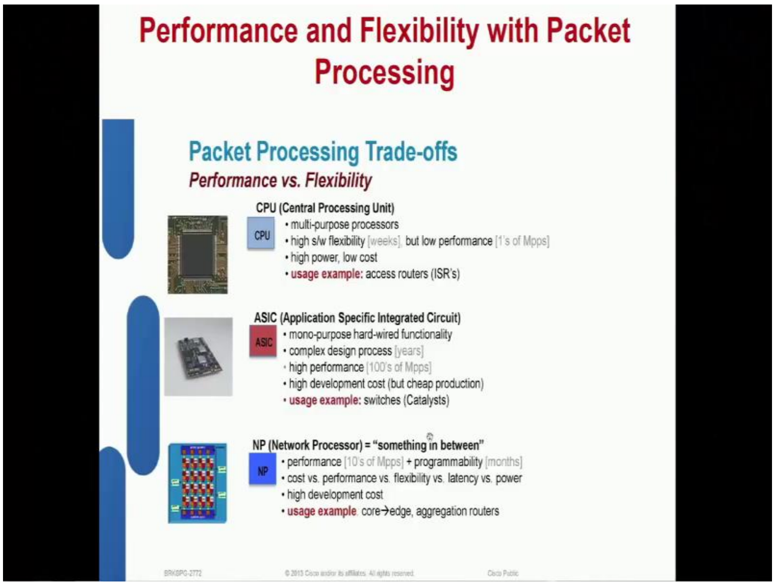
Information Security - II
Prof. V. Kamakoti
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 42
Network Processor Architecture - Week 8

(Refer Slide Time: 00:09)



Performance and Flexibility with Packet Processing

Packet Processing Trade-offs

Performance vs. Flexibility

CPU (Central Processing Unit)

- multi-purpose processors
- high s/w flexibility [weeks], but low performance [1's of Mpps]
- high power, low cost
- usage example: access routers (ISR's)

ASIC (Application Specific Integrated Circuit)

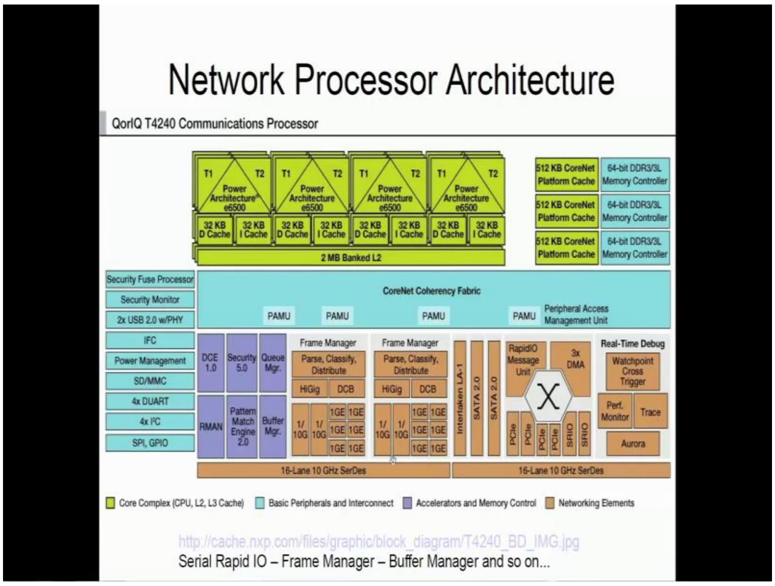
- mono-purpose hard-wired functionality
- complex design process [years]
- high performance [100's of Mpps]
- high development cost (but cheap production)
- usage example: switches (Catalysts)

NP (Network Processor) = "something in between"

- performance [10's of Mpps] + programmability [months]
- cost vs. performance vs. flexibility vs. latency vs. power
- high development cost
- usage example: core→edge, aggregation routers

BRKSPG-2772 © 2013 Cisco and/or its affiliates. All rights reserved. Cisco Public

(Refer Slide Time: 00:10)



Network Processor Architecture

QorIQ T4240 Communications Processor

🟩 Core Complex (CPU, L2, L3 Cache) 🟦 Basic Peripherals and Interconnect 🟪 Accelerators and Memory Control 🟧 Networking Elements

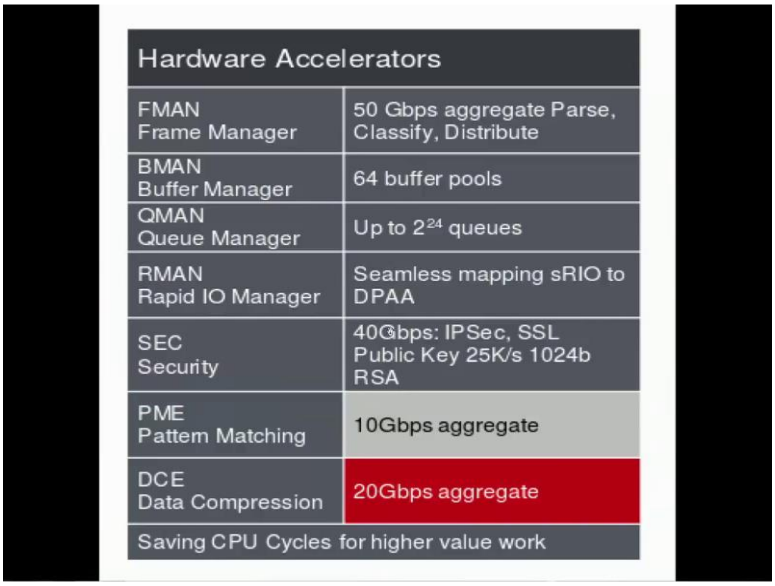
http://cache.nxp.com/files/graphic/block_diagram/T4240_BD_IMG.jpg

Serial Rapid IO – Frame Manager – Buffer Manager and so on...

How does the network processor architecture look like? This we have taken an example of actually 4240, they call it as a Communication Processor. So, whatever we had discussed, you will see some parts of it inside this because what are the architecture seem is we have looking at this network processors inter connected by a switch but what goes inside each network processor is something like this. So, the first functionality that we need is the frame manager. So, when a data packet comes through a 1 gig or a 10 gig port. So, you have to now take this data packet and then look at the frames, parse it, classify the frames and then distribute. If you remember, if the data packet comes in one of these ports and then goes into one of these ports, we told that we need not look into the top level layer.

We look at that architecture in a previous slide. So, we sent through this port alone but if this goes into one of the ports here what happens is that you have take the data put it in some place, say memory or something and then transmit the data packet to this place and that is why you have, these kind of and the second thing that you see in this network process the buffer manager. We call it as a traffic manager in that previous slide. The third thing you have is the queue manager because you can have priority various priorities for queues. So, you have the queue manager here and then you have security engines, this is essentially for encryption and other things and this is separate from your networking part because this is common, if I take the data packets from here it can go into security and then return back. So, this is common to all these things.

