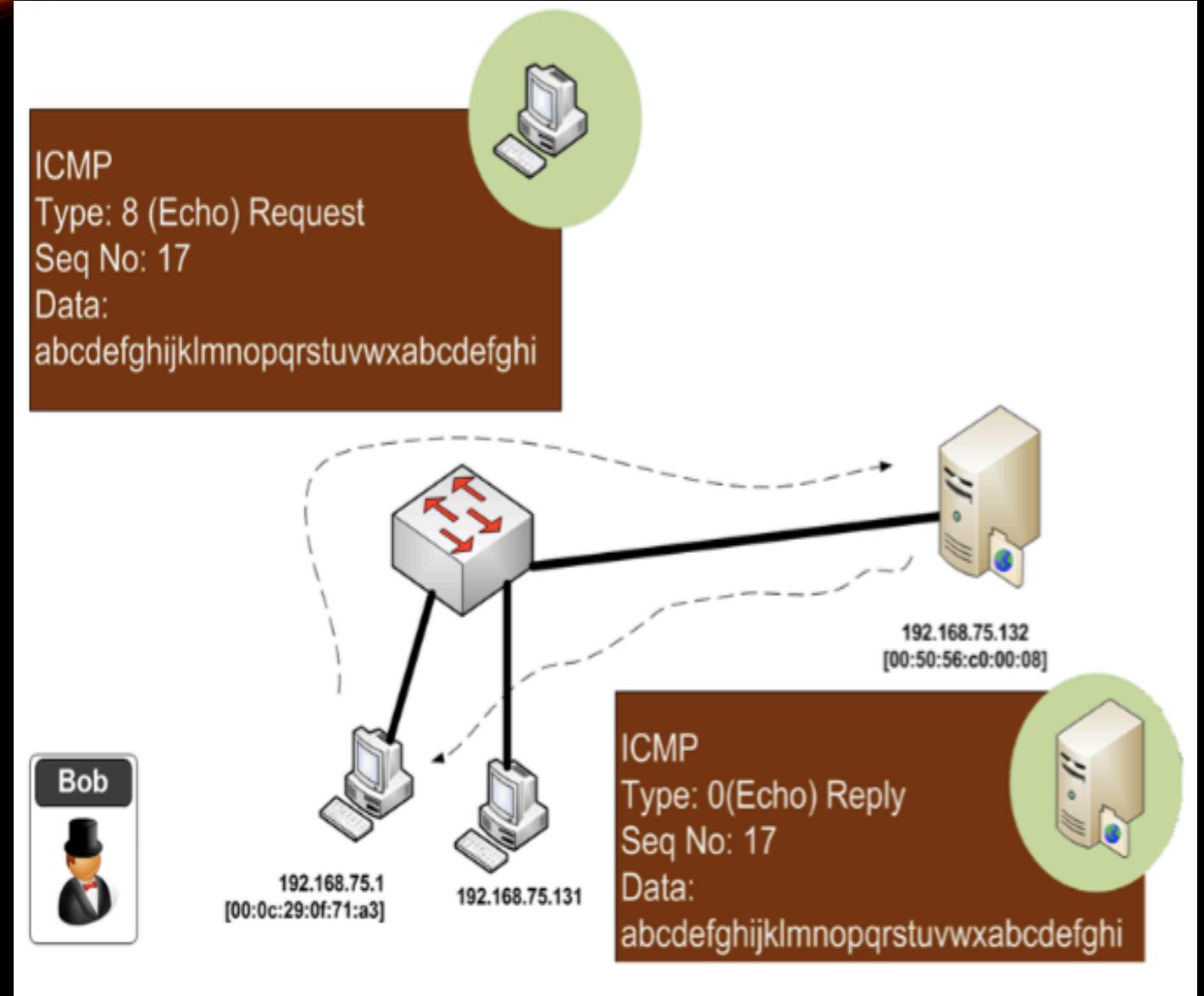
Query:

