**MODULE IV : IP Routing Protocols**

TCP/IP Dynamic Routing Protocols:General Routing Concepts and Terms-TCP/IP Static Routing-TCP/IP Interior Gateway Protocols-t TCP/IP Exterior Gateway Protocols Configuring IP Routing Protocols on Routers: Choosing the Right Protocol-Route Selection-General Routing Information-Managing Static Routing- Configuring Dynamic IGP and BGP IP Routing ProtocolsRoute pand Redistribution. Network Troubleshooting, Performance Tuning, and Management Fundamentals: Network Analysis and Performance Tuning-Develop Troubleshooting Skills-Network Management Fundamentals.

## General Routing Concepts

Routers use a routing protocol to know all the available paths of the network and to select the best and the fastest path to forward incoming packets. A routing protocol provides the following functionalities.

- Provide a virtual map of all paths of the network.
- Calculate the cost of each path and help a router to select the best and fastest path.
- Detecting any change in the network and updating all routers about that change.

There are two types of routing; static routing and dynamic routing.

In **static** routing, we have to manually provide/configure the above-listed functionalities on each router of the network. Since all configurations are done manually, a routing protocol is neither required nor used in static routing.

In **dynamic** routing, a routing protocol provides/configures the above-listed functionalities on each router of the network. Since all functionalities are provided by a routing protocol, we must have to configure and activate a routing protocol on all routers of the network.

## Dynamic Routing Protocol

The basic job of a dynamic routing protocol is to find the best, most efficient route to forward IP network traffic.The dynamic routing protocol can also find a secondary route in the event that the best route is lost. Enterprise networks commonly use multiple network paths to interconnect segments. Routing protocols provide two main advantages:

• The capability to balance the traffic load between these paths and keep traffic flowing in the event that a path is lost

• The capability to easily add routes (such as new network segments) to the network.

IP network routing can be categorized into two distinct types of routing:

• Intra Network routing

• Internetwork routing

***Intranetwork routing***, ***or interior routing***, exchanges route information between routers within defined routing processes. An intranetwork can have single or multiple routing processes. Protocols that perform intranetwork routing are known as *interior gateway protocols (IGPs)*. The *Routing Information Protocol (RIP)* and *Open Shortest Path First (OSPF)* are popular IGPs. Intranetwork routing is known as intradomain routing

***Internetwork routing*** has two dimensions: First, in the context of the global Internet, internetwork routing is the exchange of routing information between large, centrally administered networks known as *autonomous systems (ASs)*. A particular type of routing protocol known as *Exterior Gateway Protocol (EGP)* performs this task. EGP was the first protocol created to perform this function. Today, *Border Gateway Protocol (BGP)* version 4 is the most commonly employed protocol for this task.Internetwork routing is known as interdomain routing

## Routing Metrics

Routing metrics are used by dynamic routing protocols to establish preferences for a particular route. All dynamic routing protocols use some form of route metrics. The goal of route metrics is to provide the capability for the routing protocol to support the following network attributes:

• *Route diversity* exists when two or more unrelated access points or paths exist for the same network.

• *Route redundancy* exists when two or more access points to the same network exist with equal metrics.

• *Load balancing* is the practice of distributing network traffic evenly across multiple links

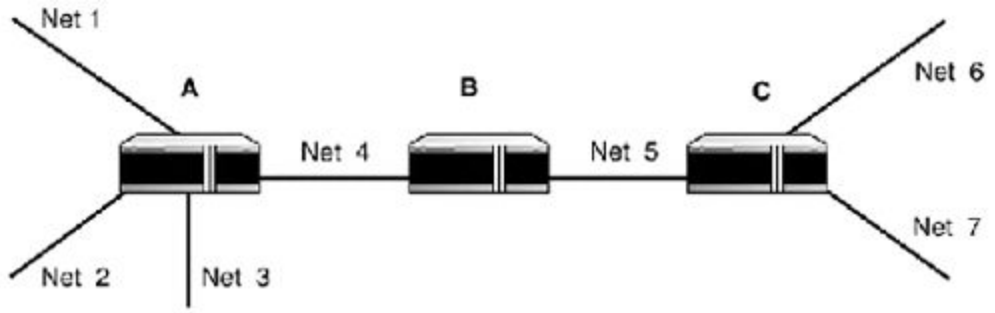
The following list describes the most common routing metric variables:

