



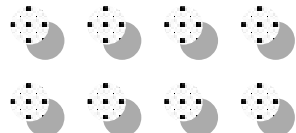
Erasmith Presentation

On Technical Concepts

01/29/25

Table of Contents

- Introduction for EMS
- ITIL
- OSI Model
- Basic Commands
- DNS
- Network and Networking
- Networking Devices
- IP Addressing
- Linux



Introduction of EMS

What is EMS?

- The Enterprise Management System (EMS) is a centralized platform that acts as a "mission control" for IT environments. It provides efficient control and monitoring of distributed systems by:
- Filtering, correlating, and processing events from network devices, databases, and applications.
- Offering a graphical interface for real-time management.
- Mapping complex dependencies between system components.



Key Features of EMS

- **Quick Problem Solving:** EMS shows how system failures affect business and helps prioritize fixes.
- **Real-Time Monitoring:** Provides a web-based interface to check and manage system health.
- **Service Management:** Ensures quality services while keeping costs low.

Why is EMS Important?

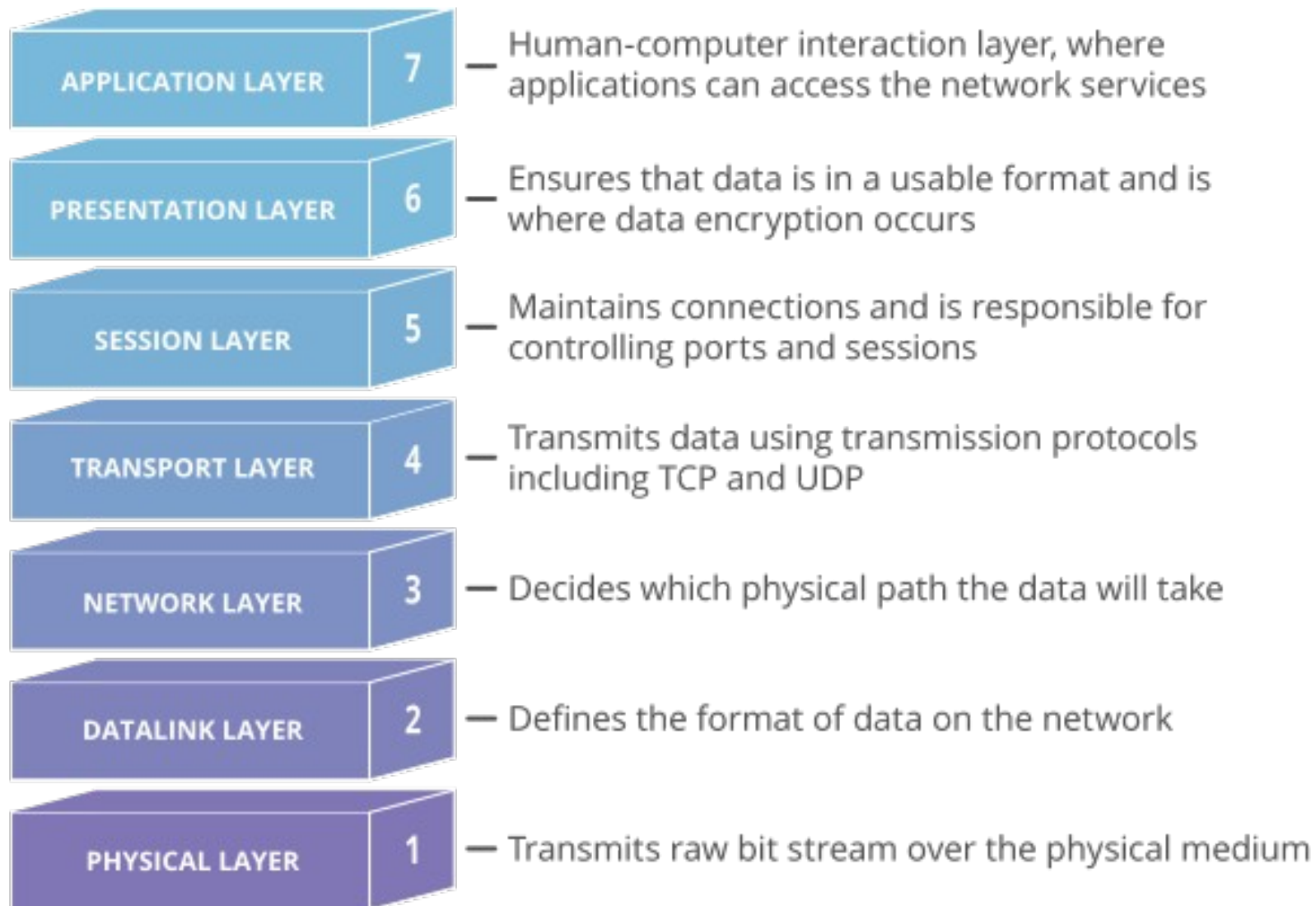
- It makes IT management easier by showing everything in one place.
- Helps prevent problems before they occur.
- Reduces downtime by fixing issues faster.