(Refer Slide Time: 02:17)



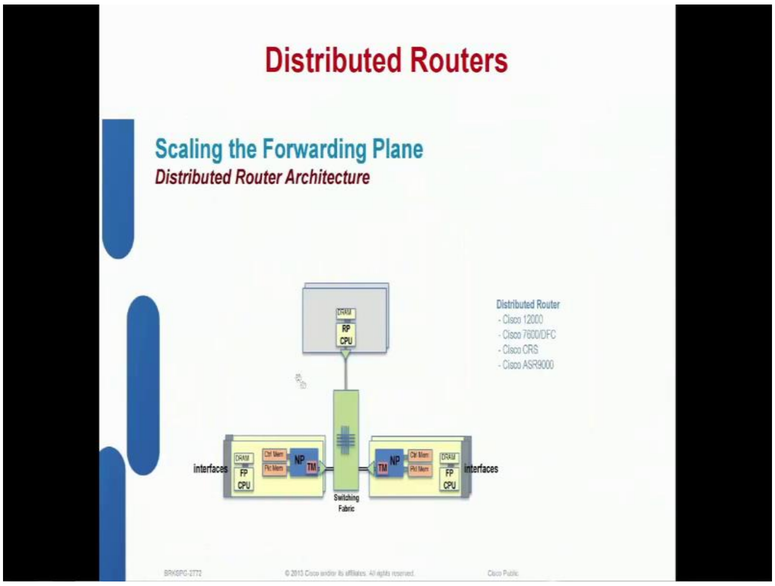
Hardware Accelerators	
FMAN Frame Manager	50 Gbps aggregate Parse, Classify, Distribute
BMAN Buffer Manager	64 buffer pools
QMAN Queue Manager	Up to 2^{24} queues
RMAN Rapid IO Manager	Seamless mapping sRIO to DPAA
SEC Security	40Gbps: IPSec, SSL Public Key 25K/s 1024b RSA
PME Pattern Matching	10Gbps aggregate
DCE Data Compression	20Gbps aggregate
Saving CPU Cycles for higher value work	

Something like this, if you look at this, these are some of the parts of network processor for one, from frame acceleration and all that and then they also have some extra acceleration. Other than this, you have the regular processing stuff, L2 cache, L1 cache and all those things, Power PC architecture and all those things. This is normal what you see in your regular general purpose process. The only thing extra is a kind of a fabric that inter connects these guys together.

Instead of a Bus you might use a Switch. Bus you have contention and all that you can have a 16 cross 16 switch or something to communicate between these guys. Then the rest, you have memory and all those things which are normal and then as I told you, the route processor has all these power management, security, monitor and all those things. The only part that is related to the networking is this, having a frame manager and then pattern match engine that is actually the hardware. So, what they usually do is, instead of using software for parse algorithms and all that, they use this hardware accelerator. You have a Frame Manager, which can go up to 50 gigabits per second and you can parse, classify and distribute it different ports that is the speed that you can get out of this. The second is the Buffer Manager, you have 64 buffer pools, this specific do this processor. If you take Cisco’s router, they manage about 64 k queues and then you have the Queue Manager, here you have up to 22 power 24 queues, even this and then your Rapid IO Manager, essentially the idea is, this queue are these process use network process use something known as data path acceleration architecture. Essentially, the idea behind this is, if I have a data going from one port to another port, I need not root it through the processor or the memory, I can just directly connect these two ports together and then route the data packets, so that is managed by this.

Then you have a Security engine and it operators at 40 gigabits per second. It supports IP Sec, SSL public keys and 1024 bits RSA and then you have Pattern Matching engine, which can operate at around 10 gigabits. All these are hardware rates, if you program it, you may not get this a rast speed and these are rast speed and then finally, Data Compression engine which can work at 20 Gbps. So, the idea here is, if you go back most of the operations that are done by general purpose process are taken over by the these accelerators and they have special hardware for doing these kind of job, that is the major difference between your general purpose processor and a network processor and this is exactly what we saw I mean what goes inside this.

(Refer Slide Time: 05:36)



Distributed Routers

Scaling the Forwarding Plane

Distributed Router Architecture

Distributed Router
- Cisco 12000
- Cisco 7600/DFC
- Cisco CRS
- Cisco ASR9000

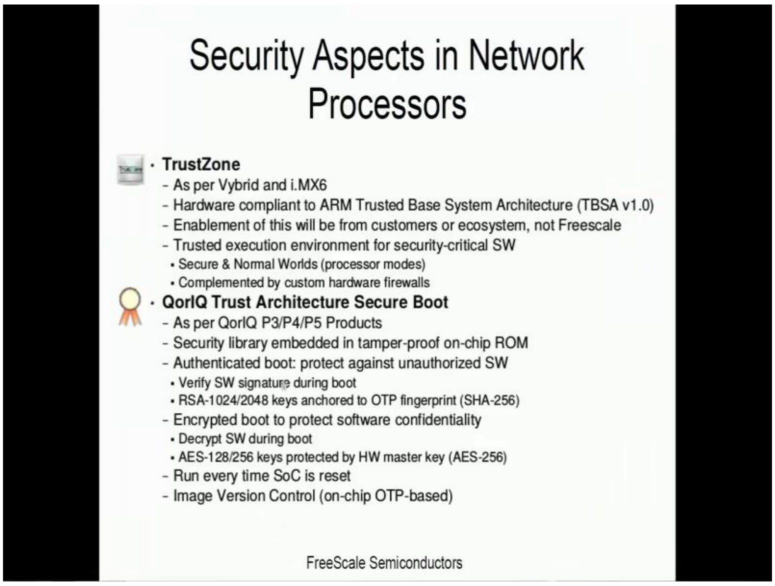
BRKSPG-2772

© 2013 Cisco and/or its affiliates. All rights reserved.

Cisco Public

Now, let us look at security aspects of this network process.