- *Hop count*: Hop count is the number of intermediate systems (routers) between the router and the destination router.
- *Bandwidth* : This metric reflects the interface's ideal throughput. For example, a serial interface on a Cisco router has a default bandwidth of 1.544Mbps, and Ethernet has a default bandwidth of 10Mbps.
- *Load*: The load metric varies based on the actual usage (traffic).
- *Delay*: Delay is the total time needed to move a packet across the route. The shortest time is the best route.
- *Reliability*:Reliability estimates the chance of a link failure and can be set by an administrator or established by the given protocol.
- *Cost*: This metric sets the preference for a given route. The lower the cost, the more preferable the route. Most routers have a default value for each type of interface. The interface's default cost is directly related to its speed.

## Network Convergence

*Convergence* is the process of bringing all the routing tables of all the routers in the network to a state of consistency. Routing information is distributed between physically connected routers as

broadcast or multicast messages. Network information is designated in a router-to-router (hop-to-hop) fashion the same way that IP datagrams are delivered.




Router A has four networks attached to it. Router B is directly attached to Router A. Router A sends information about all of its directly connected networks to Router B. Router B then tells Router C about all of the networks it knows about: its own directly connected networks, and all of Router A's directly connected networks. Router C tells Router B about its directly connected networks and Router B tells Router A about Router C's networks.

*Convergence time* is how long it takes for routers to learn the network topology and/or changes in the network topology. When a change takes place, the network is in a state of flux, and it is possible that some routers will forward traffic to paths that are not available or no longer exist. In large networks, it is preferable to use a routing protocol that has a fast convergence time.

## Distance-vector routing protocol

Distance-vector routing protocols use the Bellman–Ford algorithm. In these protocols, each router does not possess information about the full network topology. It advertises its distance value (DV) calculated to other routers and receives similar advertisements from other routers unless changes are done in the local network or by neighbours (routers). Using these routing advertisements each router populates its routing table. In the next advertisement cycle, a router advertises updated information from its routing table. This process continues until the routing tables of each router converge to stable values.Some of these protocols have the disadvantage of slow convergence.

## Link-state routing protocol

In link-state routing protocols, each router possesses information about the complete network topology. Each router then independently calculates the best next hop from it for every possible destination in the network using local information of the topology. The collection of best-next-hops forms the routing table.

This contrasts with distance-vector routing protocols, which work by having each node share its routing table with its neighbours. In a link-state protocol, the only information passed between the nodes is information used to construct the connectivity maps.

Examples of link-state routing protocols:

- Open Shortest Path First (OSPF)
- Intermediate system to intermediate system (IS-IS)

## TCP/IP Static Routing

### TCP/IP Interior Gateway Protocols

An **interior gateway protocol** (**IGP**) is a type of protocol used for exchanging routing information between gateways (commonly routers) *within* an autonomous system (for example, a system of corporate local area networks). This routing information can then be used to route network-layer protocols like IP.

Specific examples of IGPs include :

1. Routing Information Protocol (RIP)
2. Interior Gateway Routing Protocol (IGRP)
3. Enhanced Interior Gateway Routing Protocol (EIGRP)
4. Open Shortest Path First (OSPF)

**1. Routing Information Protocol** (**RIP**)

- The **Routing Information Protocol** (**RIP**) is one of the oldest distance-vector routing protocols which employ the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination. The largest number of hops allowed for RIP is 15, which limits the size of networks that RIP can support.
- RIP uses the User Datagram Protocol (UDP) as its transport protocol, and is assigned the reserved port number 520.

