Gateway and Routing

Indian Computer Emergency Response Team
Department of Information Technology
Ministry of Communications & Information Technology
New Delhi

Ruchi Gola
ruchi@cert-in.org.in

Agenda

- **Routing Definition**
- **OSI Reference Model: Pre-requisite in understanding Routing**
- **Information required for routing**
- **Routers and security**
- **Security Policy for Router**

  Checklist against Physical Security Aspect for Router security Policy
  Static Configuration Security Aspect
  Dynamic Configuration Security Aspect
  Network security aspect of Router Security Policy

Routing

- A definition of routing as provided by Cisco Systems Inc.:

“Is the act of moving information across an internetwork from source to destination”.

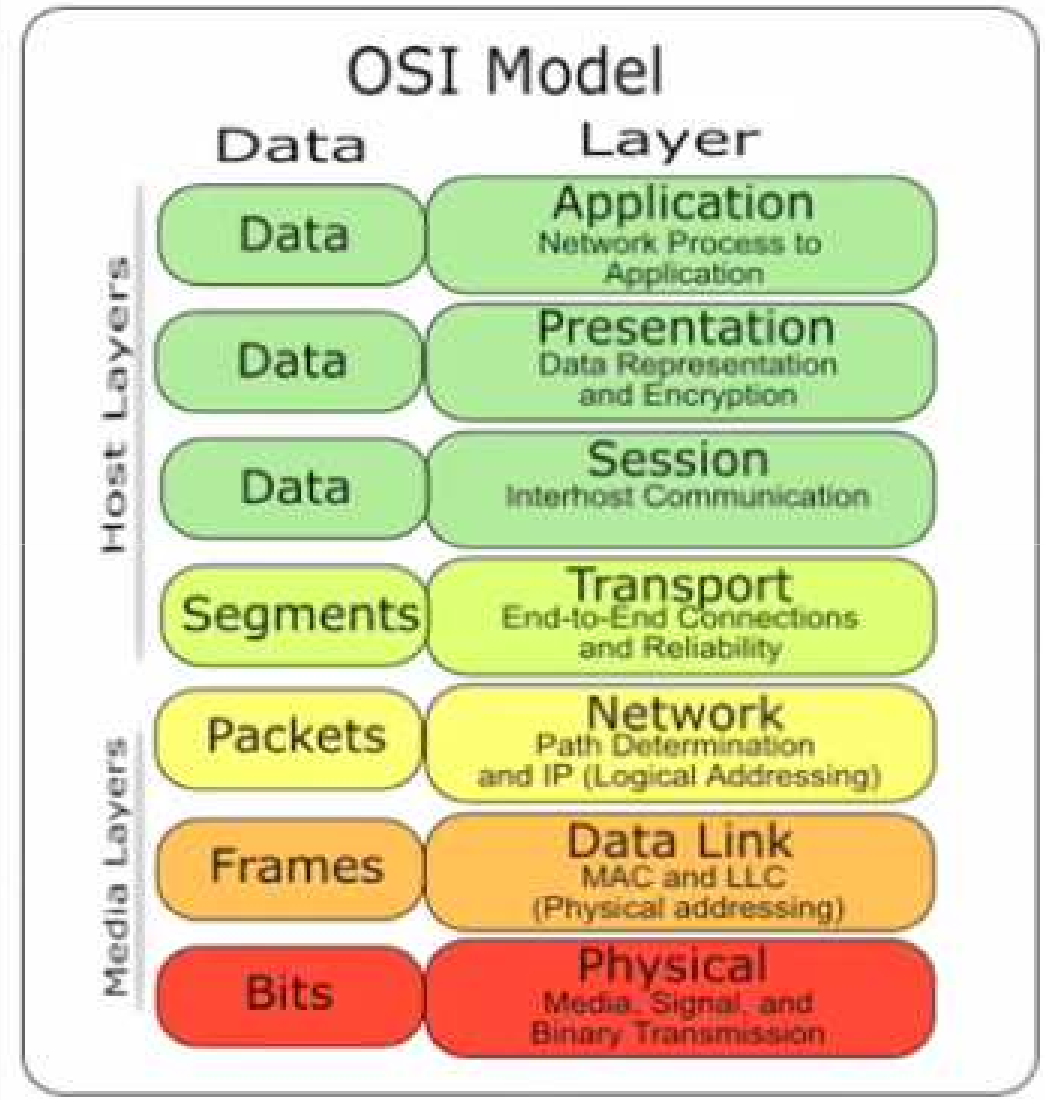
The key term in this definition is “internetwork”.

