

Information Security - II
Prof. V. Kamakoti
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 40
Network Processors, Security and Performance

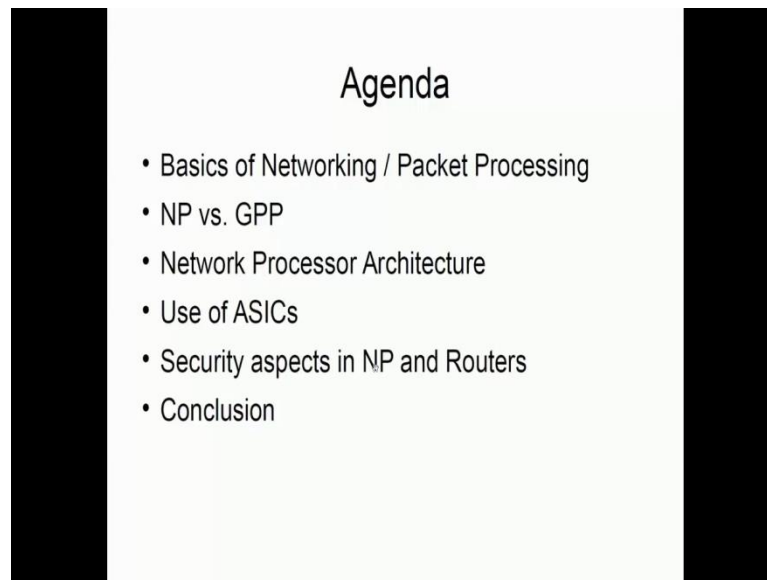
(Refer Slide Time: 00:09)



Network Processors, Security and
Performance

Welcome to the section on Network processors, Security and Performance. This is going to be an introductory level talk on, how one goes about designing a router, a network processor within a router and then what are all the components within a high speed router that you can see. The question is what is the difference between a general purpose processor and a network processor. So, we will try to explain this during this whole lecture and we will also look at some sample, a single network processor sample. There are other companies which also make network processor, but we have taken up an example of 42,40 because in the previous section, Vasan would have talked about the free scale processor. So, we are taking one of the free scale processors as an example. The agenda for this talk is something like this.

(Refer Slide Time: 01:06)



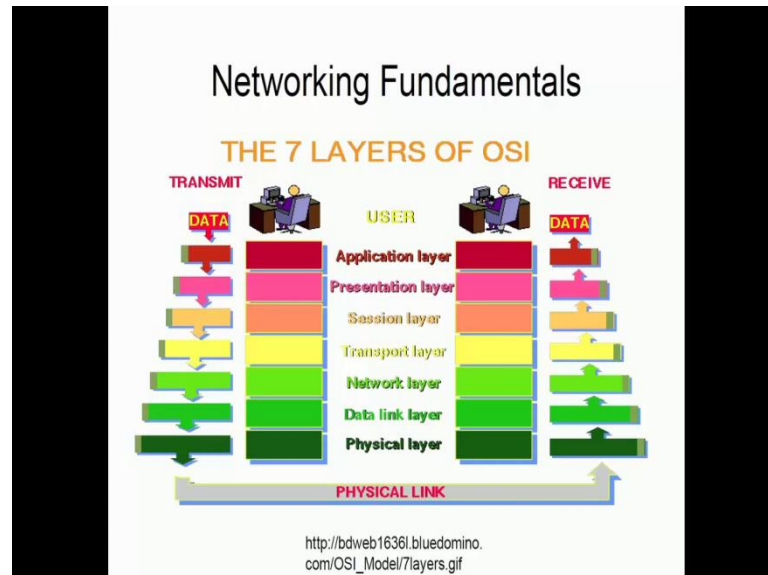
We will look at basics of networking and packet processing and then we will look at, it probably may not be in the same order, but what you are going to look at is; see once see we have to understand what is networking and what is packet processing, before you understand the architecture. Just like in a general purpose processor you talk about billion logic and things like that and then understand about bits, bytes and all those things. We will also look at the packet processing of the networking processors so there is the next level, I mean we can take it consider it as a next level.