ITIL

ITIL is a framework of best practices for delivering IT services. ITIL's systematic approach to IT service management can help businesses manage risk, strengthen customer relations, establish cost-effective practices, and build a stable IT environment that allows for growth, scale and change.

OSI

- The **Open Systems Interconnection** (OSI) model describes seven layers that computer systems use to communicate over a network.
- The OSI 7-layer model is still widely used, as it helps visualize and communicate how networks operate, and helps isolate and troubleshoot networking problems.



Basic Commands

PING COMMAND

- Ping is a command-line utility that acts as a test to see if a networked device is reachable.

TELNET Command

- Telnet is a computer protocol that was built for interacting with remote computers.
- Telnet is one of the simplest ways to check connectivity on certain ports.
- **Command: telnet [domainname or ip] [port]**

```
kira@kira-ASUS-TUF:~$ telnet google.com 80
Trying 142.250.196.46...
Connected to google.com.
Escape character is '^]'.
GET / HTTP/1.1
Host: google.com

HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/
Content-Type: text/html; charset=UTF-8
Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-rmAkRQRjvl8b4pwPCyKZdg' 'strict-dynamic'
ttp;;report-uri https://csp.withgoogle.com/csp/gws/other-hp
Date: Tue, 28 Jan 2025 14:03:00 GMT
Expires: Thu, 27 Feb 2025 14:03:00 GMT
Cache-Control: public, max-age=2592000
Server: gws
Content-Length: 219
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
```

Netstat Command

- Displays active TCP connections, ports on which the computer is listening.

Parameters

- -a: Shows active TCP connections and listening TCP/UDP ports.
- -b: Displays executable creating connections or listening ports (requires permissions).
- -e: Shows Ethernet stats (bytes/packets sent/received). Combine with -s.
- -n: Displays active TCP connections with numeric addresses/ports.
- -o: Shows active TCP connections with Process ID (PID). Combine with -a, -n, -p.
- -p <Protocol>: Shows connections/stats for specified protocol (e.g., TCP, UDP, IPv6).
- -s: Displays protocol stats (e.g., TCP, UDP, ICMP). Use with -p for specific protocols.
- -r: Displays IP routing table (same as route print).
- <interval>: Updates info every <interval> seconds (Ctrl+C to stop).
- /?: Displays help.

ARP Command

- Displays and modifies entries in the Address Resolution Protocol (ARP) cache.
- Used without parameters, arp displays help information.

- **/a [<inetaddr>] [/n <ifaceaddr>]:** Displays current ARP cache tables; specify inetaddr for a specific IP or ifaceaddr for a specific interface.
- **/g [<inetaddr>] [/n <ifaceaddr>]:** Same as /a.
- **/d <inetaddr> [<ifaceaddr>]:** Deletes an ARP entry; use inetaddr for specific IP or ifaceaddr for specific interface. Use * to delete all entries.
- **/s <inetaddr> <etheraddr> [<ifaceaddr>]:** Adds a static ARP entry; specify inetaddr (IP), etheraddr (MAC), and optional ifaceaddr for specific interface.
- **/?:** Displays help.
-

Nslookup Commands

- **Nslookup** (stands for “Name Server Lookup”) is a useful command for getting information from DNS server.
- Syntax: **nslookup [option]**

Network and Networking

- **NETWORK-** A network is an interconnection of devices
- **NETWORKING-** Networking is the communication between the interconnected devices

Types of Networks

- LAN – Local area network
- MAN - Metropolitan Area Network
- WAN - Wide Area Network

Network Devices

- **NIC:** Network Interface Card forms a bridge between a computer and the Ethernet (LAN).
- **MAC Address:** Unique identifier for network interfaces (e.g., 01-23-45-67-89-ab).
- **HUB:** Connects devices on a network; always broadcasts data.
- **Switch:** Connects devices; initially floods but switches to unicast after learning device locations.
- **Router:** Enables communication between networks in different geographical locations.

