Routers

Main functions of a router:
- Computing routing tables (RIP, OSPF, BGP)
- Accepting/Forwarding packets

Workstation Based:
- Aggregate bandwidth
  - \( \frac{1}{2} \) of the i/o bus bandwidth
  - Capacity shared among all hosts connected to switch example: 800Mbps bus can support 8 T3 ports
- Packets-per-second
  - Must be able to switch small packets
  - 100,000 packets-per-second is achievable
  - E.g., 64-byte packets implies 51.2Mbps
  - Now a days have very fast i/o buses

Switching Hardware
- Switching Hardware
  - Design Goals
    - Throughput (depends on traffic model)
    - Scalability (a function of n)
  - Ports
    - Circuit management (e.g., maps VCLs, route diagrams)
    - Buffering (input and/or output)
  - Fabric
    - As simple as possible
    - Sometimes do buffering (internal)
    - Connects input ports to output ports

Router Architecture
- Two key router functions:
  - Run routing algorithms/protocol (RIP, OSPF, BGP)
  - Accepting/Forwarding packets
Switching datagrams from incoming to outgoing link

- Input ports
  - Structure
    - Line termination
    - Data link processing
    - Lookup forwarding/queueing
  - Transmission
    - Fabric slower than input ports combined -> queuing may occur at input queues
    - Head of the line (HOL) blocking: queued datagram at front of queue prevents others in queue from moving forward
    - Queuing delay and loss due to input buffer overflow
    - If 1 is queued for 1 and 3 is queued for 1, 3’s other packets still have to wait, this is called head of line blocking.

- Output ports
  - Structure
    - Queueing
    - Data Link
    - Line Termination
  - Transmission
    - Buffering is required when datagrams arrive from fabric faster than the transmission rate
    - Scheduling discipline chooses among queued datagrams for transmission
    - Buffering when arrival rate via switch exceeds output

Types of Switching Fabrics

There are three types of switching fabrics:

1. Via Memory
   a. First gen routers:
      i. Packet copied by system’s (single) cpu
      ii. Speed limited by memory bandwidth

2. Via a Bus
   a. Datagram from input port memory to output port memory via a shared bus
   b. Bus contention: switching speed limited by bus bandwidth

3. Via an Interconnection Network
   a. Modern day - much faster
   b. Overcome bus bandwidth limitations

Types of Interconnection Networks

1. Crossbar Switch
a. Every input port is connected to every output port

2. Knockout Switch
   a. Handles if multiple packets are going to the same output port

3. Self-Routing Fabrics
   a. Banyan Network
      i. Constructed from simple 2x2 switching elements
      ii. Self routing head attached to each packets
      iii. Elements arranged to route based on this header
      iv. No collisions if input packets sorted into ascending order
      v. Complexity: nlog(2)n
   b. Batcher Network
      i. Switching elements sort 2 numbers
      ii. some elements sort into ascending (clear)
      iii. some elements sort into descending (shaded)
      iv. Elements arranged to implement merge sort
      v. Complexity nlog(2)n

IPv6

- Improves on IPv4
  - 128-bit addresses (instead of 32-bit)
    - 32-bit address space completely allocated by 2008
  - Header format helps speed processing/forwarding
  - Header changes to facilitate QoS
  - New anycast address: route to “best” of several replicated servers
- Features
  - Classless addressing
  - Multicast
  - Real-time service
  - Authentication and security
  - Auto-configuration (like DHCP)
  - End-to-end fragmentation (only in end)
  - Enhanced routing functionality, including support for mobile hosts
  - Biggest feature is security and authentication
- Notation: x:x:x:x:x:x:x (where “x” represents a 16-bit hex number)
  - Contiguous 0s are compressed
  - 47CD::A456:0124
  - IPv6 compatible IPv4 address: ::128.42.1.87
- Header
  - 40-byte base header
  - Extension headers (fixed order, mostly fixed length)
    - Fragmentation
Source routing
- Authentication and security
- Other options
  - Priority: identify priority among datagrams in flow
  - Flow label: identify datagrams in same “flow”
    - Not defined yet
  - Next header: identify upper layer protocol for data
- Dual-stack approach
  - Flow is lost
- Tunnel
  - Transmit IPv6 packets, encapsulating them in IPv4 packets
  - No flow is lost

**IPSec**

IPSec is part of the IPv6 specification, and implements network layer encryption and authentication, providing an end-to-end security solution in the network architecture itself. It provides confidentiality, integrity and authenticity of IP datagrams.

- End systems and applications do not need any changes
- Encrypted packets look like ordinary IP packets and can be easily routed through any IP network

**Technologies:**

- Adds only a few bytes to each packet
- Diffie-Hellman key exchange
- Public-key crypto for signing
- Bulk encryption
  - DES, 3DES, Blowfish, IDEA, RC4, AES etc.
- Message digest algorithms for ensuring authenticity
- Digital certificates for authentication

**Transport Modes of operation:**

- Allows devices to see the source and destination addresses
  - Enables intermediate routers to provide special services based on IP header
    - Allows attacker to perform certain traffic analysis based on this information
- If the entire IP datagram is encrypted, including the IP headers:
  - Source and dest address are also hidden
  - Prevents traffic analysis by attacker
- Used in VPNs

**Security Associations (SA):**

- Specifies: which algorithms have been used, keys, etc.
- Three parameters:
  - Security Parameters Index (SPI)
- IP Destination Address
- Security Protocol Identifier

### Authentication Header:
- Used to ensure the authenticity of the data
  - Provides support for data integrity and authentication of IP packets
- Data includes the entire IP payload including transport layer headers and also the invariant data in the IP header (like source address, destination address etc)

### Encapsulating Security Payload:
- Used to ensure confidentiality, integrity, and authenticity of data

### Key Management:
- Typically need 2 pairs of keys:
  - For AH & ESP
- Manual key management
  - System administrator manually configures every system
- Automated key management
  - For on demand creation of keys for SAs

#### Internet Key Management Protocol (IKMP/ISAKMP):
- First created authenticated secure tunnel between 2 entities and then negotiates the security association for IPSec over this tunnel.
- Internet Key Exchange (IKE), two-step process:
  - Authentication of peers
    - Using preshared keys
    - Using public key cryptography
    - Using digital signatures and public key certificates
      - Ensures non-repudiation
  - Key exchange to generate secure tunnel