(Refer Slide Time: 05:42)



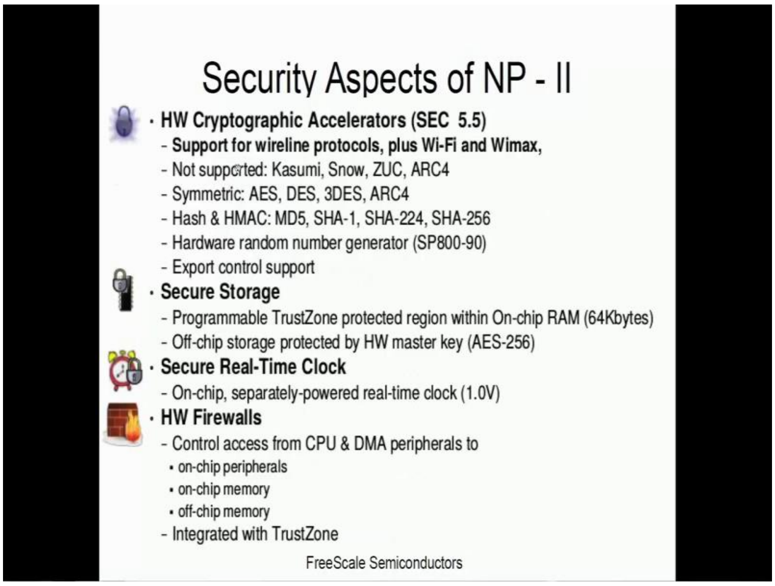
Security Aspects in Network Processors

- **TrustZone**
  - As per Vybrid and i.MX6
  - Hardware compliant to ARM Trusted Base System Architecture (TBSA v1.0)
  - Enablement of this will be from customers or ecosystem, not Freescale
  - Trusted execution environment for security-critical SW
    - Secure & Normal Worlds (processor modes)
    - Complemented by custom hardware firewalls
- **QorIQ Trust Architecture Secure Boot**
  - As per QorIQ P3/P4/P5 Products
  - Security library embedded in tamper-proof on-chip ROM
  - Authenticated boot: protect against unauthorized SW
    - Verify SW signature during boot
    - RSA-1024/2048 keys anchored to OTP fingerprint (SHA-256)
  - Encrypted boot to protect software confidentiality
    - Decrypt SW during boot
    - AES-128/256 keys protected by HW master key (AES-256)
  - Run every time SoC is reset
  - Image Version Control (on-chip OTP-based)

FreeScale Semiconductors

So, Wasan would have talked about TrustZone but it is not applicable to network process. Why TrustZone is not applicable in network process but other than that secure boot feature can be used. So, for secure boot I think high availability, high assurance boot we were discussed it.

(Refer Slide Time: 06:17)



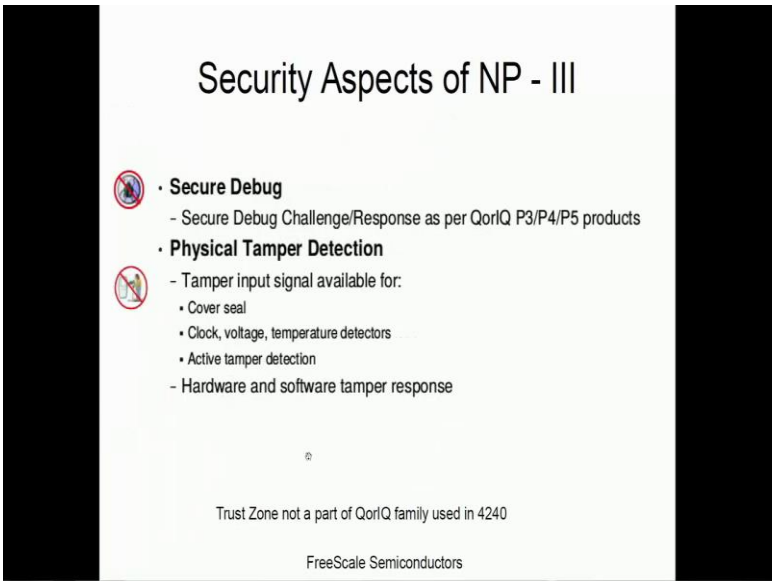
Security Aspects of NP - II

- **HW Cryptographic Accelerators (SEC 5.5)**
  - **Support for wireline protocols, plus Wi-Fi and Wimax,**
  - Not supported: Kasumi, Snow, ZUC, ARC4
  - Symmetric: AES, DES, 3DES, ARC4
  - Hash & HMAC: MD5, SHA-1, SHA-224, SHA-256
  - Hardware random number generator (SP800-90)
  - Export control support
- **Secure Storage**
  - Programmable TrustZone protected region within On-chip RAM (64Kbytes)
  - Off-chip storage protected by HW master key (AES-256)
- **Secure Real-Time Clock**
  - On-chip, separately-powered real-time clock (1.0V)
- **HW Firewalls**
  - Control access from CPU & DMA peripherals to
    - on-chip peripherals
    - on-chip memory
    - off-chip memory
  - Integrated with TrustZone

FreeScale Semiconductors

Then, we discussed Cryptographic Accelerators these are some of the important access. It supports symmetric and asymmetric keys and then hash and SHA and all those things, then a random number generator which is very important for cryptography. You can have Secure Storage, obviously, it is needed to ensure that at least your processor is protected but as I told you there are attacks that can happen outside the processor, how you are protected is to use good network architecture and things like that. One of the things, in any protocols is the real time clock. Many of the protocols actually sink based on clocks. So, you need a real time clock and then they also put some security feature like Firewalls say control access from CPU to DMA and peripherals, that is internal fire lose within the processor.

(Refer Slide Time: 07:18)



Security Aspects of NP - III

- **Secure Debug**
  - Secure Debug Challenge/Response as per QorIQ P3/P4/P5 products
- **Physical Tamper Detection**
  - Tamper input signal available for:
    - Cover seal
    - Clock, voltage, temperature detectors
    - Active tamper detection
  - Hardware and software tamper response

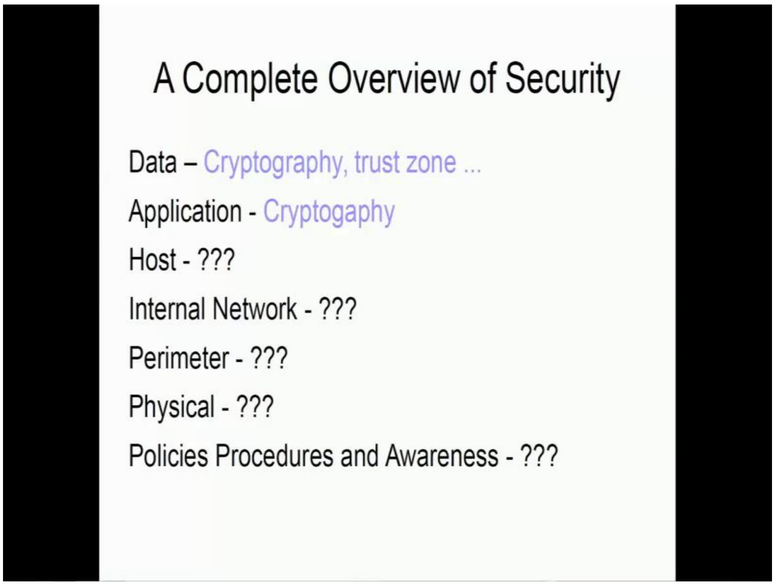
Trust Zone not a part of QorIQ family used in 4240

FreeScale Semiconductors

Then, these are Secure Debug and tamper proof and all that; I think Wasan would have discussed it. Trust zone is not a part of this and we will find out why. This is a overall architecture of a network processor and instruction less stress will correspond to whatever hardware accelerator you are. So, they will supply a bunch of libraries which you have to use to invoke these hardware accelerators.