IP Addressing

- Two versions of addressing scheme
 - - IP Version 4 – 32 bit addressing
 - - IP Version 6 – 128 bit addressing

IP ADDRESS CLASSES

- Total IP Addressing Scheme is divided into 5 Classes



Class Ranges

- Class A Range: 0.0.0.0 - 127.255.255.255
- Class B Range: 128.0.0.0 - 191.255.255.255
- Class C Range: 192.0.0.0 - 223.255.255.255
- Class D Range: 224.0.0.0 - 239.255.255.255
- Class E Range: 240.0.0.0 - 255.255.255.255

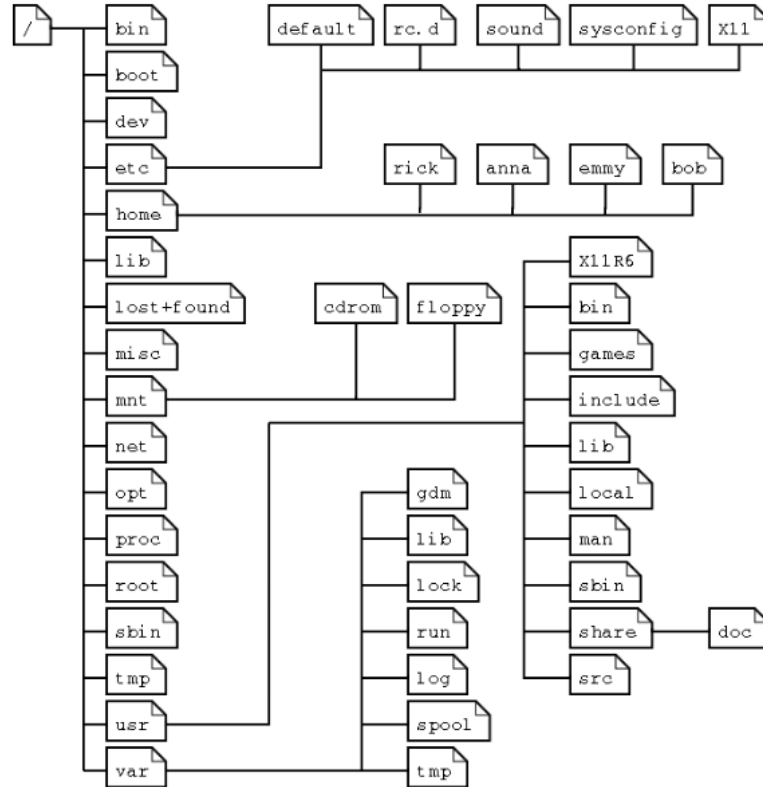
OCTET FORMAT

- CLASS A is written as N.H.H.H
- CLASS B is written as N.N.H.H
- CLASS C is written as N.N.N.H

Private and Public IP Address

- Private IP Address:
- Class A: 10.0.0.0 – 10.255.255.255
- Class B: 172.16.0.0 – 172.31.255.255
- Class C: 192.168.0.0 – 192.168.255.255

Linux File System



- /bin: Common programs for system and users.
- /boot: Startup files, kernel, and GRUB boot loader data.
- /dev: References to peripheral hardware, represented as files.
- /etc: System configuration files (like Windows Control Panel).
- /home: Home directories for users.
- /initrd: Boot information (do not remove).
- /lib: Libraries for system and user programs.
- /lost+found: Stores recovered files after failures.
- /misc: Miscellaneous purposes.
- /mnt: Mount point for external file systems (e.g., CD-ROM).
- /net: Mount point for remote file systems.
- /opt: Extra/third-party software.
- /proc: Virtual file system with system resource info (man proc for details).
- /root: Root user's home directory (different from /).
- /sbin: System admin programs.
- /tmp: Temporary space, cleared on reboot.
- /usr: Programs, libraries, and docs for user programs.
- /var: Variable files (logs, mail queue, temp storage, etc.).

Important Log Files

- `/var/log/syslog` (Debian/Ubuntu) or `/var/log/messages` (RHEL/CentOS): Stores global system activity, including startup messages.
- `/var/log/auth.log` (Debian/Ubuntu) or `/var/log/secure` (RHEL/CentOS): Records security events like logins and root actions.
- `/var/log/kern.log`: Contains kernel events, errors, and warnings for troubleshooting custom kernels.
- `/var/log/cron`: Logs scheduled task (cron job) execution details.
- `/var/log/boot.log`: Records bootup messages, including issues with shutdowns, reboots, or boot failures.

Basic Commands



- Ls - Command to list the contents of the directory
- Cat - used to concatenate files.
- Cp - used to copy files
- Mv - used to move files
- Rm - used to remove files
- Rmdir - delete the directory
- Mkdir - Make a directory
- Chmod - Change the attribute of an existing file
- Ln - create a link for a file
- Man,info - gives information and options about a command

- Chown – command to check the ownership of a file
- Ip , ifconfig – display and configure ip address
- Top – shows system resource utilization
- Tail – shows the last 10 lines of a file
- Head – show the first 10 liens of a file
- Locate – helps to locate a file

Tmux

- Tmux new -S session_name – create a session
- Ctrl+b , d – detach session
- Tmux ls – list all sessions
- Tmux attach-session -t session_id – reattaches the session

Server Command

- Uptime – shows the running time of the server
- Date – shows the date, time and timezone of the server
- lsb_release – shows the OS details of server

- Uname – to display the architecture
- Init – used to change the init or run level on the server

THANK YOU