Versions of RIP is:

- Routing Information Protocol Version 1 (RIPv1)
- Routing Information Protocol Version 2 (RIPv2)
- Routing Information Protocol Next Generation (RIPng)

**2. Interior Gateway Routing Protocol** (**IGRP**)

- It is a distance vector interior gateway protocol (IGP) developed by Cisco. It is used by routers to exchange routing data within an autonomous system.

- IGRP is a proprietary protocol. IGRP was created in part to overcome the limitations of RIP when used within large networks.
- The maximum configurable hop count of IGRP-routed packets is 255 (default 100), and routing updates are broadcast every 90 seconds (by default).
- IGRP uses protocol number 9 for communication.[2]IGRP supports multiple metrics for each route, including bandwidth, delay, load, and reliability; to compare two routes

**3. Enhanced Interior Gateway Routing Protocol (EIGRP)**

- It is an advanced distance-vector routing protocol that is used on a computer network for automating routing decisions and configuration. The protocol was designed by Cisco Systems as a proprietary protocol, available only on Cisco routers.
- EIGRP is used on a router to share routes with other routers within the same autonomous system. Unlike other well known routing protocols, such as RIP, EIGRP only sends incremental updates, reducing the workload on the router and the amount of data that needs to be transmitted.
- EIGRP replaced the Interior Gateway Routing Protocol (IGRP) in 1993. One of the major reasons for this was the change to classless IPv4 addresses in the Internet Protocol, which IGRP could not support.

**4. Open Shortest Path First (OSPF)**

- It is a routing protocol for Internet Protocol (IP) networks.
- It uses a link state routing (LSR) algorithm and falls into the group of interior gateway protocols (IGPs), operating within a single autonomous system (AS).
- OSPF is a widely used IGP in large enterprise networks.
- It implements Dijkstra's algorithm, also known as the shortest path first (SPF) algorithm.
- The shortest path through a network was calculated based on the *cost* of the route, taking into account bandwidth, delay and load.
- Therefore OSPF undertakes route cost calculation on the basis of link-cost parameters, which can be weighted by the administrator. OSPF was quickly adopted because it became known for reliably calculating routes through large and complex local area networks.

**TCP/IP Exterior Gateway Protocols**

Exterior routing protocols are used to exchange routing information between autonomous systems. The routing information passed between autonomous systems is called *reachability information*. Reachability information is simply information about which networks can be reached through a specific autonomous system

“The classic definition of an Autonomous System is a set of routers under a single technical administration, using an interior gateway protocol and common metrics to route

packets within the AS, and using an exterior gateway protocol to route packets to other ASs."

Exterior routing protocols are:

1. **Exterior Gateway Protocol (EGP)**
2. **Border Gateway Protocol (BGP)**

### 1. Exterior Gateway Protocol (EGP)

- A gateway running EGP announces that it can reach networks that are part of its autonomous system. It does not announce that it can reach networks outside its autonomous system.
- Before sending routing information, the systems first exchange EGP *Hello* and *I-Heard-You* (I-H-U) messages.
- These messages establish a dialog between two EGP gateways. Computers communicating via EGP are called *EGP neighbors*, and the exchange of Hello and I-H-U messages is called *acquiring a neighbor*.
- Once a neighbor is acquired, routing information is requested via a *poll*. The neighbor responds by sending a packet of reachability information called an *update*.
- The local system includes the routes from the update into its local routing table. If the neighbor fails to respond to three consecutive polls, the system assumes that the neighbor is down and removes the neighbor's routes from its table. If the system receives a poll from its EGP neighbor, it responds with its own update packet.