We will see the difference between network processor and general purpose processor and we will see a sample network processor architecture and we will also see why ASICs are very important in network processor architecture. Other than security, one of the things that is needed in network processor is performance; therefore, we have to have both security and performance in a network architecture. Not there is not needed in your general purpose processor, but general purpose processors are used for say implementing algorithms, that implement security and then you also have secure chips, which can be added to the network processor and so on.

But then we will see why this becomes very important, we will be considering only the routers that are available in the industries. I am mostly going to take some examples of Cisco routers, because these materials are available on the web, so I have taken Cisco

routers as an example and then finally we will see what these that in designing network processor we should also consider both security and performance together.

(Refer Slide Time: 02:43)

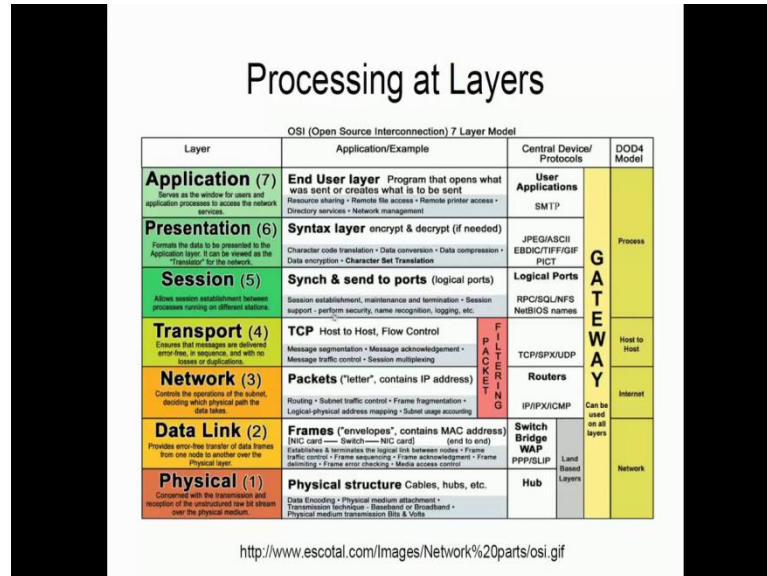


Thus, let us start with some networking fundamentals and this is a very well known fundamental stuff that most of you study, even though many of protocol don't follow this, but this can be taken as a standard. One of the things that we can look at is, see you use a transmit data package and then it is (Refer Time: 03:02) by another user and then what happens is the data packets you start adding headers and then the headers increase in size. So, if you look at this, it starts with a small data and then with every level layer that goes down, the data packets increase in size.

If you look at a router that operates more or less of the network layer and so at the network layer you call them as packets, data packets and then at the data link layer you call them as frames, the physical or a data link layer you, this is the terminology that we use. We will look at the operations that happen at this network layer, we will look at some protocols and in general how protocols process data packets. So, protocols is a way of exchanging information between two systems and then we will look at how, see that there is the commonality in this kind of packet processing and that is the reason. So, we will consider both network and data link, at data link they call it as a switching and even at the network layer you can do switching, so they are called route switchers. Then we will look

atswitching as a concept in general and then see how processor can be designed to meet the needs of performance and security.

(Refer Slide Time: 04:24)



Now, going into the detail, if you look at this let us concentrate mostly on the network or the data link layer. So, as I told you it is called packets of the network layer and frames of the data link layer, so when it comes at the packet level then the most important aspects that a router has to take care of is routing and then configuration of routers, how to configure the routers and how do you assemble smaller packets into larger packets or take bigger packets and cut it into smaller packets and so on. These are all some of the functionality that a router has to provide.

Then going down at the frames, a similar functionality is provided but here what happens is you are looking at error checking and things like this, cyclic redundancy check and so on and physical structure, you have to do physical data encoding and there are two mediums which you will usually transmit a data with wired or wireless and so on. So, another important aspect in these layers is, I mean in network processor is the power that it consumes. So obviously, I mean in general purpose is people go on to (Refer Time: 05:30) for example, the processor that Vasanth discussed in the last section, it has low power, ARM Cortex is low power. Now can we achieve that kind of low power in networking because wireless itself takes a lot of power to transmit the data, so that is another aspect in networking, where power is also one of the major considerations. Now there are other

things see, they on the right hand side you can see the devices that actually work are the different layers.

