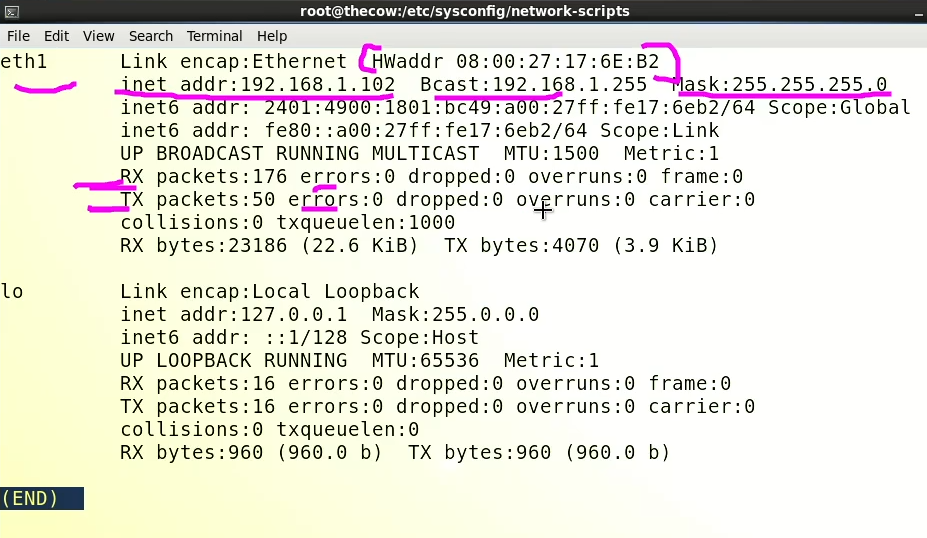
Lecture 04

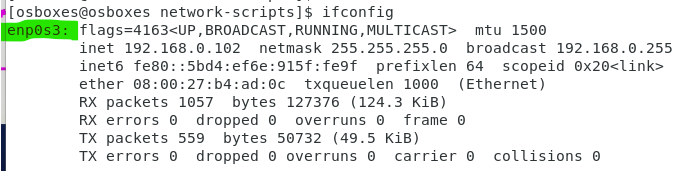
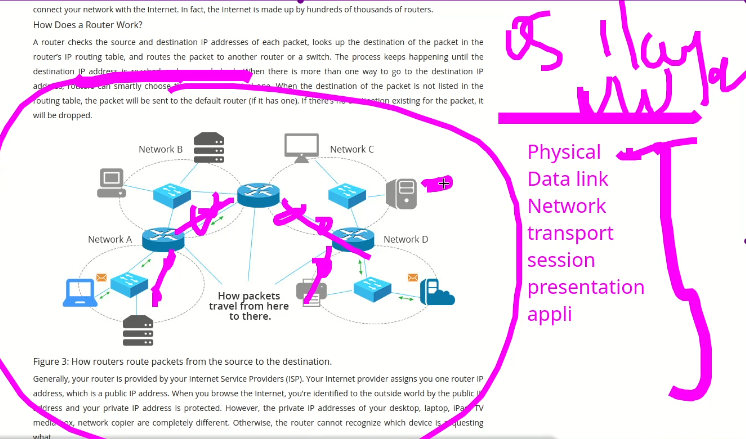
**NW5-Protocols-Ports-OSILayer.ts**

$ ifconfig



RX – received packets

TX – transferred packets

* IP addresses are sued to reach the specific location on network
* In RHL 7 & 8 eth0 is called “ens”
* 
* Driver (eth0 in RHL 6) is always associated with ports or interface. Not NIC no “eh0”or driver
* Each port has unique MAC ID 🡪 2 ports 2 MAC IDs and so on…
* “lo” interface 🡪 loopback interface is always present even if there is no NIC
* Used for local machine (for testing purpose) connection. 🡪 it is not connected outside the network.
* Its IP is 127.0.0.1 🡪 this IP is called “localhost”.
* OSI layers (model)
* Used for troubleshooting purpose
* Supposes if NIC is not working an Administrator will say “there is an issue with physical layer”
* 
* “transport layer” is brain of OSI model which is used for data packet travelling
* For the sake of remembering it remember this phrase
* “Please Do Not Tell Secret Password Any”

