**COMMON PORTS**

**Telnet - Telecommunications Network**

* TCP/23
* Login remotely
* Console Access
* In-the-clear communication (not secure)
* Not best choice for production systems

**SSH - Secure Shell**

* tcp/22
* Looks and acts like Telnet
* Encrypted communication link

**DNS - Domain Name System**

* udp/53
* Converts names to IP addresses.

**SMTP - Simple Mail Transfer Protocol**

* TCP/25
* Server to Server mail transfer
* Also used to send mail from a device to a mail server

**SFTP - Secure File Transfer Protocol**

* TCP/22
* Encrypted using SSH

**FTP - File Transfer Protocol**

* TCP/20 (Active mode data), TCP/21 (Control)
* Transfers files between systems

**TFTP - Trivial File Transfer Protocol**

* UDP/69
* Simple file transfer application
* No authentication

**DHCP - Dynamic Host Control Protocol**

* UDP/67, UDP/68
* Automatic configuration of IP addresses, subnet mask and other options
* Requires DHCP server
* Dynamic / pooled
  + IP addresses assigned in real-time from a pool
* Each system is given a lease and must be renewed at set intervals

**DHCP Reservations**

* Addresses are assigned by MAC address in the DHCP server
* Quickly manage addresses from one location

**HTTP HTTPS - Hypertext Transfer Protocol (secure)**

* HTTP
  + TCP/80
* HTTPS
  + TCP/443

**SNMP - Simple Network Management Protocol**

* UDP/161
* Gather statistics from network devices

**RDP - Remote Desktop Protocol**

* TCP/3389
* Share a desktop from a remote location

**NTP - Network Time Protocol**

* UDP/123
* Every device has its own clock (switches, routers, etc)

**SIP - Session Initiation Protocol**

* VOIP signaling
  + TCP/5060, TCP/5061

**SMB - Server Message Block**

* TCP/445
* File sharing, printer sharing
* Also called CIFS (Common Internet File System)
* Direct SMB communication over TCP without NetBIOS transport

**POP / IMAP**

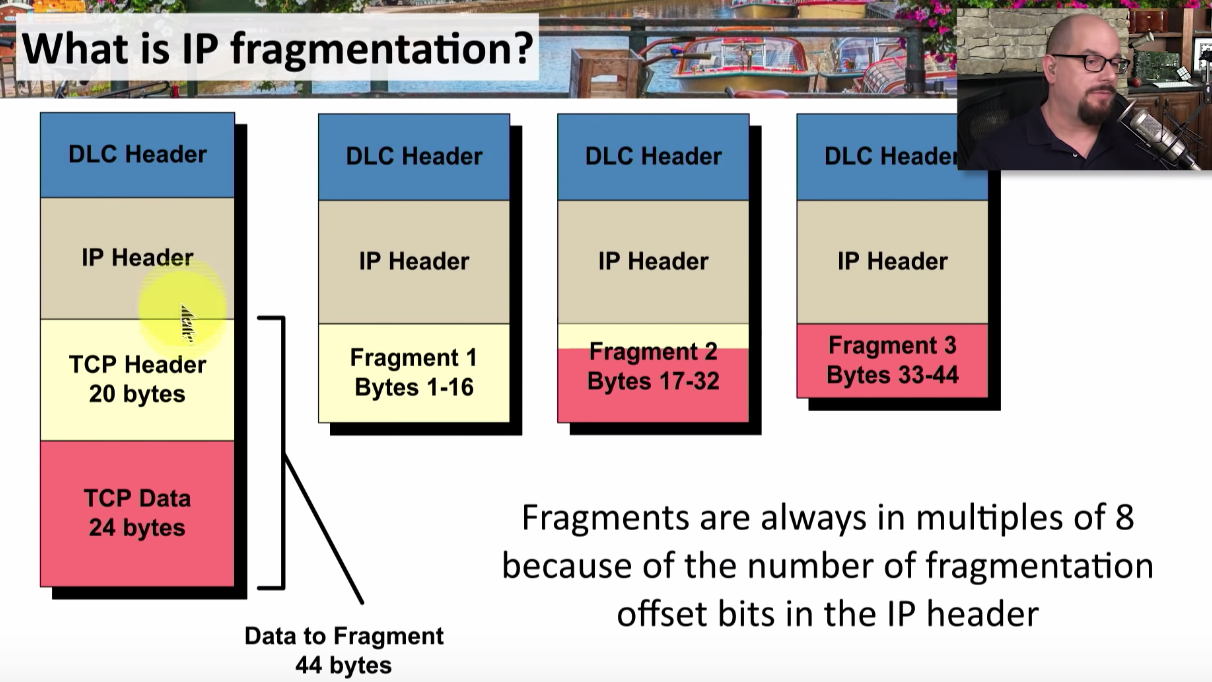
* Receive emails from email server
  + Authenticate and transfer
* POP3 - Post Office Protocol v3
  + TCP/110
  + Basically mail transfer authority
* IMAP 4 - Internet Message Access Protocol
  + TCP/143
  + Includes management of email inbox from multiple clients

