Volume 4, Issue 12, December 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Comparative Study of Routing Protocols with Subnetting Implementation in Cisco Packet Tracer

Pritesh Kumar Jain*, Manoj Sindhwani, Shippu Sachdeva
Asst. Professor, Department of ECE,
Lovely Professional University,
Punjab, India

Abstract— This Paper covers comparison of routing methodology based on logical addressing using subnetting, concept of Dynamic Host Configuration Protocol (DHCP). Routing protocols are used to transmit packets across the Internet. Routing protocols specify how routers communicate with each other. The router has prior knowledge about the adjacent networks (based on routing algorithm), which can assist in selecting the routes between two nodes. There are various types of routing protocols that are Inter domain and Intra domain, Routing Information protocol (RIP) ,open shortest path first (OSPF)and Enhanced Interior Gateway Routing Protocol (EIGRP) have been considered as the pre-eminent routing protocols for real-time applications. Subnet allows administrators to divide their private network into virtually defined segments with many advantages of subnetting. Dynamic Host Control Protocol is a service that automatically assigns IP addresses to devices that connect to the network.

Keywords— OSPF, RIP, EIGRP, DHCP, CPT

I. INTRODUCTION

A routing protocol is defined as a set of messages, rules, and algorithms used by routers for the overall purpose of learning routes. This process includes the exchange and analysis of routing information. Each router chooses the best route to each subnet in a process known as path selection and finally places those best routes in its IP routing table. Examples of a routing protocol include RIP, EIGRP, OSPF, and BGP. Routing protocols [1] [7] help routers learn routes by having each router advertise the routes it knows. Each router begins by knowing only directly connected routes. After that, each router sends messages, defined by the routing protocol, that list the routes. When a router hears a routing update message from another router, the router hearing the update learns about the subnets and adds routes to its routing table. If all the routers participate, all the routers can learn about all subnets in an internetwork.

II. CLASSIFICATION OF ROUTING PROTOCOL

1. Static Routing

Network administrators can create routing tables manually, but it is a tedious task. The only advantage is that the administrator knows the exact path data is taking to get to a destination, making static routing tables predictable and manageable. Static routing works best in small networks.

2. Dynamic Routing

A less tedious way to create a routing table is dynamically. Dynamic routing requires each device in a network to broadcast information about its location, which other devices use to update their routing tables. Frequent broadcasting keeps the tables up to date. Dynamic routing protocols use different algorithms to help routers refine path selection: interior, exterior, link state and distance vector, according to where they are in a network and what type of information they provide.

3. Interior and Exterior Protocols

Interior gateway protocols, as the Internet community calls them, are typically used in small, cooperative set of networks such as might be found on a university campus. One of the oldest interior protocols is Routing Information Protocol, or RIP. Newer interior protocols include Interior Gateway Routing Protocol, or IGRP, and Open Shortest Path First, or OSPF. Cisco network devices can also use Cisco's proprietary Enhanced Interior Gateway Routing Protocol, or EIGRP. Interior protocols are fairly easy to set up, but do not scale well to large networks. For large networks, network administrators use an exterior protocol such as Border Gateway Protocol, or BGP, to connect large entities like corporate and university networks to the Internet

4. Link-State Protocol

As its name implies, a link-state protocol collects data about the links or segments between one device and another. Mostly this data is about distance and connectivity, but in some networks link-state data includes information about bandwidth, traffic loads, and type of traffic accepted on the links. OSPF is a link-state routing protocol.

5. Distance-Vector Protocol

Two basic pieces of data are exchanged in distance-vector protocols, distance to the destination and which vector direction to take to get there. RIP is a simple distance-vector protocol that keeps a table of paths it learns and the distances to them.

6. Hybrid Protocols

Not all routing protocols fall into the categories defined above. For example, Cisco's proprietary EIGRP is sometimes described as a hybrid of the link-state and distance-vector protocols. Cisco describes EIGRP as "an enhanced distance-vector protocol that calculates the shortest path to a network." The BGP exterior gateway protocol uses an algorithm called path vector, which means it keeps track of paths used and compares them to determine the best one.

