International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 3, March 2016

# Design and Implementation of secure communication between Two Branches of a company using IPSec protocol In CLI and GUI modes

S. Sri Priya[1], M.Vijaya Bhaskar Reddy[1], G. Sagar Reddy[1], G.Guru Prasad[1]
M.Lakshmi Narayana Reddy[2], B.Neelima[2]
[1]B.Tech IVth Year AITS-Tirupati, [2]Asst.Professor AITS-Tirupati

**Abstract**:

*Now a day's most of the corporate business network infrastructure needs to securely transfer data across the Internet. Data can be a company's top-secret information regarding product designs, product release dates, patent information, HR employee investigations, etc. This project provides insight for a secure solution to this business need using Virtual Private Network (VPN). There are a number of VPN protocols in use that secure the transport of data traffic over a public network infrastructure.*

*Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session[1]. IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to host). A virtual private network (VPN) is a technology for using the Internet or another intermediate network to connect computers to isolated remote computer networks that are inaccessible. A VPN provides security so that traffic sent through the VPN connection stays isolated from other computers on the intermediate network. VPNs can connect individual users to a remote network or connect multiple networks together. For example, a user may use a VPN to connect to their work computer terminal from home and access their email, files, images, etc.*

*Corporate migration to VPN connections across the Internet is beginning to become very attractive because of the tremendous cost savings. VPN remote users get the impression of being directly connected to the central network via a point-to-point link[1].*

**Keywords:** *Internet Protocol Security (IPSec), Internet Engineering Task Force (IETF), Virtual Private Network (VPN).*

## INTRODUCTION:

Network security consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator[2]. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done[3]. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password. Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming. To implement network security IPSec protocol is used.

### Command Line Interface (CLI):

A command line interface (CLI) enables users to type commands in a terminal or console window to interact with an operating system. Users respond to a visual prompt by typing a command on a specified line, and receive a response back from the system. Users type a command or series of commands for each task they want to perform.

### Graphical User Interfaces (GUI):

A graphical user interface (GUI) uses graphics, along with a keyboard and a mouse, to provide an easy-to-use interface to a program. A GUI provides windows, pull-down menus, buttons, scrollbars, iconic images, wizards, other icons, and the mouse to enable users to interact with the operating system or application.

### IPv4 - TCP/IP Model:

A majority of the internet uses a protocol suite called the Internet Protocol Suite also known as the TCP/IP protocol suite. This suite is a combination of protocols which encompasses a number of different protocols for different purpose and need. Because the two major protocols in this suite are TCP (Transmission Control Protocol) and IP (Internet Protocol), this is commonly termed as TCP/IP Protocol suite[4]. This protocol suite has its own reference model which it follows over the internet. In contrast with the OSI model, this model of protocols contains less layers. This model is indifferent to the actual hardware implementation, i.e. the physical layer of OSI Model. This is why this model can be implemented on almost all underlying technologies.

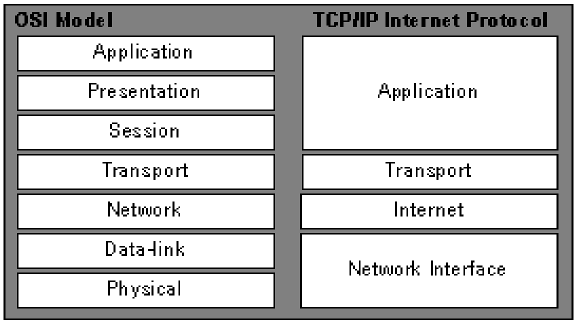


**Figure: Comparative depiction of OSI and TCP/IP Reference Models**

Transport and Internet layers correspond to the same peer layers. All three top layers of OSI Model are compressed together in single Application layer of TCP/IP Model.

### Internet Protocol Version 4 (IPv4):

Internet Protocol is one of the major protocols in the TCP/IP protocols suite. This protocol works at the network layer of the OSI model and at the Internet layer of the TCP/IP model[3]. Thus this protocol has the responsibility of identifying hosts based upon their logical addresses and to route data among them over the underlying network.

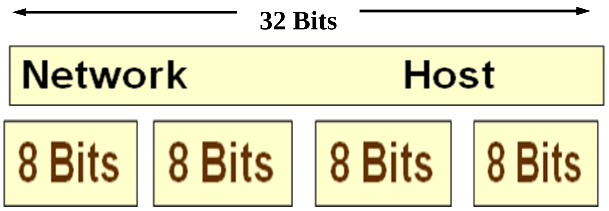
IP provides a mechanism to uniquely identify hosts by an IP addressing scheme. IP uses best effort delivery, i.e. it does not guarantee that packets would be delivered to the destined host, but it will do its best to reach the destination. Internet Protocol version 4 uses 32-bit logical address.

