**Ethernet Hub:**

An **Ethernet hub**, **active hub**, **network hub**, **repeater hub**, **multiport repeater** or **hub** is a device for connecting multiple Ethernet devices together and making them act as a single network segment. It has multiple input/output (I/O) ports, in which a signal introduced at the input of any port appears at the output of every port except the original incoming. A hub works at the physical layer (layer 1) of the OSI model. The device is a form of multiport repeater. Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it detects a collision.

Hub has no intelligence.

A network hub is an unsophisticated device in comparison with, for example, a switch. A hub does not examine or manage any of the traffic that comes through it: any packet entering any port is rebroadcast on all other ports. Effectively, it is barely aware of frames or packets and mostly operates on raw bits or *symbols*. Consequently, due to the larger collision domains, packet collisions are more frequent in networks connected using hubs than in networks connected using more sophisticated devices.

**Ethernet switch**:

An **ethernet switch** is a device used to build a network connection between the attached computers (allows computers to talk to each other). It differs from an ethernet hub: While a hub will send incoming data packets to all ports, a switch understands the packets' addressing scheme and will send any data packet only to its destination port, thus limiting the number of collisions (data sent at the same time).

---------------------------------------------------------------------------------------------------------------------------------

Q) What are Private addresses?

A)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| RFC1918 name | IP address range | number of addresses | largest[**CIDR**](http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing)block (subnet mask) | host id size | mask bits | [***classful***](http://en.wikipedia.org/wiki/Classful_network)description |
| 24-bit block | 10.0.0.0 - 10.255.255.255 | 16,777,216 | 10.0.0.0/8 (255.0.0.0) | 24 bits | 8 bits | single [class A network](http://en.wikipedia.org/wiki/Class_A_network) |
| 20-bit block | 172.16.0.0 - 172.31.255.255 | 1,048,576 | 172.16.0.0/12 (255.240.0.0) | 20 bits | 12 bits | 16 contiguous class B networks |
| 16-bit block | 192.168.0.0 - 192.168.255.255 | 65,536 | 192.168.0.0/16 (255.255.0.0) | 16 bits | 16 bits | 256 contiguous class C networks |

APIPA provides address range from 169.254.0.0 – 169.254.255.255

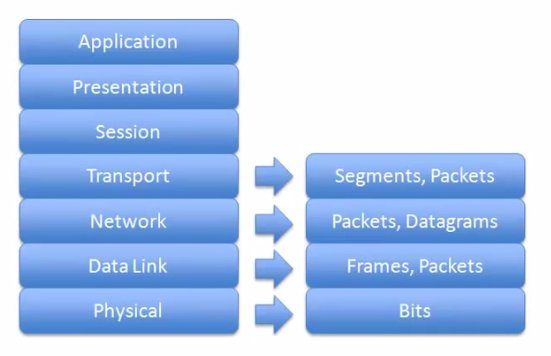
------------------------------------------------------------------------------------------------------------------------------------

ICND1:

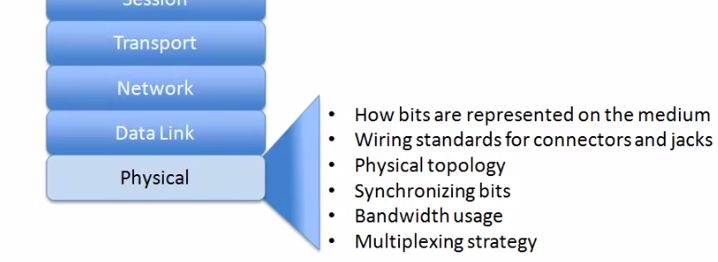
OSI is a reference model, OSI is not a reverence model.

I mean, Not every layer has to be populated with the implementation. It all depends on the scenario.

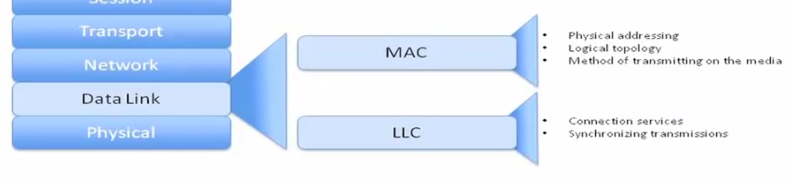
Protocol Data Units at different layers:



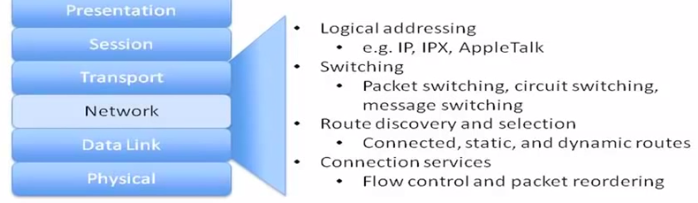
Physical Layer:



Data Link Layer:



Network Layer:



-----------------------------------------------------------------------------------------------------------------------------------------

Q) What is Packet Switching?

A) IP layer at sender machine divides the message received from TCP into multiple packets and sends over the internet, **Identification** field in IP header maintains the sequence of these packets. Destination IP layer re-assembles the packets using this **Identification** field in IP header, if the sequence is missing, all the packets are discarded. It is upto the TCP to maintain the ordering by using **seq\_ num** field in TCP header. Here IP is a “physical layer” and TCP is a “logical layer” for packet switching.

------------------------------------------------------------------------------------------------------------------------------------------

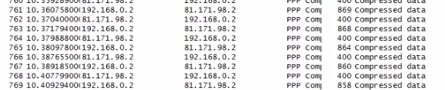
----------------------------------------------------------------------------------------------------------------------------------

Q) Why IPSec VPN?

A) Your immediate ISP will not be able to know, what you are doing, when you are through VPN. ISP cannot know your IP address. ISP cannot track your packets.

There are different protocols used in VPN , one is PPTP and the other is L2TP.

So, If ISP runs a Wireshark for my IP, then he will see some thing like this. Each packet is encrypted.



So here 192 is my IP and 81 is VPN server IP back and forth.

----------------------------------------------------------------------------------------------------------------------------------