This term implies that there is a least one routing

device between the source and the destination

This device in its simplistic form is actually a ROUTER(also called gateways or IP forwarders)

OSI Reference Model: Pre-requisite in understanding Routing



- Network Layer, layer 3 is the layer where the functionality of routing is added to the data packets. outers operate here.

- The Network Layer handles interaction with the network address scheme and connectivity over multiple network segments. It describes how systems on different network segments find and communicate with each other“.

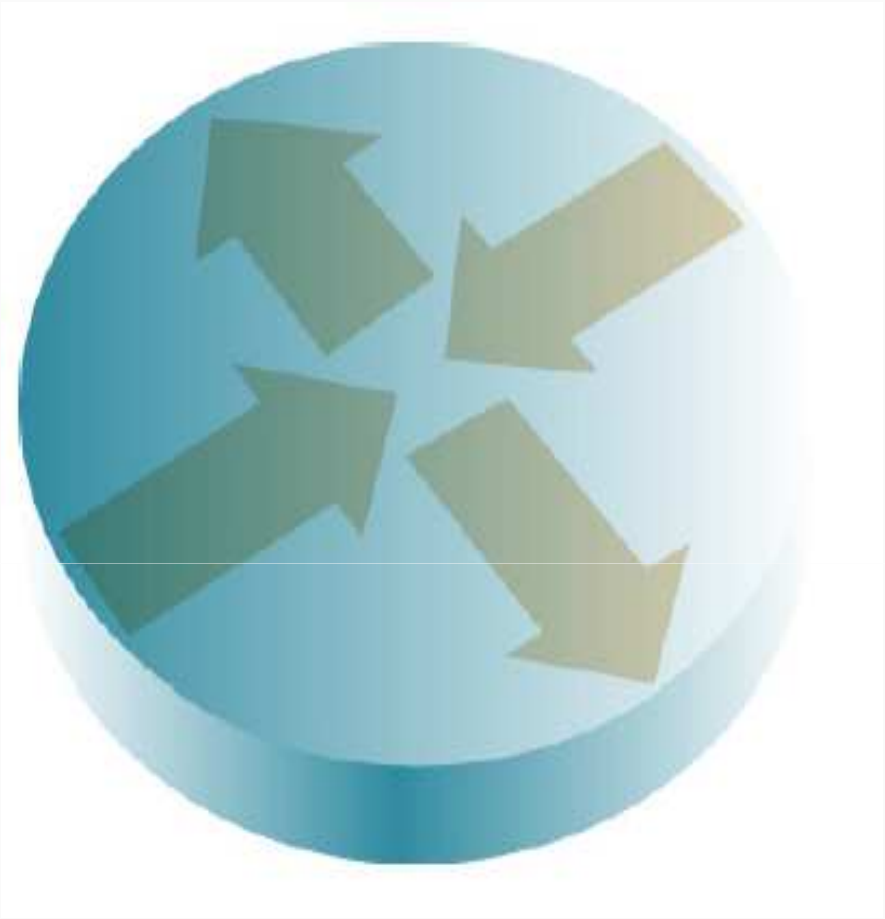
- A router is required to properly forward data between clients on different segments.

Routers

- Receive datagrams from hosts on their network(or other connected routers)

- Must decide how to forward to the desctination-which may or may not be on the attached network

- Maintains routing tables and check each datagram's destination address against the routing table before forwarding the datagram on to the next router or to the appropriate destination



Information required for routing

- There are two required pieces of information for routing;
  →an Internet Protocol (IP) address
  →identification of Routed/Routing Protocols.