So, any questions let us break for two minutes and any questions until now. In this section, we actually understood about what is networking and why packet processing is important, why switching is important and then you also look at the growth of the history of network process. Why network process came into existence and then we also looked at a brief architecture of a network process. See there are many companies that make network process, what we gave is one example, Intel actually make some process. Yeah (Refer Time: 08:34) the point is, ASIC essentially performance wise they are expensive, any ASIC will perform much better than a general purpose stuff but only thing is in high speed routers actually they are configured. I will tell you, why ASIC are used only in switching because the point is that when you have to move data from one network processor to another network processor, processors have to process at that speed and the data has to be routed at that speed. We will see that when you come to performance. Any questions from other places, so, if there are no questions we will just proceed. We have seen about network processor architecture. Now, let us come to the important accepts of security.

(Refer Slide Time: 09:39)



A Complete Overview of Security

Data – Cryptography, trust zone ...

Application - Cryptogaphy

Host - ???

Internal Network - ???

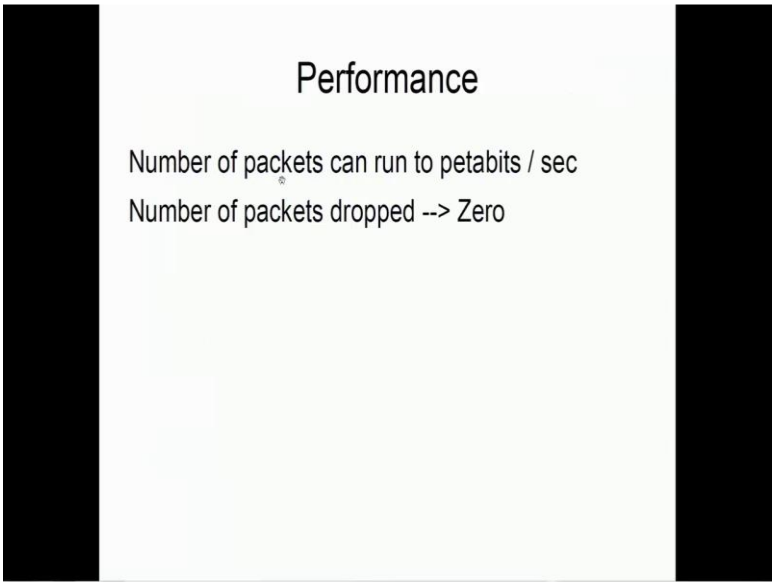
Perimeter - ???

Physical - ???

Policies Procedures and Awareness - ???

We saw that in security there were seven levels of security or layers. The data layer, you can have cryptography, you can have trust zone, you can have secure boot, etcetera, protect the memory and all those things. At the application layer, you have cryptography that is used and then your applications like firewalls and all those things but what is the protection for a host? What is the protection for an internal network? For examples someone clocks your port that means send junk data packets, so that your port to reads and once it reads and drops but then it is reading that is the point. Then, if you connect it as a network, how do you provide perimeter security? How do you provide physical security? How do you provide policies? So, we will not be able to answer all these questions with network process but at least we should be able to answer some of these questions. Now, with security why do we need? Why do we have hardware accelerators? That is because you have to have fast data processing. We will look at performance then will understand why we need separate hardware accelerators for all these things.

(Refer Slide Time: 10:51)



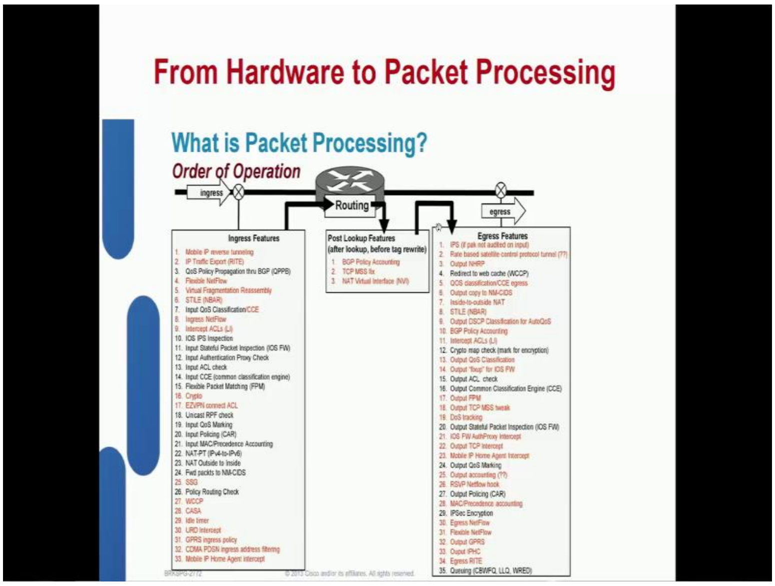
Performance

Number of packets can run to petabits / sec

Number of packets dropped --> Zero

Number of packets that router can get, can go into petabits per second and then number of dropped packets should be more or less zero because in any drop packets it has to be retransmitted by top level protocols and things like that. There are lot of complications in protocols.

(Refer Slide Time: 11:10)



From Hardware to Packet Processing

What is Packet Processing?

Order of Operation

Ingress Features

1. Mobile IP reverse tunneling
2. IP Traffic Export (RITE)
3. QoS Policy Propagation thru BGP (QPPB)
4. Flexible NetFlow
5. Virtual Fragmentation Reassembly
6. STILE (NBAR)
7. Input QoS Classification/CCE
8. Ingress NetFlow
9. Intercept ACLs (LI)
10. IOS IPS Inspection
11. Input Stateful Packet Inspection (IOS FW)
12. Input Authentication Proxy Check
13. Input ACL check
14. Input CCE (common classification engine)
15. Flexible Packet Matching (FPM)
16. Crypto
17. EZVPN connect ACL
18. Unicast RPF check
19. Input QoS Marking
20. Input Policing (CAR)
21. Input MAC/Precedence Accounting
22. NAT-PT (IPv4-to-IPv6)
23. NAT Outside to Inside
24. Fwd packts to NM-CIDS
25. SSG
26. Policy Routing Check
27. WCCP
28. CASA
29. Idle timer
30. URD Intercept
31. GPRS ingress policy
32. CDMA PDSN ingress address filtering
33. Mobile IP Home Agent intercept

Post Lookup Features
(after lookup, before tag rewrite)