### Definition of IP address:

**Internet Protocol address** (**IP address**) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. Each host on a TCP/IP network is uniquely identified at the IP layer with an address. The IP address is also known as Protocol address. The IPv4 address is 32 bits long (2^32=4294967296)

### IPv4 Address Scheme:

What the Internet machines see an IP address? 110010100000011100100000000000000001. For human understanding the 32 bits of IP address are separated into 4 bytes of 8 binary digits .Each binary byte is converted into decimal and is separated by a dot hence also known as Dotted Decimal Notation How we see an IP address? 140.179.220.220



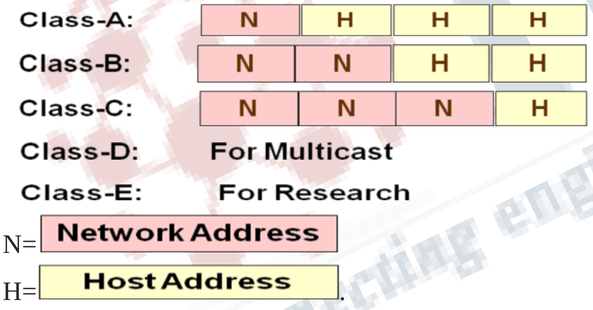
172 . 16 . 122 . 204

In decimal the address range is 0.0.0.0 to 255.255.255.255, The IP address is of the form <networkID, hostID>

**IP address classes:**

There are five classes of addresses A, B, C, D & E. A, B & C classes are used to represent host and network address. Class D is a special type of address used for multicasting. Class E is reserved for experimental use. Network ID '0' is not used. Network ID '127' is reserved for loop back and is used for internal testing.

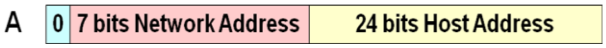
**IP address format is:**



## Identifying a class of address:

**Class A :**

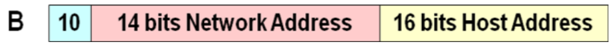
The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127, i.e.



Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks ($2^7$-2) and 16777214 hosts ($2^{24}$-2).

**Class B:**

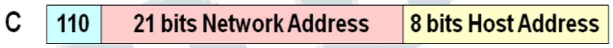
An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.



Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x. Class B has 16384 ($2^{14}$) Network addresses and 65534 ($2^{16}$-2) Host addresses.

**Class C:**

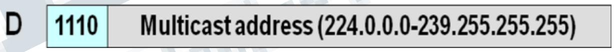
The first octet of Class C IP address has its first 3 bits set to 110, i.e.



Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x. Class C gives 2097152 ($2^{21}$) Network addresses and 254 ($2^8$-2) Host addresses.

**Class D:**

Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of:

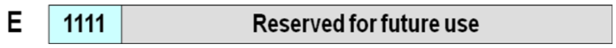


| Class | 1st Octet Decimal Range | 1st Octet High Order Bits |
|---|---|---|
| A | 1-126 | 0 |
| B | 128 – 191 | 10 |
| C | 192 – 223 | 110 |
| D | 224 – 239 | 1110 |
| E | 240 – 254 | 1111 |

Class D has IP address rage from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

**Class E :**

This IP Class is reserved for experimental purposes only for R&D or Study.



| | | |
|---|---|---|
| E | 1111 | Reserved for future use |

IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

Private networks can use IP addresses anywhere in the following ranges:

Class A- **10.0.0.0 to 10.255.255.255** (16,777,216 IP addresses)**;** Class B **- 172.16.0.0 to 172.31.255.255** (1,048,576 IP addresses)**;** Class C **- 192.168.0.0 to 192.168.255.255** (65,536 IP addresses)

## Routing:

Routing is the process of selecting best paths in a network. In the past, the term routing also meant forwarding network traffic among networks. However, that latter function is better described as forwarding**.**

### Static routing:

Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from a dynamic routing traffic.[1] In many cases, static routes are manually configured by a network administrator by adding in entries into a routing table, though this may not always be the case. Unlike dynamic routing, static routes are fixed and do not change if the network is changed or reconfigured. Static routing and dynamic routing are not mutually exclusive. Both dynamic routing and static routing are usually used on a router to maximise routing efficiency and to provide backups in the event that dynamic routing information fails to be exchanged. Static routing can also be used in stub networks, or to provide a gateway of last resort.

### Dynamic routing:

Dynamic routing, also called adaptive routing, describes the capability of a system, through which routes are characterized by their destination, to alter the path that the route takes through the system in response to a change in conditions. The adaptation is intended to allow as many routes as possible to remain valid (that is, have destinations that can be reached) in response to the change.

### Routing protocol:

A **routing protocol** specifies how **routers** communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. **Routing** algorithms determine the specific choice of route. Each **router** has a priori knowledge only of networks attached to it directly.