If you look at this network layer, you have routers and then just below the network layer you can use a switch or a bridge or a wireless access point and then below that you have hub. But usually a network process are used only at these two levels, that is a routing and switching point.

(Refer Slide Time: 06:26)

Packet Processing – Layer 3

Characteristics	RIPv1	RIPv2	EIGRP	IS-IS	OSPF	BGP
Distance vector	✓	✓	✓			✓
Link-state				✓	✓	
Classless		✓	✓	✓	✓	✓
VLSM support		✓	✓	✓	✓	✓
Automatic route summarization	✓	(can be disabled using no auto-summary)	(can be disabled using no auto-summary)			✓
Manual route summarization		✓	✓	✓	✓	✓
Hierarchical topology required				✓	✓	
Size of network	Small	Small	Large	Large	Large	Very large
Metric	Hops	Hops	Composite metric	Metric	Cost	Path attributes
Convergence time	Slow	Slow	Very fast	Fast	Fast	Slow

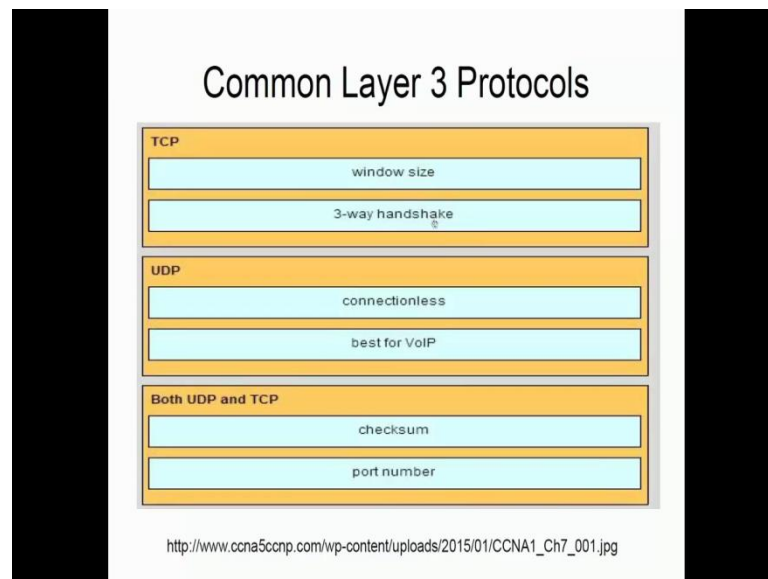
<http://www.ebrahma.com/wp-content/uploads/2013/10/Chartstics-of-Routing-protocols.png>

Now, moving on to what happens at the routing layer, see if you look at the routing layer, you have to take care; any router has to take care of all these kinds of protocols that can run on the routers. In order to take care of these protocols very straightforward, you see that there are bunch of algorithms that they are implementing, like distance vector algorithm and so on, link state algorithm and so on. So, for that you definitely need a general purpose processor, in any router box you will have a general purpose processor.

Now the other aspect of this is; it also needs, look at this, it also has to converge quite quickly, the algorithms have to converge quite quickly which essentially means that you have to transmit the packets and get the information, then the converge to a routing point very quickly; that means, you really need high speed processor and you would have read in your course that usually they make use of pipelining and parallelism for getting high speed and we will see that we will be using massive parallelism because the packets can be processed in parallel, in a network processor.

Therefore, every network processor will have massive parallelism and the other aspects of routing protocols. We will see that almost all the routing protocols actually take data package, do some kind of processing and then send the data package to some other piece. This is the common operation that actually happens in a router or a switch, I mean, I am talking in general, but let us see the specifics as we go on.