1. BGP Policy Accounting
2. TCP MSS fix
3. NAT Virtual Interface (NVI)

Egress Features

1. IPS (if pak not audited on input)
2. Rate based satellite control protocol tunnel (??)
3. Output NHRP
4. Redirect to web cache (WCCP)
5. QOS classification/CCE egress
6. Output copy to NM-CIDS
7. Inside-to-outside NAT
8. STILE (NBAR)
9. Output DSCP Classification for AutoQoS
10. BGP Policy Accounting
11. Intercept ACLs (LI)
12. Crypto map check (mark for encryption)
13. Output QoS Classification
14. Output "fixup" for IOS FW
15. Output ACL check
16. Output Common Classification Engine (CCE)
17. Output FPM
18. Output TCP MSS tweak
19. DoS tracking
20. Output Stateful Packet Inspection (IOS FW)
21. IOS FW AuthProxy Intercept
22. Output TCP intercept
23. Mobile IP Home Agent Intercept
24. Output QoS Marking
25. Output accounting (??)
26. RSVP Netflow hook
27. Output Policing (CAR)
28. MAC/Precedence accounting
29. IPSec Encryption
30. Egress NetFlow
31. Flexible NetFlow
32. Output GPRS
33. Ouput IPHC
34. Egress RITE
35. Queuing (CBWFQ, LLQ, WRED)

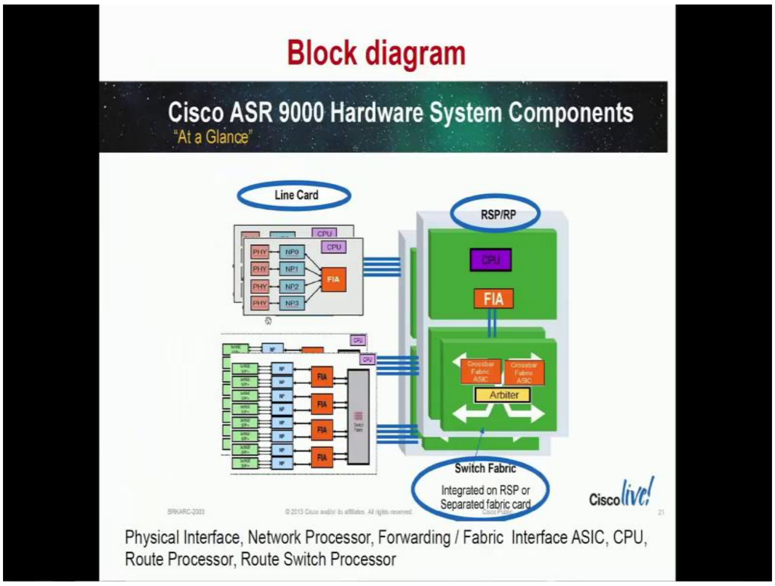
BRKSPG-2772

© 2013 Cisco and/or its affiliates. All rights reserved.

In hardware to packet processing, this is what a router does actually. This on the left hand side you see the bunch of ingress feature that has to be given in a router, that is once a data packet enters to a particular port, these are all some of the things that has to be done. There are about 33 operations they have identified like some of this includes IOS and IPS, packet inspection and then ACL access control list check and so on. There are so many operations that have been done at the input port. Then the process of routing is more or less very easy, it has only three operations.

On the egress you have so many operations. Now, why I cannot do ASIC for this because I need programmability, the first part of it is I need programmability because I have to do so many activities and the protocol keeps changing because protocol is changed by IATF, IATF, if any company goes with the request, they will put a committee and if the committee approves it, they will just change it. Then you need programmability for your processors, if you go with ASIC what is going to happen. That is one of the reasons why they are not going with the ASIC; they go with network process because this operations can be programmed.

(Refer Slide Time: 12:32)



Block diagram

Cisco ASR 9000 Hardware System Components

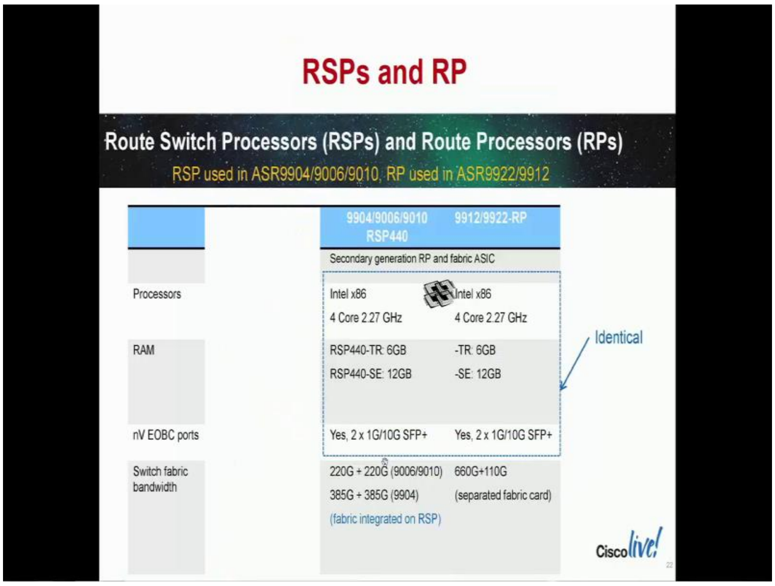
"At a Glance"

Physical Interface, Network Processor, Forwarding / Fabric Interface ASIC, CPU, Route Processor, Route Switch Processor

Let us look at this hardware. We had seen how the router designs happen. If you look at the real hardware, high speed router ASR 9000, which we saw, these are all the network processors, the blue color ones are the network process and these are connected to the ports, these are all the ports. So, each processor can manage many ports. Look at this. This at least has three lines in this case. Similarly, each one of this is attached to a fabric interface ASIC. As I told you, this part of it is exchanging data from, so that you can move the data packets from this network processor and then go into some operations and then go it back into another port.

In this case, if you look at this, a data packet will come via this port then it is processed by a network processor. Then it goes in to a fabric interface ASIC, then it goes into the arbiter or whatever it is. It makes a routing decision then it again comes via these packets. It has to go back in this direction. So, if you look at this, the amount of data that comes in, let us assume that even one of this is 10 gig ports, suppose I have four ports connected together, then the total is 40 gig and you always design for maximum performance. So, 40 gigs going into a FIA and 40 gigs also coming into this port then switching has to happen at that speed and then the data packet has to be travelled to the components that include here. So, here you have a route processor or this is also known as a route switch processor, which is a general purpose CPU and then here as the network process and then here is the ASIC, which is the cross bar switch. Sometimes, they use cross bar sometimes they use a banyan network and so on. There are many technologies for these switches.