### 1. Border Gateway Protocol (BGP)

- *Border Gateway Protocol* (BGP) is the leading exterior routing protocol of the Internet. It is based on the OSI *InterDomain Routing Protocol* (IDRP).
- BGP supports *policy-based routing*, which uses non-technical reasons (for example, political, organizational, or security considerations) to make routing decisions.
- Thus BGP enhances an autonomous system's ability to choose between routes and to implement routing policies without relying on a central routing authority.
- This feature is important in the absence of core gateways to perform these tasks.
- Routing policies are not part of the BGP protocol. Policies are provided externally as configuration information.

## Configuring IP Routing Protocols on Cisco Routers

### Choosing the Right Protocol

- Static routing, which is by far the easiest and most problem-free method, is tedious to manage in large networks and provides no recovery facility when link failures occur.
- Dynamic routing protocols address the shortcomings of static routing, but do, however, come with their own operational concerns.
- Unfortunately, when selecting an IP announcement methodology, there is no single correct answer. The way to avoid this problem is to examine the network's topology, availability, and performance requirements through a series of questions:

1. What kind of network is this?
2. What is the network diameter ?
3. Is CIDR/VLSM addressing support required?
4. Does the network use redundant or multiple paths between network segments?
5. What type of equipment will be used to route traffic on the network, and is a standards-based routing protocol required?
6. What are the performance requirements of the routers in the network? For example, is convergence time a factor?

### Comparison of routing protocol

| Protocol Feature | RIP v1/v2 | IGRP | EIGRP | OSPF | Static | BGP |
|---|---|---|---|---|---|---|
| Supports classful addressing | yes | yes | yes | yes | yes | yes |
| Interior Gateway Protocol | yes | yes | yes | yes | no | no |
| Exterior Gateway Protocol | no | no | no | no | no | yes |
| Supports classless addressing | yes (V2) | no | yes | yes | yes | yes |
| Supports load sharing | no | yes | yes | yes | no | yes |
| Supports authentication | yes (V2) | no | yes | yes | no | yes |
| Easy implementation | yes | yes | yes | yes | no | no |

| | | | | | | |
|---|---|---|---|---|---|---|
| Routing algorithm | DV | DV | DUAL | LS | none | DV |
| Supports weighted metrics | no | yes | yes | yes | no | no |
| Fast convergence | no | yes | yes | yes | yes | yes |
| Uses broadcasts for route updates | yes (v1) | yes | no | no | no | no |
| Uses multicast for routing updates | Yes (v2) | no | yes | yes | no | no |
| Supports large network diameters | | no | yes | yes | yes | yes |
| DV=Distance Vector; LS=Link State; DUAL=Diffusing Update Algorithm | | | | | | |

**Route Selection**

- The router will use all the available sources of reachability information to construct the most accurate and efficient routing table.
- An administrative distance, which is used to determine a route's integrity.
- Default administrative distances are:

| Protocol | Distance |
|---|---|
| Connected interface | 0 |
| Static route | 1 |
| EIGRP summary route | 5 |
| BGP (external) | 20 |
| EIGRP (internal) | 90 |
| IGRP | 100 |
| OSPF | 110 |
| RIP | 120 |
| EIGRP (external) | 170 |
| BGP (internal) | 200 |
| Unknown | 255 |

**General Routing Information**

There are several IOS commands used for controlling and displaying information about IP routing**.**

**Display commands:**

<show ip route>

<show ip route connected>

<show ip route [address/hostname]>

<show arp>

<show ip protocol>
<show ip masks>
<show ip masks [network address]><traceroute>

**Control commands:**

<clear ip route *>
<clear ip route [network] [mask]>
<clear arp>

**Managing Static Routing**

**Display commands:**

<show ip route>
<show interface [type/slot/port]>

**Global configuration commands**:

<ip route [network] [mask] [gateway] [administrative distance]>
<ip classless>
<ip subnet-zero>
<ip forward-protocol udp [port number]>
<no ip source-route>

**Interface configuration subcommands:**

<ip helper address [ip address]>
<bandwidth>
<mtu>
<no ip redirects>
<no ip unreachables>

**Control commands:** <copy tftp [route-table-name]>

- Static routes are set in the Cisco IOS using the <ip route> configuration EXEC command.
- With the IOS, static route entries are managed as an IP routing process, so they are reloaded after routing table flush.