(Refer Slide Time: 07:59)

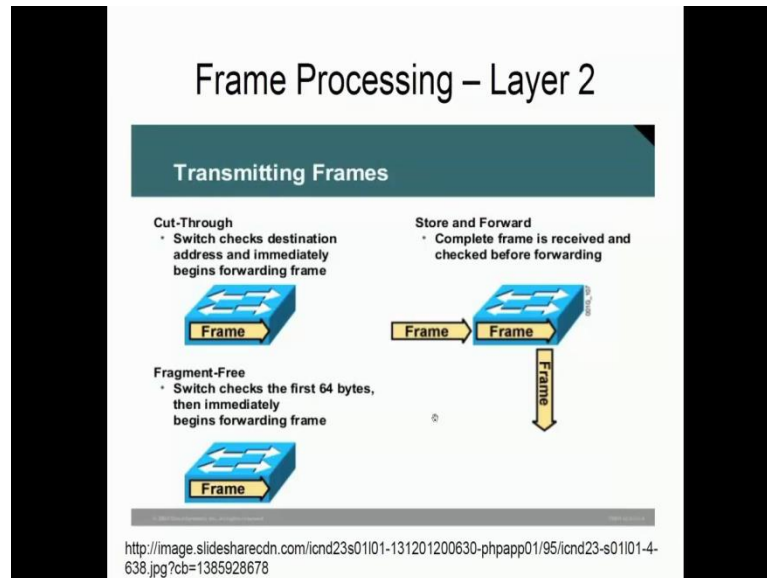


The other thing about this routing protocol is even though there are different types of routing protocols, they travel over either TCP or UDP. For example, you can have RIP all these things so all these protocols exist at this level and then they exchange data packets and all those applications that run on top, see there are two kinds of protocols, one is routing protocols and routed protocols. Routing protocols or these guys, that we have listed, routed protocols are protocols like IP, UDP, where they carry data packets and based on the information that is obtained by using routing protocols, routing happens.

Now these kind of protocols, have look at this they have a three way handshake, TCP has a three way handshake these also have to be managed. If you look at this UDP just dumps data packets, if you take UDP it just dumps data packets, it does not bother whether the link is full or not. We have to take care of these kind of stuffs, so if you dumping data packets; How does the router handle it? Does it buffer? The packets or does it drop the packets and so on. These are all some of the things that a router has to take a decision and then finally, both of them used check sum; that means, every packet that

comes in, you have to calculate check sum; that means, you need a really very fast processor to do check sum calculation.

(Refer Slide Time: 09:41)



Now, at the layer 2, at layer 3 we can implement some algorithms and then get it working. At layer 2 what happens, layer 2 there are different types of; you have to transmit the frames and for frame transmission, usually they use two types of routing known as cut through switching and then fragment free switching. So, cut through switching and store and forward switching cut through switching essentially what happens is, as soon as the packets enter a port, the bits are read and then immediately the frames are get forwarded to another port. So, if you look at this, it has to perform very high speed matching and then forward the data packets quickly.

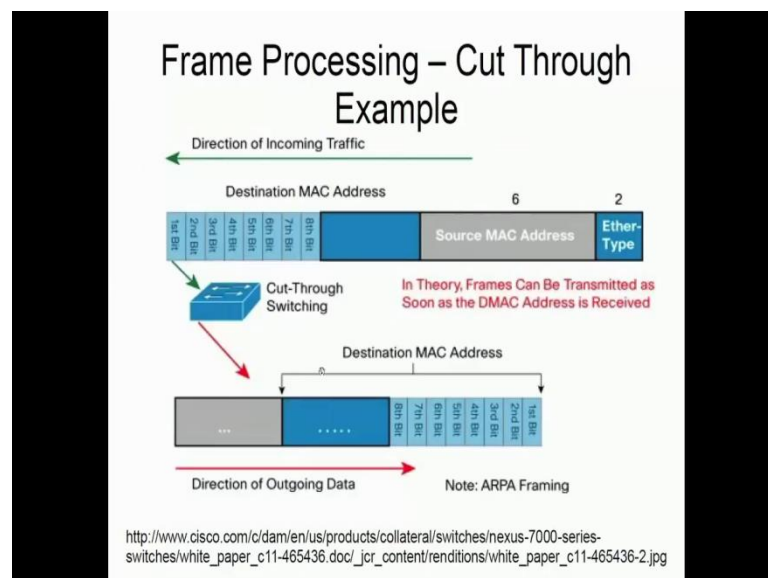
So, the first thing that happens is, if you look at this the headers; headers have to be (Refer Time: 10:31) and then they have to be matched against a particular table and then they have to be forwarded. So, three operations have to happen very quickly and it is not if this happens for every packet and if you are talking about Giga bytes per second and then Tera bytes or Tera bytes per seconds, I mean then you see how much speed is needed to process this packet.