(Refer Slide Time: 14:37)



RSPs and RP

Route Switch Processors (RSPs) and Route Processors (RPs)

RSP used in ASR9904/9006/9010, RP used in ASR9922/9912

	9904/9006/9010 RSP440	9912/9922-RP
	Secondary generation RP and fabric ASIC	
Processors	Intel x86 4 Core 2.27 GHz	Intel x86 4 Core 2.27 GHz
RAM	RSP440-TR: 6GB RSP440-SE: 12GB	-TR: 6GB -SE: 12GB
nV EOBC ports	Yes, 2 x 1G/10G SFP+	Yes, 2 x 1G/10G SFP+
Switch fabric bandwidth	220G + 220G (9006/9010) 385G + 385G (9904) (fabric integrated on RSP)	660G+110G (separated fabric card)

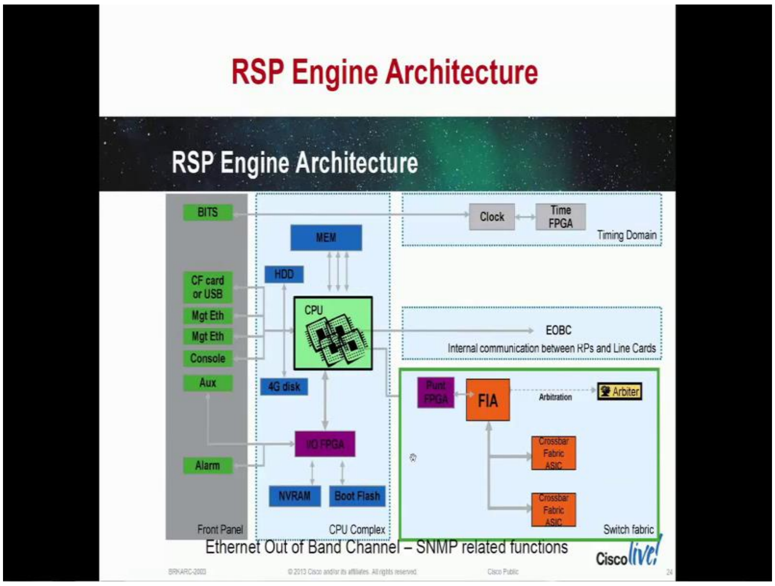
Identical

Cisco live!

22

Now, usually this is Route Switch Processor, you can have a general purpose processor. Usually, x86 4 core 2.27 is actually used in 9000 process, which is actually normal that you find in your server boots but one of the things you should see is the switch fabric bandwidth, that is runs into 220 gig and so on. So, this is all data from field data not theoretical data.

(Refer Slide Time: 15:10)



RSP Engine Architecture

RSP Engine Architecture

Ethernet Out of Band Channel – SNMP related functions

Cisco live!

BRKARC-2003

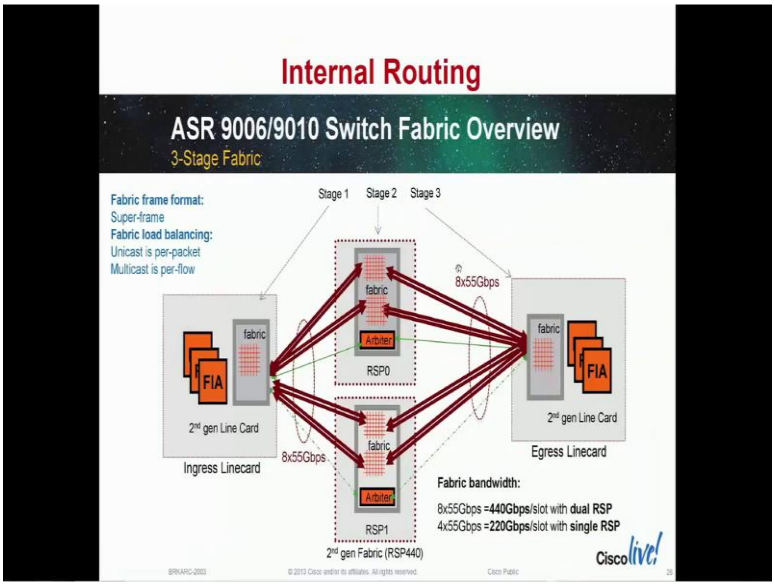
© 2013 Cisco and/or its affiliates. All rights reserved.

Cisco Public

24

Now, Route Switch Processor how does it look at like. So, even here you can have more than one CPU because of the data speeds you can have more than one CPU. Then these are all regular CPU complex whatever the most important thing is the timing and then they use for internally communicating. Here, they use something known as Ethernet out of band channel for communicating here and then you have fabric interface ASIC, orbit ratio and connection. So, this is the route switch processor, this is the general ASIC.

(Refer Slide Time: 15:52)



Internal Routing

ASR 9006/9010 Switch Fabric Overview

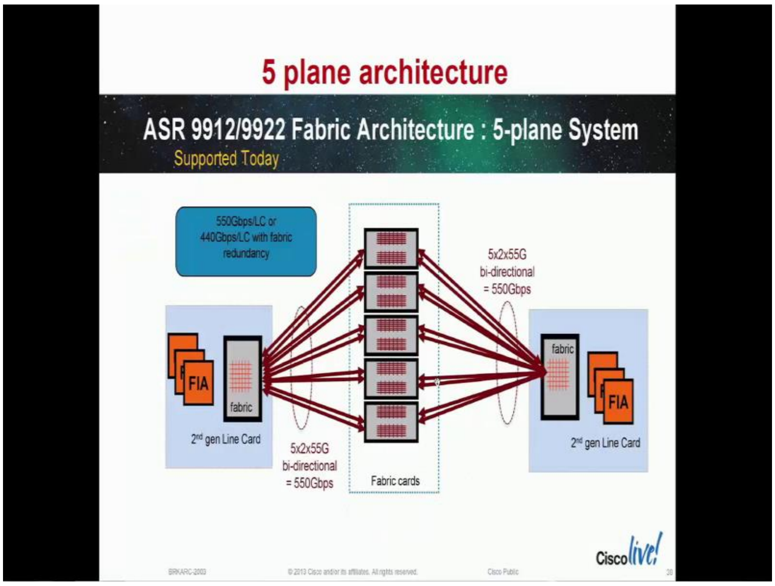
3-Stage Fabric

Fabric frame format:
Super-frame
Fabric load balancing:
Unicast is per-packet
Multicast is per-flow

Fabric bandwidth:
8x55Gbps =**440Gbps**/slot with **dual RSP**
4x55Gbps =**220Gbps**/slot with **single RSP**

Now, what happens to the Switching Fabric? If you look at this, the data comes from a Ingress Linecard. Remember; once it enters Ingress Linecard then there are 30 operations that I showed you that has to be done by the network processor. After it is done then it is sent to ASIC, now this is where I use the cross bar switch just for performance and that is why these routers are pretty expensive. For example, one of the routers can go up to 12 linecards and the linecards can each have minimum. Even if you consider 16 ports per linecard operating at 1 giga hertz 1 giga bit per second then you can calculate it 1 into 16 into 12 at the speed and this has to switch at that speed. So, what happens here is they have something known as a route switch processor. So, if you look at the fabric bandwidth, if you look at this is. This is approximate numbers that they are given 8 into 55 giga bits per second. So, per slot it is 440 giga bits per second that is a kind of switching speed that you need and remember all the switching speeds are based on the clock frequency and clock frequency proportional to power. So, that is where it takes lot of power. In fact, some of these high end routers take about 2 kilowatts of power. So, if you look at this here, it is 8 into 55 Gbps that get switched and then the output also should be at 8 into 55 Gbps. This is one architecture of a router.