1. Physical
2. Data Link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

**Protocols**

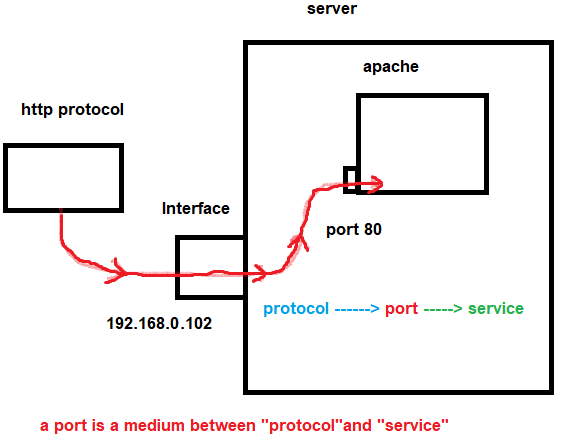
* Protocols are “set of rules”. 🡪 a bus can only run at a road not a railway track similarly a train runs on a railway track not on the road, this example of protocols. **Protocols has specific tasks to perform.**
* Network protocol travels in “transport” layer or “layer-4” while transferring and on server protocols rest in “Application layer” or “layer -4”.
* Types of protocols
  + http,ftp, smtp, ssh, nfs, dns, dhcp, smp

A network protocol is a set of rules and standards that govern how data is transmitted over a network. Some common network protocols include:

* + TCP (Transmission Control Protocol): A reliable, stream-oriented protocol that establishes a virtual connection between two devices and ensures that all data is properly received.
  + UDP (User Datagram Protocol): A connectionless, unreliable protocol that allows for faster data transfer but does not guarantee delivery or order of packets.
  + IP (Internet Protocol): A protocol that provides the foundation for communication over the internet. It is responsible for routing packets of data to their destination through a network of devices.
  + HTTP (Hypertext Transfer Protocol): A protocol used for transmitting data over the web. It is the foundation of communication for the World Wide Web. To grab web pages
  + FTP (File Transfer Protocol): A protocol used for transferring files between computers on a network. Data transfer
  + SSH (Secure Shell): A protocol used for securely accessing and managing remote systems. For remote sessions
  + DNS (Domain Name System): A protocol used to convert human-friendly domain names (such as [www.example.com](http://www.example.com/)) into IP addresses that computers can understand.
  + SMTP (Simple Mail Transfer Protocol): A protocol used for sending and receiving email.
  + DHCP (Dynamic Host Configuration Protocol): A protocol that enables network administrators to assign IP addresses to devices on a network dynamically.

IMPORTANT:- Network devices e.g routers and switches are programmed in a way that they can differentiate protocols and the tasks they perform.

**Ports**

* Ports are configured inside the devices and servers.
* **Ports are associated with protocols.**
  + Protocols come through IP and land on specific port.
  + Specific ports are associated with specific services
  + Some commonly used ports and services are,
    - Port 22: SSH (Secure Shell) - used for securely accessing and managing remote systems.
    - Port 25: SMTP (Simple Mail Transfer Protocol) - used for sending and receiving email.
    - Port 53: DNS (Domain Name System) - used for converting human-friendly domain names into IP addresses.
    - Port 80: HTTP (Hypertext Transfer Protocol) - used for transmitting data over the web.
    - Port 110: POP3 (Post Office Protocol version 3) - used for retrieving email from a mail server.
    - Port 443: HTTPS (HTTP Secure) - used for securely transmitting data over the web.
    - Port 3306: MySQL - used for connecting to a MySQL database.
    - Port 3389: RDP (Remote Desktop Protocol) - used for remotely accessing and controlling another computer.
    - Port 22: SFTP (Secure File Transfer Protocol) - used for securely transferring files between computers.
    - Port 67: DHCP (Dynamic Host Configuration Protocol) - used for assigning IP addresses to devices on a network dynamically.
* Ports are like gates 🡪 inside server specific service is starts and associated port open for connection.
* If a specific port is closed 🡪 it means that specific service is not running
* Once the specific service is started 🡪 the port associated with this service also opens
* To open port 🡪 start the service
* $ service httpd start
* To close a port 🡪 stop the service
* $ service httpd stop
* The service lays behind specific port
* 
* Port no can be changed by changing “config” file of a specific service 🡪 but it will create conflict
* Remember we can not make change in a “protocol”
* The solution is we need to inform the client that the port is changed so that the request may carry port no also like this 🡪 if apache service port is changed from 80 to 800 so the request should be like this
  + 192.168.0.102:800
* What port nos to be remembered?
* http 80
* https 443
* dns 53
* ssh 22
* telnet 23
* mysql 3306
* ftp 21 and 20
* smtp 25
* pop3 110
* imap 143
* psp3s 995
* imaps 993
* ldap 389
* rdesktop 3389
* tomcat 8080
* samba 137 and 139
* squd 3128
* all port nos are mentioned in “etc service”
* $ cat /etc/services
* Tip:- to search within use “/” followed by string
* 