**3 Security Software**

1. Firewall
2. Anti-Malware
3. Anti-Spyware

Data exists in three states]: 1) stored, 2) transmitted, 3) processed

**Networks**

Internet

LAN

A

NIC

Client

Web Server

packets packets

Packet

STIC, DST, INDEX #, Payload

The **Network Interface Controller (NIC)** is connected to a client.

**Packet sniffers** intercept and log traffic passing over a network. **Packet switching** is a method that groups all transmitted data: **Transmission Control Protocol (TCP)**- corrects the errors and **Internet Protocol (IP)** finds the address.

**Tracert (tracing route**) is used to show the route taken by packets across an IP network.

**Time to Live (TTL)** packets is a limit on the period of time or number of iterations or transmissions in a computer and computer network technology that a unit of data (a packet) can experience before it should be discarded.

**Media Access Control (MAC)** belongs to the hardware.

IP Address belongs to the software.

**3 Characteristics of Information Protection (CIA)**

1. **Confidentiality**

* Authorization i.e login & password
* Access Controls
  + Privileges : things you are allowed to do on the computer
  + Privilege escalation: coming in under a restriction set and gaining higher privileges (“pwn” or own)
  + Mandatory Access Control: To set up Control
  + Identity Based Access Controls (IBAC) : controls set for individual users
  + Role Based Access Controls (RBAC): Taking the identity controls and adding them to the group
* Authenticate
  + Single Factor (i.e. only have a password)
  + Two factors (card + code)
  + Multiple Factors
  + Token cards
  + Dongles
  + Biometrics (finger prints, facial markers, retina scan)

1. **Integrity** : Making sure Information is correct
   * Entered Correctly
   * Processed Correctly (software bugs)
   * Stored Correctly
   * Not modified without authentication
2. **Availability** : Information is where it’s needed so when it is needs you can get to it in the form you need it.
   * Redundancy: fail safe systems
   * Safe from DDS attacks

**3 Stages**

1. Prevent
   * loss of data/loss of services
2. Mitigate
   * Segments, backups, redundancy
3. Recover
   * Forensics

Security Productivity