(Refer Slide Time: 17:42)



5 plane architecture

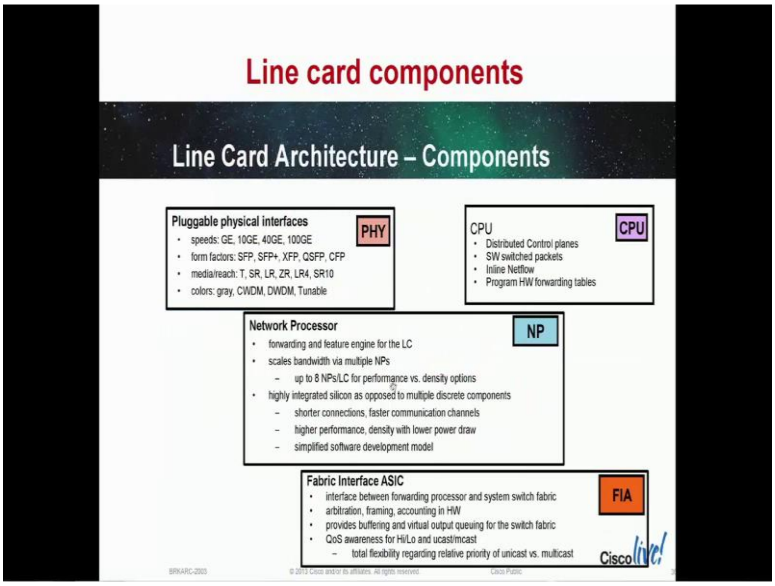
ASR 9912/9922 Fabric Architecture : 5-plane System

Supported Today

550Gbps/LC or 440Gbps/LC with fabric redundancy

Here is the other architecture where you have five bands. So, for bidirectional it carries up to 550 Gbps. So, that is why this is supported today, this is slightly old slide, it supported two years back now this has increased. They have seven layers and all that this is only five layer switching interface.

(Refer Slide Time: 18:06)



Line card components

Line Card Architecture – Components

Pluggable physical interfaces PHY

- speeds: GE, 10GE, 40GE, 100GE
- form factors: SFP, SFP+, XFP, QSFP, CFP
- media/reach: T, SR, LR, ZR, LR4, SR10
- colors: gray, CWDM, DWDM, Tunable

CPU CPU

- Distributed Control planes
- SW switched packets
- Inline Netflow
- Program HW forwarding tables

Network Processor NP

- forwarding and feature engine for the LC
- scales bandwidth via multiple NPs
  - up to 8 NPs/LC for performance vs. density options
- highly integrated silicon as opposed to multiple discrete components
  - shorter connections, faster communication channels
  - higher performance, density with lower power draw
  - simplified software development model

Fabric Interface ASIC FIA

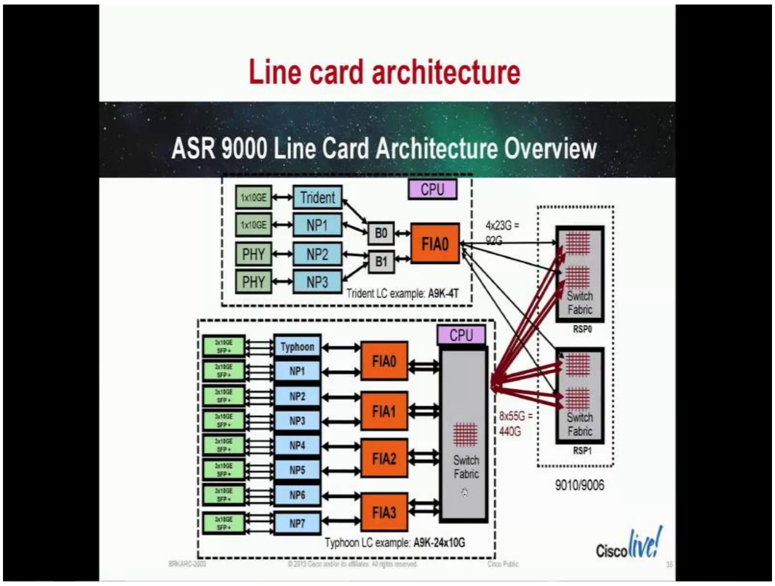
- interface between forwarding processor and system switch fabric
- arbitration, framing, accounting in HW
- provides buffering and virtual output queuing for the switch fabric
- QoS awareness for Hi/Lo and ucast/mcast
  - total flexibility regarding relative priority of unicast vs. multicast

Cisco live!

BRKARC-2003 © 2013 Cisco and/or its affiliates. All rights reserved. Cisco Public

Now, this is the component, the linecard architecture. Each linecard that we are talking about, it has got physically interfaces and it can go up to 100 giga bites speed and then the CPU can be used for control plane and then control plane operations and then the network process essentially uses a forward and feature engine. So, this is highly integrated silicon as opposed to multiple discrete components, it is all done in it, it is a core. Let us call it as a core and then the fabric interface ASIC, which actually forms the interface between this network process and the CPU. So, this is the overall configuration of a router for performance.

(Refer Slide Time: 18:56)

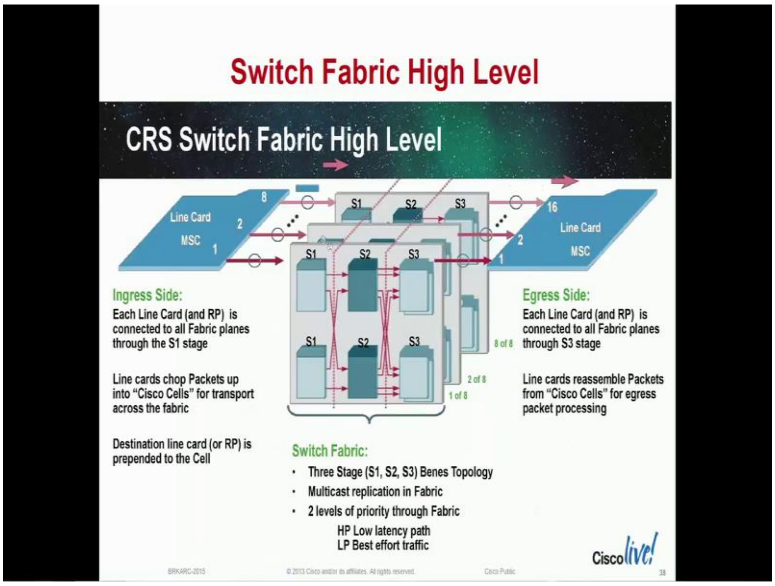


Line card architecture

ASR 9000 Line Card Architecture Overview

Here is ASR 9000 router; here is an example of how they are all interconnected. If you look at this case for example, this is a normal CPU. So, here it has 92 gig interface, where as with the linecard and other phase it is got 440 gig interface.

