

Name : Manoj Kumar Panguluru

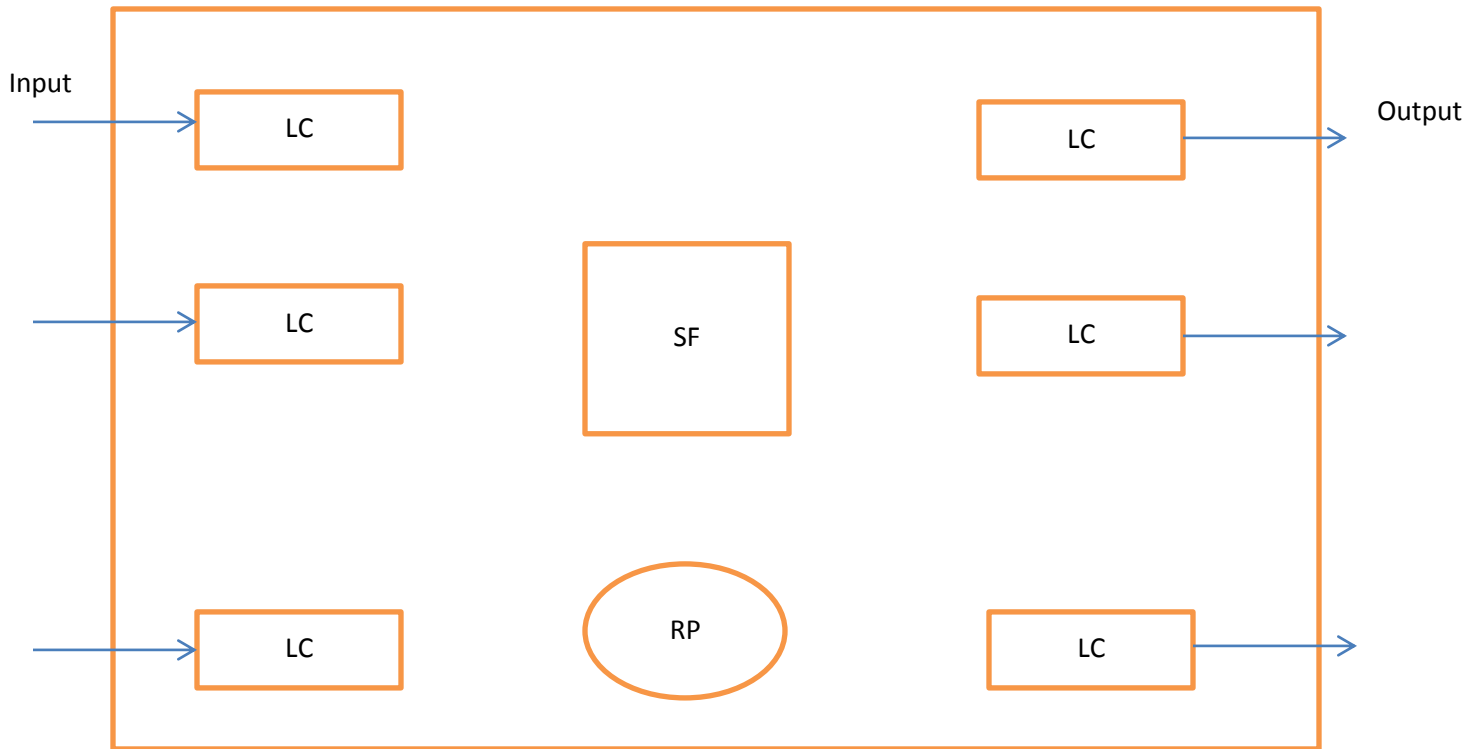
Lecture Date : 8/22/2012

General Architecture of Router:

LC : Line Card

SF : Switching Fabric

RP: Route Processor

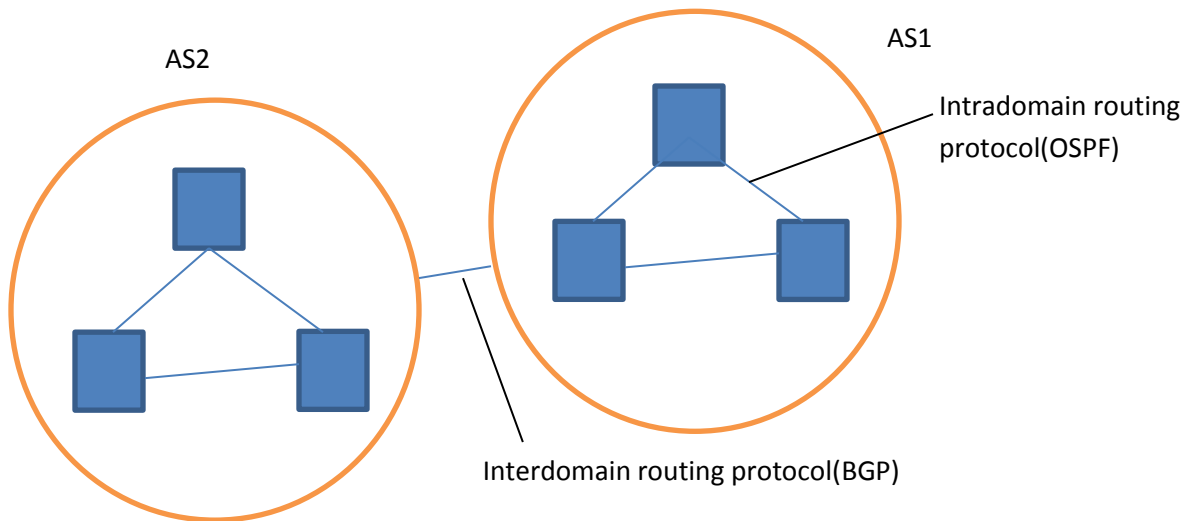


Line Card performs both the input and output functionalities.

