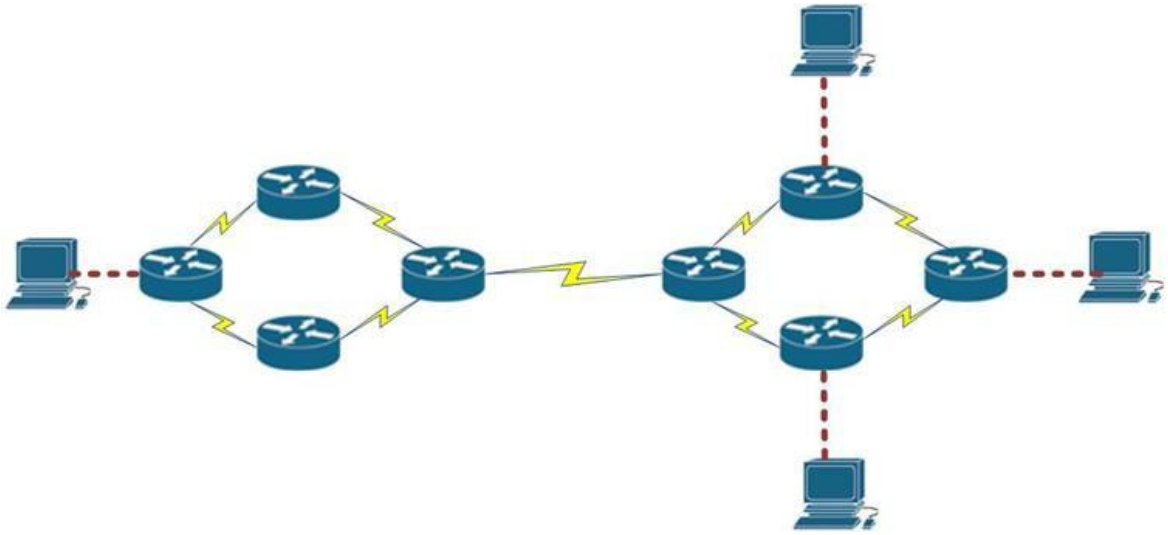
Dynamic routing protocols & Subnetting

Overview

In the previous chapter, we looked at static routing. We saw how the router finds the best path to a network. We configured static routes and traffic was able to flow between two points. In this chapter, we will give an overview of dynamic routing protocols. We will define them and learn how they are different from static routes. We will discuss their advantages over static routes, learn the different categories of dynamic routing protocols as well as classless and classful nature. We will also talk about the administrative distance and metric.

Consider the network diagram shown below.



The administrative overhead that would be needed to make communication between all these devices would be considerable. All the static routes would have to be configured.

Wouldn't it be much easier for the network administrator to just "Teach" the routers how to get from one point to another? The solution to this problem would be dynamic routing protocols. Dynamic routing protocols are a solution that is used in large networks so as to reduce the complexity in configuration that would be occasioned by having to configure static routes. In most networks, you will see a mix of both dynamic and static routes.

Definition of dynamic routing protocols

Routing protocols are used to enable the routers exchange routing information, they allow routers to learn about remotely connected networks dynamically. This information is then added to their routing tables as a basis for forwarding packets.

Classification

Dynamic routing protocols can be classified in several ways.

- Interior and exterior gateway routing protocols,
- Distance vector, path vector and link state routing protocols,
- Classful and classless.

The table below shows the various categories of dynamic routing protocols and the ones highlighted in **red**

will be the focus of this course. Others will be discussed at the CCNP and the CCIE level.

	Interior gateway protocols				**Exterior gateway protocols**
	Distance vector routing prote		***Link state routing protocols***		***Path vector routing protocol***
Classful	**RIPv1**	IGRP			EGP
classless	**RIPv2**	**EIGRP**	**OSPFv2**	IS-IS	BGPv4
IPv6	RIPng	EIGRP for IPv6	**OSPFv3**	IS-IS for IPv6	BGPv4 for IPv6

Operation of routing protocols

Now that we have an overview of routing protocols, we need to understand how they work. Routing protocols are comprised of processes, messages and algorithms that are used by routers to learn about remotely connected networks from routers that have been configured with the same routing protocols, the routes that have been learnt are added to the routing table and used as a basis for forwarding packets.

- Routing protocols function by:
- Discovering remote networks
- Maintaining current routing information

- Path determination

The routing protocol is made up of these components.

1. Data structures – this is information about remote networks. It is usually stored in the RAM and may be comprised of tables such as neighbor tables and topology tables.
2. Algorithm – this is the sequential list of steps that the routing takes when determining the best path to a particular network.
3. Routing protocol messages – these are messages that are used to maintain updated routing information. Examples include; hello messages, update messages among others.

The way routing protocols operate may differ depending on the routing protocol, however, there are certain characteristics inherent in every routing protocol.