- www.intel.com: type A, class IN

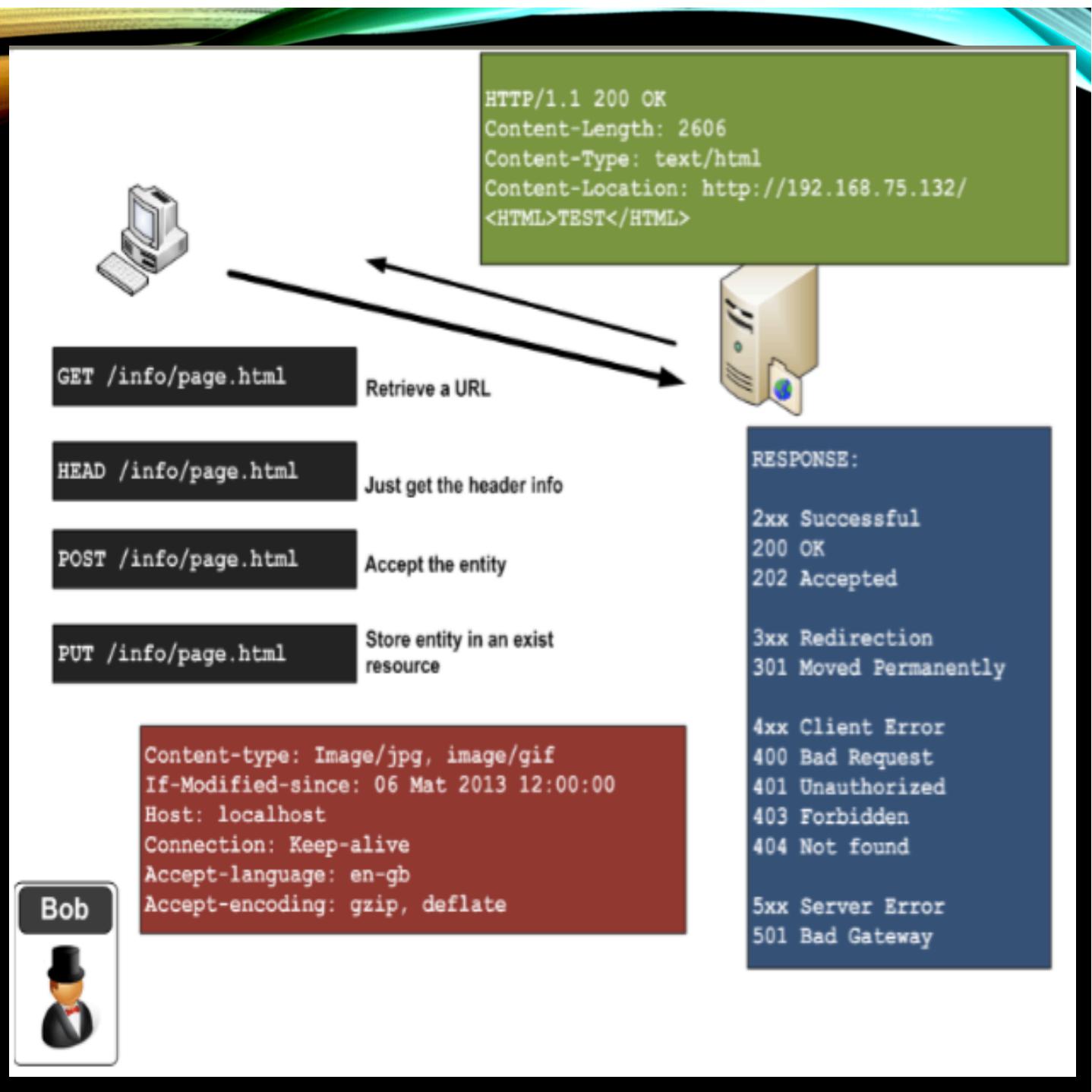
Bob

ICMP OPERATION



HTTP OPERATION



PERTANYAAN REVIEW

1. Berikut ini adalah contoh poranti jaringan intermediate (2 item)
 - a. Servers
 - b. Routers
 - c. Switches
 - d. Printers
2. Manakah dua keuntungan utama packet switched network
 - a. Banyak user dapat berbagi bandwidth jaringan pada waktu yang sama
 - b. Link aman digunakan antar hosts
 - c. Packet dikirimkan melalui dedicated circuit
 - d. Reliabilitas, paket dapat melintasi jalur berbeda sesuai ketersediaan pada waktu yang sama

PERTANYAAN REVIEW

3. Apa pengertian tentang information integrity?
 - a. Hanya user yang sah yang dapat mengubah data
 - b. Hanya user yang sah yang dapat melihat data
 - c. Hanya user yang sah yang memiliki akses ketika membutuhkannya
 - d. Hanya user yang sah yang dapat merusak data
4. Manakah yang bukan tujuan utama keamanan?
 - a. Authorisation
 - b. Confidentiality
 - c. Availability
 - d. Integrity

PENILAIAN

Kegiatan	Prosentase
Tugas #1	xx %
UTS	xx % > Tugas
Tugas #2	xx %
UAS	>= 45%
Kehadiran	OK >= 75% > tidak bisa ikut UAS