Every router has one more Route Processors. The basic functionality of RP is perform routing using different routing protocols. For example: Routing across domains is done via BGP. Intradomain routing is done using OSPF/RIP.

Basics of Internet Routing:

Internet consists of many autonomous systems. Each domain can administer its own routing protocol (intradomain routing).



Only selective routers perform BGP.

Output of the routing process is stored in the Forward Information Base.

IP Prefix	Output Port
1010*	1
10*	2
0*	3
11*	4

Ex: If Destination IP is of the form 1011... then output port = 1

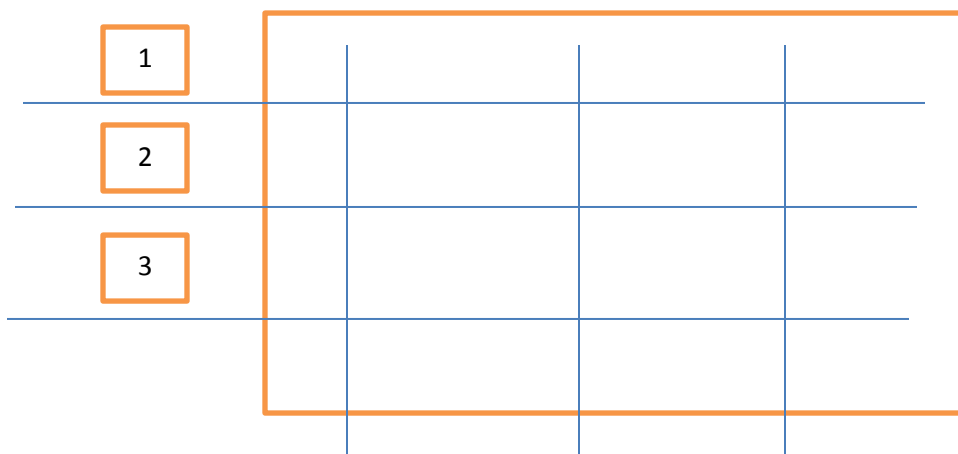
Destination IP = 1000... then output port =2

If there are multiple matches then the longest prefix match is taken as the output.

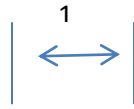
Matching is done in the input Line card using IPLookup(which uses longest prefix match)

Switching Fabric:

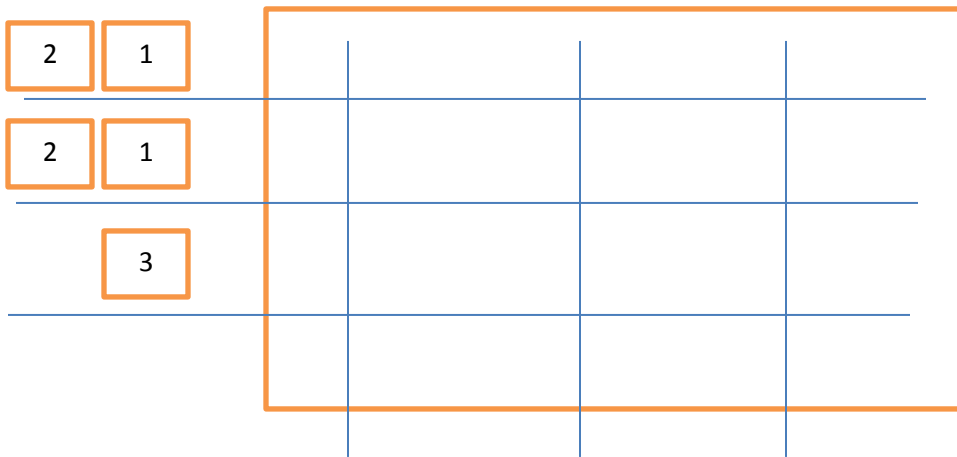
This decides how to switch the packets across the input and the output ports.



Here the interconnect is programmable. Also it has synchronous circuitry.



At time t the packets are in input LC. At time $t+1$ the packets are in output LC. The interconnect is enabled during the cycle. The connection pattern keeps on changing every cycle as it depends on the input and hence the switch configuration must be computed for each cycle. This computation is a very challenging problem. Naïve implementation will have very bad throughput. Goal is to achieve 100% but in a naïve switch only 58.6% is achieved(as per proved concepts).



In the above example if one could notice only one packet would go through in naïve implementation.

Input Queuing (All packets are queued in I/p port and the order of the packets cannot be changed (FIFO)). This leads to head of line blocking. If we assume uniform steady traffic model the steady state throughput = $2/\sqrt{2}$ which is equivalent to 58.6%

Better implementation might involve reversing the order of the packets so as to achieve better/higher throughput. However it has some downsides. For smaller switches all possible permutations can be looked but for bigger switches it is not feasible.

Packet Classification:

Firewall does packet classification. However the forwarding depends on number of factors like Source IP, Source port, Destination IP, Destination Port, Protocol etc. Involving lot of factors makes it harder to perform the classification.

Measurement Techniques:

Easy to do it in low speeds (using Hash table) but need better data structure for high speeds. Sampling, Streaming/Sketching are better ways of doing it in high speeds.

Security Mechanism:[Not only firewall]

IPTraceback is one example of a security mechanism. This is very useful to find the source of the attack in the case of a DDOS (Distributed denial of Service) attack. Modern routers place fingerprints in the unused fields of the header and after collecting significant fingerprint one can get the path of the attacker.