**Configuring Dynamic IGP and EGP IP Routing Protocols**

- All dynamic IP routing protocols are configured as IOS subprocesses, much the same way a router interface is configured.
- **Active mode**: you need to add each directly connected network that you wish the protocol to announce.
- **Passive mode** : it will only receive routing announcements.
- The IGP process ID is often the same number as the network's autonomous system (AS) number.
- When using RIP, no process ID is required because only one RIP process is supported.
- In IGRP, EGRP, and OSPF, where multiple processes can be supported.

- Two elements make IGRP a significant improvement over RIP are
    - Bandwidth (K1)
    - Delay (K2)
    - Reliability (K3)
    - Load (K4)
    - MTU (K5)
    - Faster convergence time
- EIGRP uses the "hello" protocol to establish relationships with the neighbors.

**Route Control and Redistribution**

- IOS usually uses dynamic routing protocols to redistribute static or dynamic routing information.
- For redistribution, use multiple dynamic routing concepts.
- With single-point connections, static routes can be used to send packets destined to external networks to the Internet gateway.
- If multiple links exist it is possible to use filtered redistribution to limit the inbound and outbound network announcements between the different routing policies using distribution lists and route-maps.
- Static route redistribution is often used instead of adding static routes on every router on the network, a single router can redistribute a collection of static routes.
- Static route redistribution can also be used to limit network announcements inside internal networks.

## Network Troubleshooting, Performance Tuning, and Management Fundamentals

**Network Analysis and Performance Tuning**

- Using a management and monitoring system on your network is the best way to identify network faults and performance issues.
- The purpose of network analysis is twofold:-
    - to implement any effective monitoring and management system.
    - to resolve network fault conditions and to improve overall network performance through performance tuning.

- Following are the some of the network analyzers:-
    - Tools - Packet analyzers or packet sniffers, software tools like ping and traceroute are some of the valuable tools. The main is proper documentation.
    - Documentation - Good documentation is very important. A network that is well designed and properly documented is easily managed.
    - Topology Maps - The map should indicate the physical locations of the equipment, network segments, and device and interface addressing information.
    - Device Information - This can be an Access or Oracle database, a set of index cards, even a set of Web pages.

- Change Log - All changes should be documented. Network patches, device moves, software and hardware upgrades, and device module additions and removals should be in the log.
- Protocol Analyzers - The function of protocol analyzers is to capture and display network protocol data.
- Time Domain Reflectors - TDR devices are used for diagnosing cable failure and associated problems.
- Bit Error Rate Testers - It used to verify and test telecom transmission circuits.
- Packet Internet Groper (Ping) - It is a simple tool for testing host reachability.
- Traceroute - To check the route to the destination host or to verify that all of the gateways in the path are up, traceroute is used. It uses ICMP echo-request messages to trace the gateway path one hop at a time.

**Developing Troubleshooting Skills**

- Some individuals are born troubleshooters and for others it can be acquired through proper learning.
- Problem resolution can be in two modes - proactive mode and reactive mode.
- The ultimate goal of proactive problem resolution is to identify problems and resolve them before they impact service performance.
- Reactive problem resolution deals with problems as they arise. Most IT and MIS shops operate to some degree in both proactive and reactive mode.
- The basic nature of information systems support requires this dual mode approach.
- A network administrator should identify the real problem and assist those actually responsible for correcting the problem.