The other way of doing this is known as a store and forward routing, where a complete frame is received. Now once you receive a complete frame, then you need a buffer, so a complete frame is received then it is checked for correctness of the frame and then it is

forwarded. As usual some of the things that, I mean and then there is a combination of these two where in a fragment free switching, what you do is you actually take the first 64 bytes, then store them and then do all the processing that you want and then forward it, you do not take the full packet.

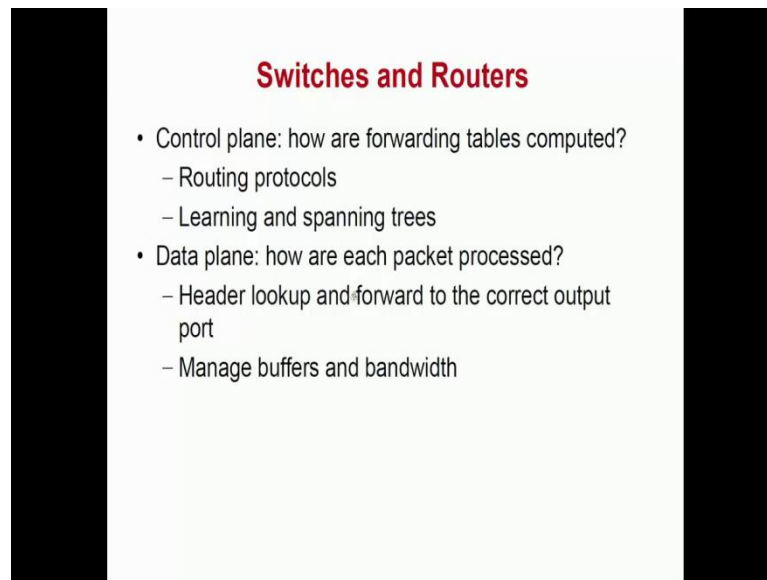
So, this is actually a compromise between the cut through and the store forward kind of a switching. Now why I am repeating, why I am saying all this is, if we look at this all these functionalities has to be incorporated into the processor, that is the idea and let us see how this is done, so that is why we share these basics.

(Refer Slide Time: 11:45)



Here is an example of cut through so as soon as the bits are received, so immediately the destination might; in theory the frames can be transmitted as soon as the D MAC address is received, as the destination MAC address is received, immediately a switching happens and then the data is forwarded. So, in this case this is a direction of incoming traffic and then immediately cut through switching happens and then the data is forwarded. In the other example of store and forward the whole packet will be stored and then a routing, a scheduler kind of stuff can take a routing decision.

(Refer Slide Time: 12:32)



Switches and Routers

- Control plane: how are forwarding tables computed?
 - Routing protocols
 - Learning and spanning trees
- Data plane: how are each packet processed?
 - Header lookup and forward to the correct output port
 - Manage buffers and bandwidth

Now if you look at both switches and routers in general, what can happen is they have; what we call it as planes, two planes; one is known as the control plane and another is known as the data plane. The control plane effectively calculates how a forwarding table is computed. So, in routing it is known as the routing table, in switching it is known as the switching table and this forwarding tables in the router is calculated using routing protocols and in switching it is; you can actually learn, self learning bridges are there; that means, as soon as an input data packet comes through, that ethernet address is put as a destination because whenever a packet with that destination comes, then this you know that the ethernet address comes in a particular port.