(Refer Slide Time: 19:22)



Switch Fabric High Level

CRS Switch Fabric High Level

Ingress Side:

Each Line Card (and RP) is connected to all Fabric planes through the S1 stage

Line cards chop Packets up into "Cisco Cells" for transport across the fabric

Destination line card (or RP) is prepended to the Cell

Egress Side:

Each Line Card (and RP) is connected to all Fabric planes through S3 stage

Line cards reassemble Packets from "Cisco Cells" for egress packet processing

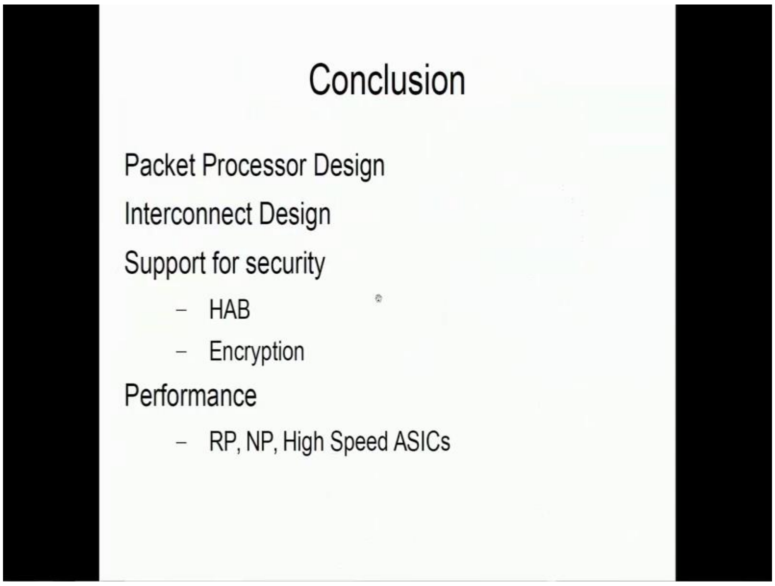
Switch Fabric:

- Three Stage (S1, S2, S3) Benes Topology
- Multicast replication in Fabric
- 2 levels of priority through Fabric

  HP Low latency path
  LP Best effort traffic

In general, this architecture router is high speed router, architecture is linecard has a route processor and this connected to see that switches can also be of different levels. We saw seven layers switches and you can have linecards of seven layer switches that is a current CRS architecture. This is a latest architecture of Cisco, this is how it is. So, essentially the idea is the back end or the back plane has more switching elements and that increases the speed and the ingress side you have so much of processing to be done. On the outgress side, you have bunch of processing to be done and these are connected via these kind of switching interface. Now, the current trend is that you put a memory, the CPU, the NPU together and they act as small cells and all these cells are interconnected via this high speed switches, so that each network processor itself can manage more number of packets and that is why you get increase in speed. So, the architecture was actually very simple.

(Refer Slide Time: 20:38)



Conclusion

Packet Processor Design

Interconnect Design

Support for security

- HAB
- Encryption

Performance

- RP, NP, High Speed ASICs

So, one we looked at the packet processor design, we saw that both for routing and switching you have to take the pro, the packet inside, do certain operations then do a forwarding and then send it to other packets and this is the basic operation in any router or a switch and the most important aspect of this is and we saw the history where we found out that from a general purpose CPU, how we moved into a network process and then we found out that the interconnect design was very important and because of this and they moved into ASIC, they did not want to design network processor in ASIC because the protocols changed the way you process and because of that if you go for ASIC then you have to replace every time the protocol or the processor changes. Therefore, they just went for interconnect design alone with the ASIC and this was also good because you had to have that much speed for switching between one linecard to another linecard, whatever packets you are getting other than this. You have to have support this security.

So, the network process by them supported lot of encryption and they had accelerators for supporting encryption and other operations. We saw that there are different kinds of operations for frame handling and all that, then for security in network operating systems you have a high availability boot, high available boot and all those things and then as far as performance is concerned, you have to have route process network process and high speed ASIC, which can increase the performance. So, as far as processor architecture networks are concerned it uses massive parallelism and pipelining.

Why pipelining because the headers have to be removed one by one. You first look at the outer header and then look at the inner header and so on. So, that can be sent through a pipeline again you build the headers in the same way so that can be looked at as a pipeline operations since there are many packets coming many ports that can be looked at as a parallel operation and your process much provide ability to handle this kind of switches. So, I stop here, this is just an introductory part, there are lot of details and how these switches are designed and all those things but then those are all not needed in this current course. So, the most important aspect is now security part of it. We see only one part like giving encryption alone is one that is provided by the hardware, the rest of the security parts has to come via coding and then better network design and so on. So, with that I stop this lecture and any questions I will be happy to answer.

Student: (Refer Time: 23:16)

Professor: Yes. Physical tempering can be done but then there are methods to manage. See, mostly networking the problem is not physical tempering, it is the data that is going out that is getting captured and then attacking the box such that it cannot perform any operation like DOS attacks, delay of service attacks because network box it does not provide the service that is intended to provide and what is a point in having a box. So, most of the attacks happen only after they penetrate a network, they penetrate machine inside an organization. Let us be clear.

What is important is the security of the network and how to ensure that your device does not get compromised. If you have most of these things in ASIC, obviously, no one can program it. So, they can just only send data packets to it and then ensure that device does it. So, the major factor here is denial of service and other attacks. All the other attacks for example, buffer flow and over flow and all that occur at the application level. Once they find out that your application has weakness then they attack it. So, from a network point of view, from a network processor point of view, it is not much you can do with security. You always trust the data packet and send it. For example, if someone encrypts a data packet which has a worm, as far as the router is concerned it tamper packet that it has to pass through, unless you put some other mechanism like firewall and things like that which will poke into the packet, they call it as deep packet inspection and all those things Any how thanks for participating in this session on network process security and performance. I hope it was useful and thanks for participation. Bye.