III. ROUTING INFORMATION PROTOCOL

RIP [2] [7] is a standardized Distance Vector protocol, designed for use on smaller networks. RIP was one of the first true Distance Vector routing protocols, and is supported on a wide variety of systems. Using RIP, a gateway host (with a router) sends its entire routing table (which lists all the other hosts it knows about) to its closest neighbour host every 30 seconds. The neighbour host in turn will pass the information on to its next neighbour and so on until all hosts within the network have the same knowledge of routing paths, a state known as network convergence. RIP uses a hop count as a way to determine network distance. Each host with a router in the network uses the routing table information to determine the next host to route a packet to for a specified destination. RIP is considered an effective solution for small homogeneous networks. For larger, more complicated networks, RIP's transmission of the entire routing table every 30 seconds may put a heavy amount of extra traffic in the network. The Routing Information Protocol, or RIP, as it is more commonly called, is one of the most enduring of all routing protocols. RIP uses the Bellman-Ford Distance Vector algorithm to determine the best “path” to a particular destination RIP has four basic components: routing update process, RIP routing metrics, routing stability, and routing timers. Devices that support RIP send routing-update messages at regular intervals and when the network topology changes. These RIP packets contain information about the networks that the devices can reach, as well as the number of routers or gateways that a packet must travel through to reach the destination address. RIP is used in LANs and WANs including versions mentioned below.

1. RIPv1

RIP 1, the original RIP specification, uses classful network routing classful networks, utilized largely for Internet routing from 1981 until 1993 when Classless Inter-Domain Routing was introduced, divides Internet address space into classes, which in turn defines network size. RIP 1 carries no subnet-mask information or routing prefixes in an Internet Protocol sub network. Thereby rendering it impossible to contain different sized subnetworks within the same network class A classful protocol, broadcasts updates every 30 seconds, hold-down period 180 seconds. Hop count is metric (Maximum 15).

2. RIPv2

RIPv2, also known as RIPv2, was developed in 1993 in response to deficiencies in the RIP 1 standard. RIP 2 carries subnetwork and subnetmask information and supports CIDR, or Classless Inter-Domain Routing. Classless Inter-Domain Routing refers to a system of methods used to distribute or allocate IP addresses and route Internet Protocol packets, which are groups of data. RIPv2 uses multicasts, version 1 use broadcasts and supports triggered updates (when a change occurs).RIPv2 router will immediately propagate its routing information to its connected neighbors. RIPv2 supports authentication and variable-length subnet masking (VLSM).

3. RIPng

RIPng[7], or RIP next generation, refers to an extension of RIP 2 developed to support the next generation Internet Protocol, or IPv6. IPv6, short for Internet Protocol version 6, the successor to the IPv4 protocol, is used for packet-switched internetworking.

RIP Advantages and Disadvantages

The major advantages of distance vector protocol[8] are that it is simple and that is an old, well-established technology that is almost universally available. Because it is simple, distance vector protocol means simple hardware. , there is no incompatibility with any Internet device. User can buy a cheaper router because all routers implement distance vector protocol. Along with this advantage there is some disadvantage of RIP which affect the efficiency and introduce delay in the network. Distance vector protocol does not always find the best path. This can be well understand by consider simple example, suppose one path has six nodes (distance = 6) but the path is very high speed and not busy at all and another path has only two nodes but is very low speed and unreliable, sometimes requiring retransmissions. Assuming that the vector includes both paths, the distance vector protocol will always choose the 2 node path although it may be a lot slower. Because of this, a newer style routing protocol called "link state protocol" was invented. Link site protocol uses a much more complicated algorithm based on information like how busy a channel is, what its transmission rate is and how reliable the connection is at the present time. Routing Information Protocol limited to 15 hops, any router beyond that distance is considered as infinity, and hence unreachable. If implemented in a large network, RIP can create a traffic bottleneck by multicasting all the routing tables every 30 seconds, which is bandwidth intensive. This results in an increased delay in delivering packets and overloads network operations due to repeated processes.

IV. OPEN SHORTEST PATH FIRST

OSPF [4] stands for "Open Shortest Path First." It is a routing algorithm used in forwarding packets over a network under the Internet protocol. The protocol is classed as an "interior gateway protocol" because its scope does not extend beyond the boundaries of the network upon which it resides. The basic function of OSPF decides which route a packet of data should be forwarded to base on the packet's ultimate destination and the state of network connections recorded in the router's routing table. This table attributes a "cost" to each route. The cost, expressed as a number, is based on distance, throughput and reliability. The system keeps a record of all possible paths across the network. This is held as a tree structure. The router will recalculate the score of each path each time a link is broken. This is called "link state routing. The end result of these calculations is that there will be paths that have a lower cost than others. These will be used in preference as they show that they are the quickest route, or "Shortest Path."

V. ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL

EIGRP [5] stands for Enhanced Interior Gateway Routing Protocol and refers to a routing protocol. A routing protocol is a formal set of rules that governs how units of data, known as packets, are forwarded, or “routed,” from one computer network to another. Once you’ve completed the basic configuration of EIGRP, you need to verify that it’s working properly EIGRP, a distance vector routing protocol, exchanges routing table information with neighboring routers in an autonomous system. Unlike RIP, EIGRP[1] shares routing table information that is not available in the neighboring routers, thereby reducing unwanted traffic transmitted through routers. EIGRP are very low usage of network resources during normal operation only hello packets are transmitted on a stable network .when a change occurs, only routing table changes are propagated, not the entire routing table and this reduces the load the routing protocol itself places on the network .

EIGRP has four basic components:

1) Neighbor discovery/recovery
2) Reliable transport Protocol
3) DUAL Finite State Machine
4) Protocol Dependent Modules

EIGRP uses five packet types:

1) Hello/Acknowledge
2) Updates
3) Queries
4) Replies
5) Requests

VI. DYNAMIC HOST CONFIGURATION PROTOCOL

Dynamic Host Configuration Protocol [6] is a service that automatically assigns IP addresses to devices that connect to the network. If a device is configured to automatically obtain an IP address, it sends out a request for an IP address when it connects to a network. The request may get more than one offer of an IP address, and the computer typically accepts the first offer that it gets. This relieves the network administrator of having to manage each device. Instead, you just have to configure the DHCP server with a range of IP addresses that are available for assignment to connecting devices. DHCP can also assign values for the address of the DNS server as well as the default gateway. All of this makes the life of a network administrator much easier.

VII. SUBNETTING

Subnet allows administrators to divide their private network into virtually defined segments. Subnets provide a lot of benefits for network administrators, and ultimately users, by making administration and routing more efficient such as: Subnetting[6] Prevents Unnecessary Broadcasts, Increases Security Options, Simplifies Administration and Controls Growth. Each IP class is equipped with its own default subnet mask which bounds that IP class to have prefixed number of Networks and prefixed number of Hosts per network. Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more Networks per IP Class. Classless Inter Domain Routing (CIDR) provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet. By using subnetting, one single Class IP address can be used to have smaller sub-networks which provide better network management capabilities.

VIII. SYSTEM MODEL

System Model Algorithm

In this network we have implemented different routing protocols like RIPv2, EIGRP, OSPF taking different topologies with the following steps:-

1) First to create particular topology by using different networking devices like routers, switches, end-devices and connections from component list in CPT[9], as mentioned in the table.

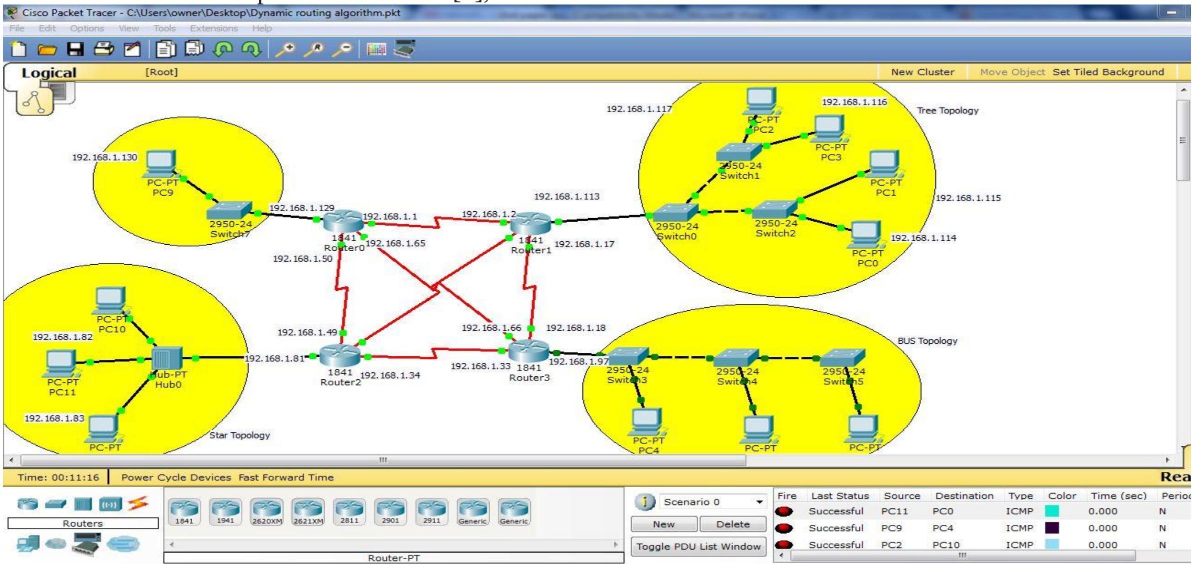

Fig.1. Implementation of Routing Protocols with Subnetting in Cisco Packet Tracer