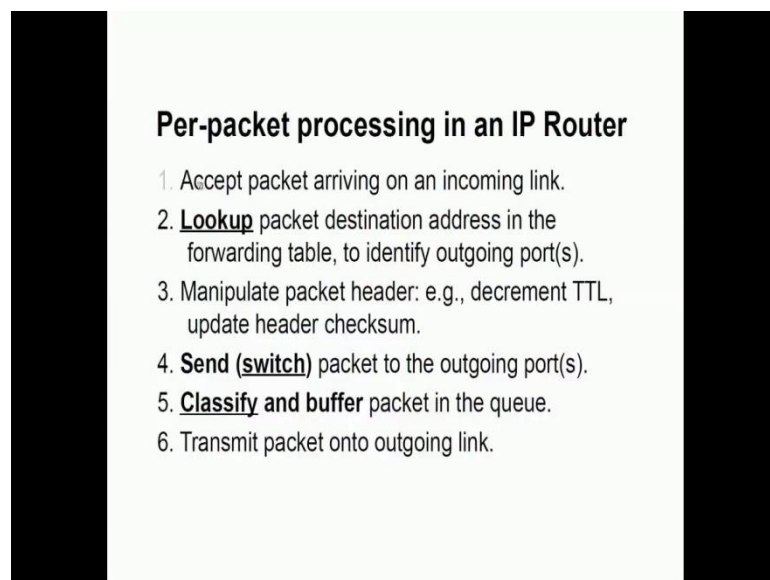
So, in that way they are known as self learning bridges and in order to avoid routing loops, you have to calculate spanning trees in the switching area. So, if you look at this the first thing is in routing protocols you need to have a processor which can do fast computation of routes and then store it in a table. In these places, you need to have circuits which can learn about the MAC addresses and then which can do the spanning tree calculation quickly, to ensure that the package now go into a loop, also these are the two operations that happen at the control plane.

In the data plane, the question is how are each packet processed. So, the first thing that happens is the header lookup and forward to the correct output port. This is true, even with the routing protocol or with switching and one of the things that we have to look at

is how do you manage buffers and bandwidth and these two are essential for quality of service. You should know that the internet has best effort delivery; that means, the data packets need not be;are not,say you cannot reliable get the data packets from one end to the other end.

Let us see how these concepts can be brought in into the network processors and what all the functionalities.Other than this, you have security aspects for example, the data packets can also be encrypted. You need to have some fast encryption and decryption they can happen in the devices.

(Refer Slide Time: 15:13)



Per-packet processing in an IP Router

1. Accept packet arriving on an incoming link.
2. **Lookup** packet destination address in the forwarding table, to identify outgoing port(s).
3. Manipulate packet header: e.g., decrement TTL, update header checksum.
4. **Send (switch)** packet to the outgoing port(s).
5. **Classify and buffer** packet in the queue.
6. Transmit packet onto outgoing link.

This is what happens, accept packet arriving on incoming link or a port, then look up the packet destination address in the forwarding table to identify outgoing ports, manipulate the packet header and then send the packet to the outgoing ports and classify and buffer packet in the queue. It depends on what is the kind of policies you put in and transmit the packet into the outgoing. So, these are the major operations that happen inside a router. Now you have to design a hardware to take care of this.

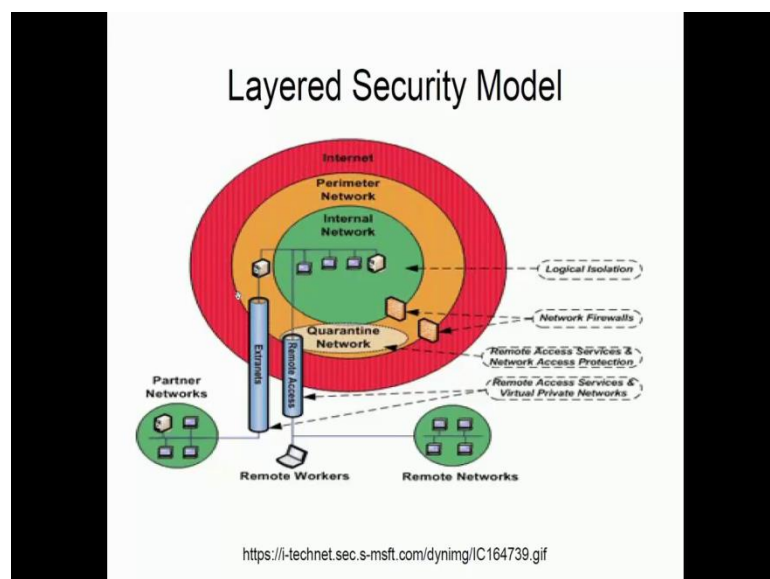
(Refer Slide Time: 15:42)

Network Security

- Defending protocols against attacks
- Defending take over of devices
- Defending packets against attacks
- Defending devices against attacks
- Maintaining QoS under attacks
- ...
- ...
- ...