**LDAP - Lightweight Director Access Protocol**

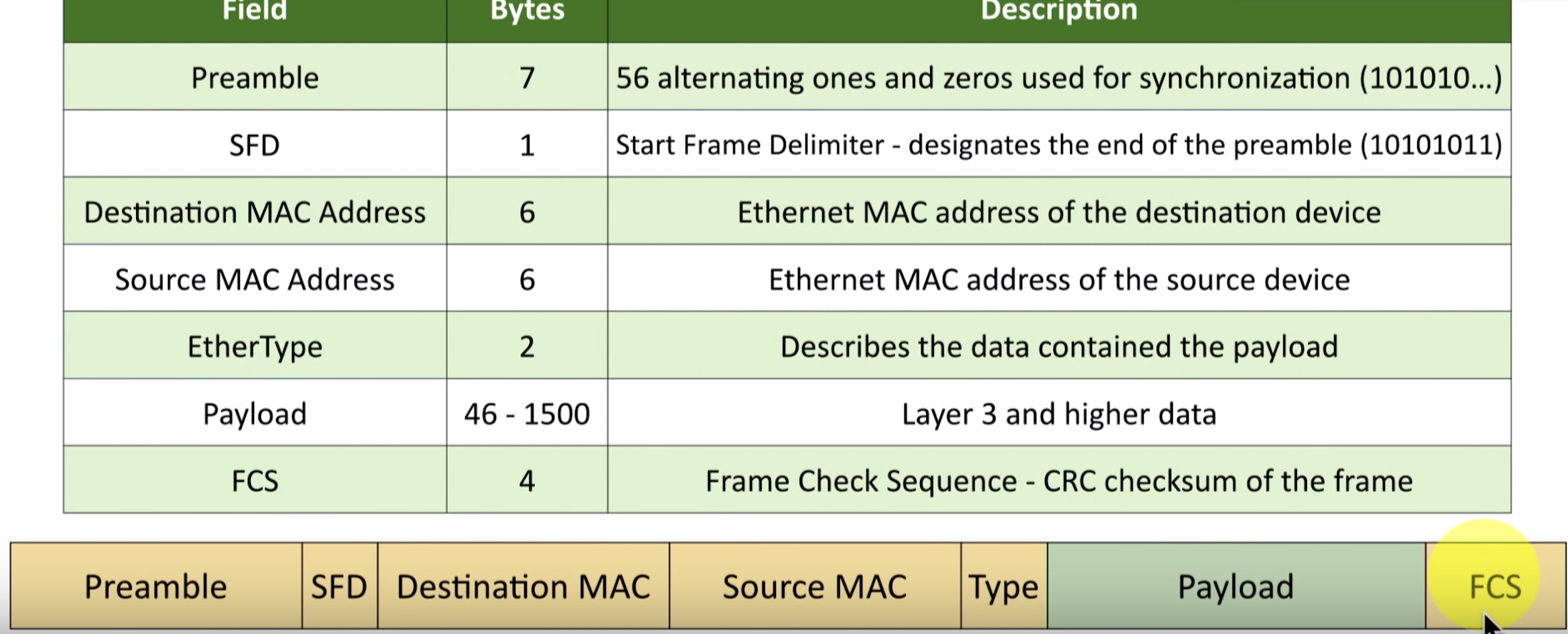
* TCP/389
* Store and retrieve information in a network directory
* LDAPS (Secure)
* TCP/636
* Non-standard implementation of LDAP over SSL

**H.323**

* TCP/1720
* VoiP Signaling
* ITU Telecommunication H.32x protocol series
* Setup and manage VoiP sessions

****

# THE ETHERNET FRAME



# OSI MODEL - Open Systems Interconnection Reference Model

* Layer 7 - Application
* Layer 6 - Presentation
* Layer 5 - Session
* Layer 4 - Transport
* Layer 3 - Network
  + The ‘routing’ layer
  + Internet Protocol (IP)
  + Fragments frames to traverse different networks
* Layer 2 - Data Link
  + The basic network ‘language’
    - The foundation of communication.
  + Data Link Control (DLC) protocols
    - MAC address on Ethernet
  + The ‘switching’ layer
* Layer 1 - Physical
  + Signaling, cabling, connectors
  + Not about protocols

# MAC Address

* Ethernet Media Access Control address
  + The physical address of a network adapter
  + Unique to a device
* 48 bits / 6 bytes long
  + Displayed in hexadecimal
  + First 3 bytes is the **Organizationally Unique Identifier**
    - (The manufacturer)
  + Last 3 bytes is the **Network Interface Controller-Specific**
    - (The serial number)

# i.e. 8c:2d:aa:4b:98:a7

* Layer 2 of the OSI model