**Network Management Fundamentals**

**Network Management Functions**

- Network management consists of separate and distinct tasks that contribute to the management of a complex collection of interdependent systems.
- The primary network management functions include the following:
  - Physical infrastructure, interconnection cabling, network hardware installation, etc. Cable testing and length validation also fall into this category.
  - Device configuration, bridge, router, switch, and repeater configuration. Creating and updating network topology maps, installation location, and other basic configuration information. Proper network documentation is essential when diagnosing network problems and performing performance testing.
  - Link and services monitoring, network performance baselining, and periodic performance revaluation. Proactive and reactive hardware, link and network service failure detection. Network security monitoring.

- In small office networks (generally 20 to 50 nodes), these duties are often performed by a network administrator.

- In large enterprises (100 to 1000 nodes), some kind of Network Management System (NMS) is generally required.

**NMS Architecture**

- An NMS consists of the network hardware components that need to be managed running a software or firmware-based management interface or agent, a network management protocol, and a network management console.
- Depending on the size and scope of the NMS, there can be one or several Network Management Consoles (NMC).
- The NMC is a computer that operates one or more management entities.
- These management entities perform basic management functions.
- This collects information and the data is stored in specialized databases that are used for performance analysis, problem tracking and resolution, trouble ticketing, and inventory control.
- Most NMCs also perform automatic device discovery and topology mapping.
- Following figure shows the basic NMS relationship structure.

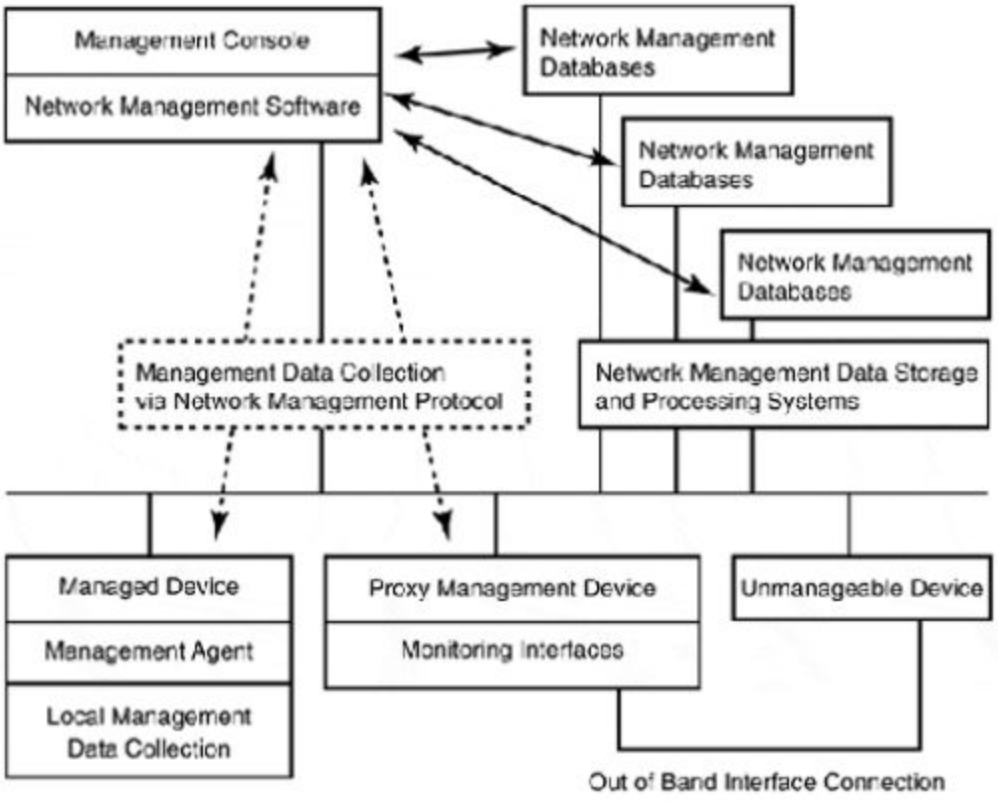



Fig. The basic NMS architecture model