Table I: specification list of networking devices

Sr. No.	Name of Device	Specification
1	Router(1841)	2 Fast-Ethernet Ports and 4 Serial Ports
2	Switch(2950-24)	24 Fast-Ethernet Ports
3	Generic Hub	6 Ports
4	End Devices	PC
5	Connections	Serial DCE, Copper Straight-Through and Copper Cross-Over Cable

2) The connections between routers are serial DCE, between routers to switches or hubs, are Copper Straight-Through, and between switch to switch is Copper Cross-Over.
3) To configure the routers, we have executed several commands in command line interface (CLI) Tab.
4) Implementation of Hybrid Topology (like Star, Tree, Bus Topology) is also considered in this model.
5) Finally to implement RIPv2 in this system design model we have used following syntax-
   Router(config)#router rip
   Router(config-router)#network 192.168.1.0
   Router(config-router)#version 2
   Router(config-router)#exit
   Similarly we can configure all routers using ripv2, with their respective network addresses.
6) To implement EIGRP in this system design model we have used following syntax-
   Router(config)#router eigrp 10 (This 10 number is process ID)
   Router(config-router)#network 192.168.1.0
   Router(config-router)#exit
   Similarly we can configure all routers using eigrp, with their respective network addresses.
7) To implement OSPF in this system design model we have used following syntax-
   Router(config)#router ospf 1 (This 1 number is process ID)
   Router(config-router)#network 192.168.1.0 0.0.0.15 area 0 (wild card mask)
   Router(config-router)#exit
   Similarly we can configure all routers using ospf, with their respective network addresses.

IX. SUMMARY OF COMPARISON BETWEEN ROUTING PROTOCOLS

To understand the concept we summarize the fundamental differences between various routing protocol in the table mentioned below.

Table II: summary of comparative study between routing protocols

Protocol	RIP	EIGRP	OSPF
Suitable for	Small Networks	Large Networks	Large Networks
Ease of Use	Easy	Easiest	Complex
Support VLSM	Only in RIPv2	Yes	Yes
Bandwidth Consumption	High	Low	Moderate
Loop Free	No	Yes	Yes

X. CONCLUSION

In this paper the network is demonstrated in Cisco packet Tracer, with various routing protocols and an additional concept of subnetting. The subnet allows the administrator to divide their private network into virtually defined segments.After comparison we find that the best protocol is EIGRP because it provides better performance than RIPv2 and OSPF, in terms of fast convergence time. While comparing OSPF and RIP, OSPF dominates RIP in terms of average throughput and instant delay in different size of network.

REFERENCES

[1] Shravan K. Naivety and Santosh K. Balsu (2011) “Performance Comparison of EIGRP and ISIS/RIP Protocols”, School of Computing/Telecom, Karlskron, Sweden.
[2] Khalid Abu Al-Saud, Mohammed Saleh (2008) “Impact of MD5 Authentication on Routing Traffic for the Case of EIGRP, RIPv2 and OSPF”, University Utara Malaysia
[3] Lemma.E, Hussain .S, Anjelo .W (2010) “Performance Comparison of EIGRP/IS-IS and OSPF/IS-IS”, Blenkinge Tekniska Hogskolan, Sweden.
[4] Ayub,N., et al. (2011). Performance Analysis of OSPF and EIGRP Routing Protocols with Respect to theConvergence, European Journal of Scientific Research, ISSN 1450-216X Vol.61 No. 3, pp434-447.
[5] Farhangi, S. et al. (2012). Performance Comparison of Mixed Protocols Based on EIGRP, IS-IS and OSPF for Real Time Applications, Middle-East Journal of Scientific Research 12 (11): 1502-1508, 2012 ISSN 1990-9233.
[6] Lammle, Todd. (2011). Cisco Certified Network Associate Study Guide, Wiley Publishing, Inc., Seventh Edition.
[7] http://www.ehow.com
[8] Computer Networks by Andrew s Tenenbaum, 4th edition
[9] http://cisco.netacad.net