- Exchange of information on interfaces to discover neighboring routers
- Exchange of routes that have been advertised
- Running of the algorithm so as to determine the best path
- Adding of best paths to the routing table
- Detection of topology changes and making the necessary changes

These are the general steps routers will take. However, the processes differ with each routing protocol and will be discussed at a later stage

Advantages

- Exchange of routing information when there is a topology change is dynamic.
- Less administrative overhead as compared to static routes which have to be manually configured
- Less error prone than static routing.
- Scalability, since there is less administrative overhead than static routes.

Disadvantages

- Require more expertise by the administrator, they are not as simple to configure as static routes.
- They use more of the routers resources; such as CPU and RAM.

Routing Information protocol:

RIP Overview The Routing InformationProtocol (RIP) Version 1 uses broadcast UDPdata packets, and RIPv2 uses multicast packets to exchange routing information. Cisco software sends routing information updates every 30 seconds, which is termed advertising. If a device does not receive an update from another device for 180 Routing Information Protocol 1 seconds or more, the receiving device marks the routes served by the non updating device as unusable. If there is still no update after 240 seconds, the device removes all routing table entries for the non updating device.

A device that is running RIP can receive a default network via an update from another device that is running RIP, or the device can source the default network using RIP. In both cases, the default network is advertised through RIP to other RIP neighbors. The Cisco implementation of RIP Version 2 (RIPv2) supports plain text and message digest algorithm 5 (MD5) authentication, route summarization, classless interdomain routing (CIDR), and variable-length subnet masks (VLSMs).

Router(config)#router rip	Enable RIP routing protocol
Router(config-router)# network a.b.c.d	Add a.b.c.d network in RIP routing advertisement
Router(config-router)# no network a.b.c.d	Remove a.b.c.d network from RIP routing advertisement
Router(config-router)# version 1	Enable RIP routing protocol version one (default)
Router(config-router)# version 2	Enable RIP routing protocol version two

Router(config-router)# no auto-summary	By default RIPv2 automatically summarize networks in their default classful boundary. This command will turn it off.

Router(config)#no router rip	Disable RIP routing protocol
Router#debug ip rip	Used for troubleshooting. Allow us to view all RIP related activity in real time.
Router#show ip rip database	Display RIP database including routes

Subnetting:

What is Subnet Mask?

If we recollect from the previous lessons, an IPv4 address has two components, the network part and the host part. Really, IPv4 address is a combination of IPv4 address and Subnet mask and the purpose of subnet mask is to identify which part of an IPv4 address is the network part and which part is the host part. Subnet mask is also a 32 bit number where all the bits of the network part are represented as "1" and all the bits of the host part are represented as "0".

If we take an example for a Class C network,192.168.10.0, the address part and the subnet mask can be represented as below.

Component	Binary	Decimal
Address Part	11000000.10101000.00001010.00000000	192.168.10.0
SN Mask	11111111.11111111.11111111.00000000	255.255.255.0

For a Class C IPv4 address,the first three octets are used to represent the Network part and the lact octet is used to represent the host part. From the above table, we can see all "1" in the network part and all "0" in nthe host part. When this subnet mask is converted to a decimals, it will become 255.2555.255.0. The default subnet mask for a Class C network is 255.255.255.0, Class B network is 255.255.0.0 and Class A networkis 255.0.0.0

What is a Network Address?

A network address is used to identify the subnet that a host may be placed on and is used to represent that network. We can find the network address by assigning all bits in the host part as 0.

What is Directed Broadcast?

The host id value containing all 1's in the bit pattern indicates a directed broadcast address. A directed broadcast address can occur in the destination IPv4 address of an IP datagram,but never as a source IPv4 address. A directed broadcast address will be seen by all nodes on that network. For example, the broadcast id for the network 192.168.10.0 will be 192.168.10.255.

A directed broadcast is sent to a specific network identified in the Network part of the IPv4 address. Routers on the network configured to forward-directed broadcasts will send the IP datagram to the final router that connects the destination specidied in the network part, and the router at the destination network should forward it to the destination host.

What is Limited Broadcast?

Limited broadcast is another type of broadcast, sent to destination IPv4 address of 255.255.255.255. The limited broadcast can be used in Local Area Networks (LAN),where a broadcast never crosses a router to reach another network. If a broadcast is to be done over the local network, you can use the limited broadcast. A limited broadcast address can never appear as a source IPv4 address; it can appear only as a destination IPv4 address

What is CIDR?

Classless Inter-Domain Routing (CIDR, RFC 1517,RFC 1518,RFC 1519,RFC 1520) was published in 1993 to keep the internet from running out of IPv4 addresses. The "classful" system of allocating IPv4 addresses can waste many IPv4 addresses.Any organization who need just a few IPv4 addresses more than 254 must get a Class B address block of 65533 IPv4 addresses.Even much more IPv4 addresses are wasted in the case of Class A,where total usable IPv4 addresses per network is 16777214 ((2^24) - 2).

The original "IPv4 Class A networks" uses 8 bits to represent the network part, "Class B networks" uses 16 bits to represent the network part and "Class C networks" uses 24 bits to represent the network part. CIDR replaced these categories with a more generalized network prefix. This network prefix could be of any length, not just 8, 16, or 24 bits.