Now the other part; not only you have to design a hardware take care of this, you also got to protect your devices against attacks. Your protocols have to defend against attacks, you have to define the take over of devices because it is not just designing a processor, the router or the device that uses the processor carries information. So, how are you going to protect that information and then you have to also provide quality of service. You do not want voice calls to drop now and then even try does not like it.

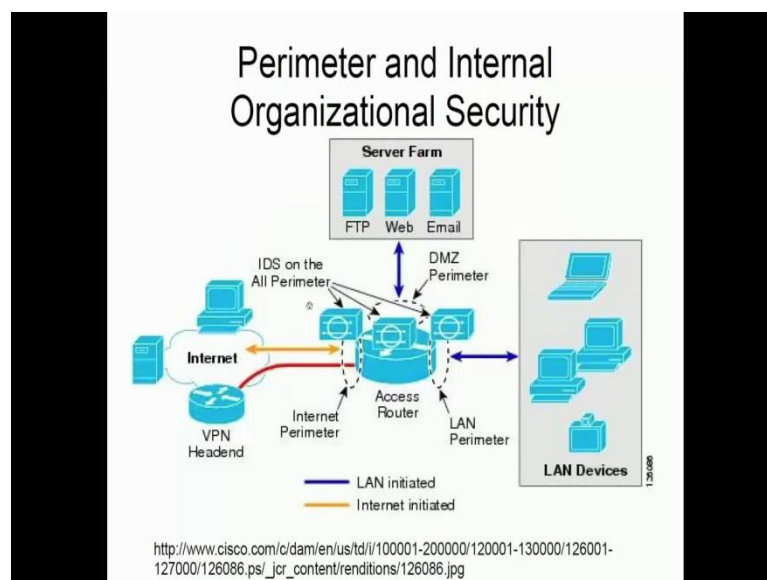
(Refer Slide Time: 16:24)



For this what people have done is, you have a layered model of security. So, the first top you have the internet then you have perimeter security and then you have the internal network security and then you have something known as a quarantine zone or quarantine network or a demilitarized zone, we will see how this is architecture. So, if you look at this you are not going to look at security in isolation, I mean for example, I think in the previous talk you would have talked how to boot securely. Now is that alone enough in a router for example, I mean if I boot securely in a router, in an operating system if I boots securely and then ensure that processor are isolated, yes I provide good amount of security.

But what happens in a router because in a router data packets can come from outside and they can initiate buffer attacks and other things like that or they need not even initiate buffered attacks, what they will do is I will clog a port, just by sending too many data packets. What will you do? You have a secure operating system that is fine you have a secure processor, but if I clog your port, no data is going to get transmitted. So, you have to have mechanisms for preventing these things; also that is very important while considering the router architecture. So, you should have your network processor must be careful of handling these kind of issues.

(Refer Slide Time: 17:55)