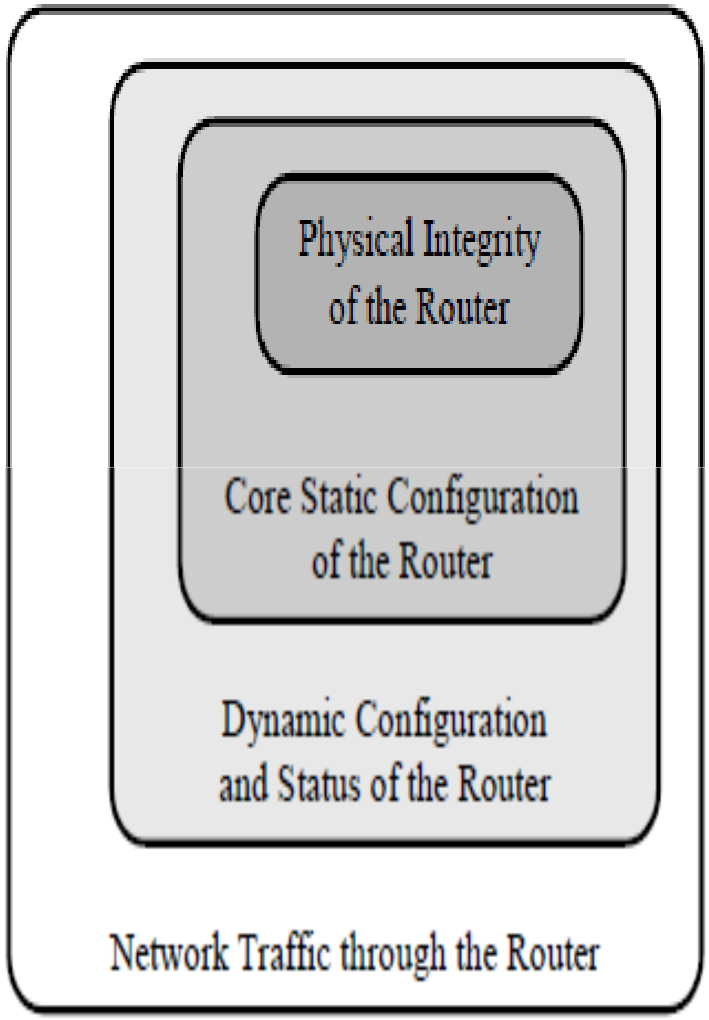
- A routed protocol is a protocol by which data can be routed.eg. IP, IPX, and AppleTalk. Such a protocol requires an addressing scheme based on which the router will be able to identify the network to which a host belongs, in addition to identifying that host on that network.

- A routing protocol, on the other hand, is only used between routers. Its purpose is to help routers building and maintain routing tables.eg.OSPF,BGP etc.
- Routers do not pass broadcast traffic
- Build their routing tables statically or by using routing tables
  -Distance vector routing : RIP,IGRP,EIGRP
  -Link state routing : OSPF,IS – IS
  -Path vector routing : BGP

Routers and security

- Add security to the network by separating broadcast domains and implementing the rule sets.
- Define what traffic is allowed to traverse the device and what cannot through the use of ACLs(access control lists)
- Protecting the router itself as they are available to the remote networks.

Security Policy for Router



Physical Security Aspect

- **Physical Security Aspect for Router security Policy**
  - • Designates who is authorized to install, de-install, and move the router.
  - • Designates who is authorized to perform hardware maintenance and to change the physical configuration of the router.
  - • Designates who is authorized to make physical connections to the router.
  - • Defines controls on placement and use of console and other direct access port connections.
  - • Defines recovery procedures for the event of physical damage to the router, or evidence of tampering with the router.

Static Configuration Security Aspect

- Designates who is authorized to log in directly to the router via the console or other direct access port connections.
- Designates who is authorized to assume administrative privileges on the router.
- Defines procedures and practices for making changes to the router static configuration (e.g. log book, change recording, review procedures)
- Defines the password policy for user/login passwords, and for administrative or privilege passwords
- Designates who is authorized to log in to the router remotely at what level.
- Designates protocols, procedures, and networks permitted for logging in to the router remotely.
- Defines the recovery procedures and identifies individuals responsible for recovery, in the case of compromise of the router's static configuration.
- Defines the audit log policy for the router, including outlining log management practices and procedures and log review responsibilities.
- Designates procedures and limits on use of automated remote management and monitoring facilities (e.g. SNMP)
- Outlines response procedures or guidelines for detection of an attack against the router itself.

Dynamic Configuration Security Aspect

- Identifies the dynamic configuration services permitted on the router, and the networks permitted to access those services.
- Identifies the routing protocols to be used, and the security features to be employed on each.
- Designates mechanisms and policies for setting or automating maintenance of the router's clock (e.g. manual setting, NTP).
- Identifies key agreement and cryptographic algorithms authorized for use in establishing VPN tunnels with other networks (if any).

Network security aspect of Router Security Policy

- Enumerates protocols, ports, and services to be permitted or filtered by the router, for each interface or connection (e.g. inbound and outbound), and identifies procedures and authorities for authorizing them.
- Describes security procedures and roles for interactions with external service providers and maintenance technicians.

Response Strategy in case of Compromise

- Enumerates individuals or organizations to be notified in the event of a network compromise.
- Identifies relevant configuration information to be captured and retained.
- Defines response procedures, authorities, and objectives for response after a successful attack against the network, including provision for preserving evidence and for notification of law enforcement**.**