For example; 172.16.120.213 255.255.128.0 can be represented in CIDR format as 172.16.120.213/17, because there are 17 bits used for network part.

Classless Inter-Domain Routing (CIDR) includes supernetting (supernetting is the method of using contiguous blocks of address spaces to simulate a single, larger, address space), VLSM (Variable Length Subnet Masking,a method of subnetting a subnet) and route aggregation (method representing multiple networks using a single entry in a router's routing table. This can greatly reduce the size of the routing tables in routers).

Class C Subnetting Tutorial

Subnetting is done by taking the bit/s from host part and adding it to the network part. Consider the same Class C example given above. Remember, the first three octets of a Class C network is used to represent the network and the last octet is used to represent the host. The default format for a Class C IPv4 addressis Network.Network.Network.Host.

To make things easy, you may remember this.

If all the bits in the host part are "0", that represents the network id.

If all the bits in the host part are "0" except the last bit, it is the first usable IPv4 address.

If all the bits in the host part are "1" except the last bit, it is the last usable IPv4 address.

If all the bits in the host part are "1", that represents the directed broadcast address.

All the IPv4 addresses between the first and last IPv4 addresses (including the first and last) can be used to configure the devices.

Class C - One Bit Subnetting Tutorial

Consider the network shown above. If we include one bit from the host part to the network part, the subnet mask is changed into 255.255.255.128. The single bit can have two values in last octet, either 0 or 1.

11000000.10101000.00001010.0 | 0000000

11111111.11111111.11111111.1 | 0000000

That means, we can get two subnets if we do a single bit subnetting.

SN No	Description	Binaries	Decimal

1	Network Address	11000000.10101000.00001010.00000000	192.168.10.0
	First IPv4 address	11000000.10101000.00001010.00000001	192.168.10.1
	Last IPv4 address	11000000.10101000.00001010.01111110	192.168.10.126
	Broadcast Address	11000000.10101000.00001010.01111111	192.168.10.127
2	Network Address	11000000.10101000.00001010.10000000	192.168.10.128
	First IPv4 address	11000000.10101000.00001010.10000001	192.168.10.129
	Last IPv4 address	11000000.10101000.00001010.11111110	192.168.10.254
	Broadcast Address	11000000.10101000.00001010.11111111	192.168.10.255

The network 192.168.10.0 is divided into two networks, each network has 128 total IPv4 addresses and 126 usable IPv4 addresses (two IPv4 addresses are used in each subnet to represent the network address and the directed broadcast address). The subnet mask for one bit subnetting is 255.255.255.128.

Class C - Two Bit Subnetting Tutorial

If we include two bits from the host part to the network part, the subnet mask is changed into 255.255.255.192. The two bits added to network part can have four possible values in last octet and that are 00, 01, 10 and 11. That means, we can get four networks if we do a two bit subnetting.

11000000.10101000.00001010.00 | 000000

11111111.11111111.11111111.11 | 000000

SN No	Description	Binaries	Decimal
1	Network Address	11000000.10101000.00001010.00000000	192.168.10.0
	First IPv4 address	11000000.10101000.00001010.00000001	192.168.10.1
	Last IPv4 address	11000000.10101000.00001010.00111110	192.168.10.62
	Broadcast Address	11000000.10101000.00001010.00111111	192.168.10.63
2	Network Address	11000000.10101000.00001010.01000000	192.168.10.64

	First IPv4 address	11000000.10101000.00001010.01000001	192.168.10.65
	Last IPv4 address	11000000.10101000.00001010.01111110	192.168.10.126
	Broadcast Address	11000000.10101000.00001010.01111111	192.168.10.127
3	Network Address	11000000.10101000.00001010.10000000	192.168.10.128
	First IPv4 address	11000000.10101000.00001010.10000001	192.168.10.129
	Last IPv4 address	11000000.10101000.00001010.10111110	192.168.10.190
	Broadcast Address	11000000.10101000.00001010.10111111	192.168.10.191
4	Network Address	11000000.10101000.00001010.11000000	192.168.10.192
	First IPv4 address	11000000.10101000.00001010.11000001	192.168.10.193
	Last IPv4 address	11000000.10101000.00001010.11111110	192.168.10.254
	Broadcast Address	11000000.10101000.00001010.11111111	192.168.10.255

The network 192.168.10.0 is divided into four networks, each network has 64 total IPv4 addresses and 62 usable IPv4 addresses (two IPv4 addresses are used in each subnet to represent the network address and the directed broadcast address). The subnet mask for two bit subnetting is 255.255.255.192.

Class C - 3 Bit Subnetting Tutorial

If we include three bits from the host part to the network part, the subnet mask is changed into 255.255.255.224. The three bits added to network part can have eight possible values in last octet and that are 000, 001, 010, 011, 100, 101, 110 and 111. That means, we can get eight networks if we do a three bit subnetting.

11000000.10101000.00001010.000 | 00000

11111111.11111111.11111111.111 | 00000