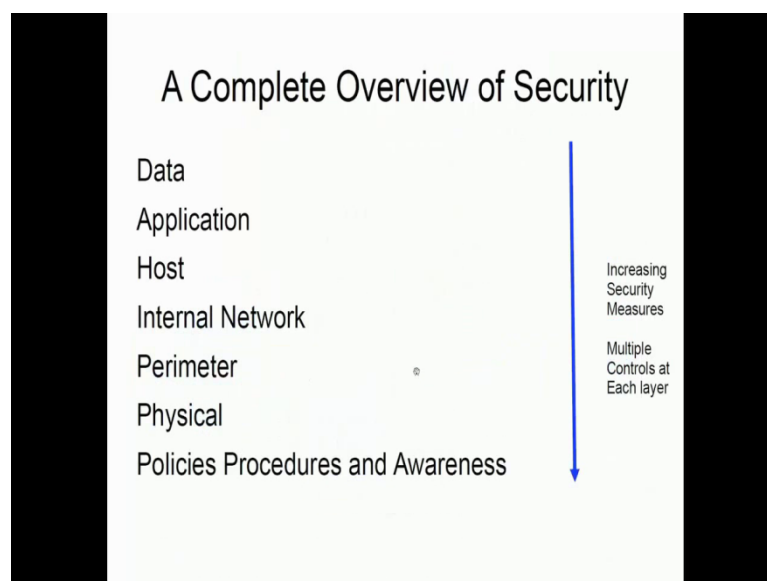


In general, what happens in any organization; how the organizations protect their network? See, for example, this is the LAN devices that are there in the organization and

this is the access router, which connects to the internet, if you look at this. Now what happens is between the; then they have something known as a demilitarized zone, now in this zone this has why it is called DMZ is because this communicates externally and also this has to go to communicate internally. You understand? If I have an email, then I go and login to the email server and this email server using a SMTP protocol has to contact another email server so that it can forward the messages or email that you send. So, this is the layer that people usually attack so that this given higher level of protection, they use something known as intrusion detection systems.

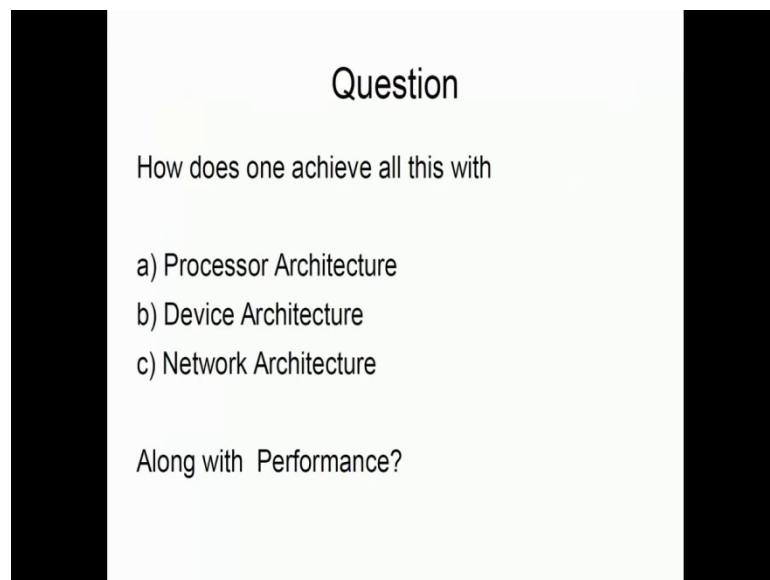
Now these devices also use network processor, so a network processor is not just about sending and receiving data, it is also about those devices, these kind of devices intrusion detection systems, firewalls and all those things using these kind of processor and then what happens is that, then your router should also provide something known as virtual private network because you have a public network and what they actually do is they tunnel the data packets. When you tunnel what happens, you put a header over a header so the header processing time increases, not only that; that increases the size of the packets and if you buffer those packets, remember if you buffer larger size packets and you need more memory; that means, more power consumption. All these things are related so if you look at this, how to I design something which can manage all this.

(Refer Slide Time: 20:04)



This is a complete overview of security, see you are suppose to have data security, you have to have application security, you have to have host security, you have to have internal network security and you have to have perimeter security, you have to have physical security and policies and procedures and awareness and as you go from top to the bottom,it is (Refer Time: 20:23) security measures and multiple controls at each layers.Now one of the things we should understand this policies, procedures and awareness, have a human related factors also,whereas if you go up to this; in this physical security is providing security guards and other things. So, if you look at our network, our devices up to this perimeter,you can have devices which can give you security and many of those devices use networkprocessors.

(Refer Slide Time: 20:55)



The slide is titled "Question" and is framed by two vertical black bars on the left and right sides. The text on the slide is as follows:

Question

How does one achieve all this with

- a) Processor Architecture
- b) Device Architecture
- c) Network Architecture

Along with Performance?

So the question now is, now that we have understood whatthis whole problem is about, the question now is;How does one achieve all this with a processor architecture, a device architecture and network architecture and along with performance.