### Classifying Routing Protocols:

Routing protocols can be classified into different groups according to their characteristics. Specifically, routing protocols can be classified by their:

For example, IPv4 routing protocols are classified as follows:

- **RIPv1 (legacy)**: IGP, distance vector, classful protocol
- **IGRP (legacy)**: IGP, distance vector, classful protocol developed by Cisco (deprecated from 12.2 IOS and later)
- **RIPv2**: IGP, distance vector, classless protocol
- **EIGRP**: IGP, distance vector, classless protocol developed by Cisco
- **OSPF**: IGP, link-state, classless protocol
- **IS-IS**: IGP, link-state, classless protocol
- **BGP**: EGP, path-vector, classless protocol

The ***classful routing protocols***, RIPv1 and IGRP, are legacy protocols and are only used in older networks. These routing protocols have evolved into the ***classless routing protocols***, RIPv2 and EIGRP, respectively. Link-state routing protocols are classless by nature.

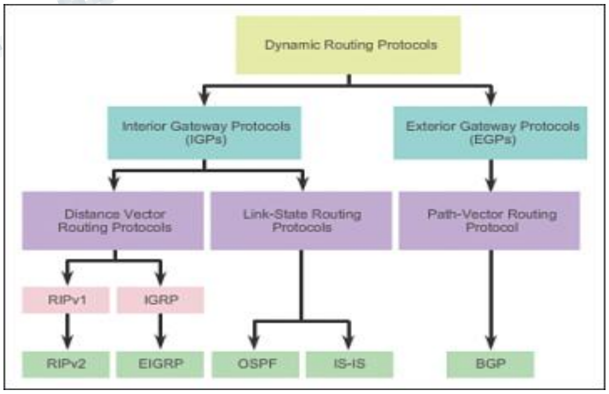

Dynamic Routing Protocols
Interior Gateway Protocols (IGPs)
Exterior Gateway Protocols (EGPs)
Distance Vector Routing Protocols
Link-State Routing Protocols
Path-Vector Routing Protocol
RIPv1
IGRP
RIPv2
EIGRP
OSPF
IS-IS
BGP

**Figure -1** Routing Protocol Classification

### IGP and EGP Routing Protocols:

An ***autonomous system (AS)*** is a collection of routers under a common administration such as a company or an organization. An AS is also known as a routing domain.

Typical examples of an AS are a company's internal network and an ISP's network.

The Internet is based on the AS concept; therefore, two types of routing protocols are required:

- ***Interior Gateway Protocols (IGP)***: Used for routing within an AS. It is also referred to as intra-AS routing. Companies, organizations, and even service providers use an IGP on their internal networks. IGPs include RIP, EIGRP, OSPF, and IS-IS.
- ***Exterior Gateway Protocols (EGP)***: Used for routing between autonomous systems. It is also referred to as inter-AS routing. Service providers and large companies may interconnect using an EGP. The Border Gateway Protocol (BGP) is the only currently viable EGP and is the official routing protocol used by the Internet.

The example in Figure-2 provides simple scenarios highlighting the deployment of IGPs, BGP, and static routing.

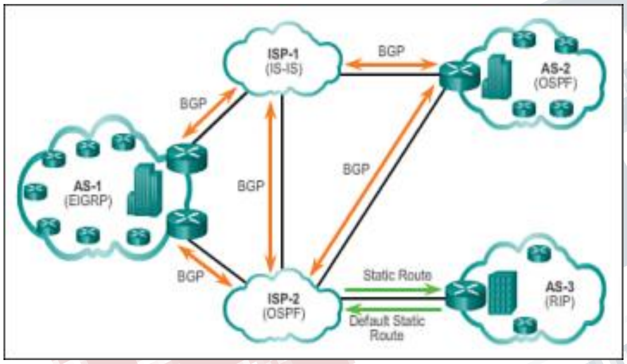


**Figure -2** IGP versus EGP Routing Protocols

There are five individual autonomous systems in the scenario:

- **ISP-1**: This is an AS and it uses IS-IS as the IGP. It interconnects with other autonomous systems and service providers using BGP to explicitly control how traffic is routed.
- **ISP-2**: This is an AS and it uses OSPF as the IGP. It interconnects with other autonomous systems and service providers using BGP to explicitly control how traffic is routed.
- **AS-1**: This is a large organization and it uses EIGRP as the IGP. Because it is multi homed (i.e., connects to two different service providers), it uses BGP to explicitly control how traffic enters and leaves the AS.
- **AS-2**: This is a medium-sized organization and it uses OSPF as the IGP. It is also multi homed; therefore, it uses BGP to explicitly control how traffic enters and leaves the AS.
- **AS-3**: This is a small organization with older routers within the AS; it uses RIP as the IGP. BGP is not required because it is single-homed (i.e., connects to one service provider). Instead, static routing is implemented between the AS and the service provider.

**Distance Vector Routing Protocols:**

Distance vector means that routes are advertised by providing two characteristics:

- **Distance**: Identifies how far it is to the destination network and is based on a metric such as the hop count, cost, bandwidth, delay, and more
- **Vector**: Specifies the direction of the next-hop router or exit interface to reach the destination

For example, in Figure 3, R1 knows that the distance to reach network 172.16.3.0/24 is one hop and that the direction is out of the interface Serial 0/0/0 toward R2.

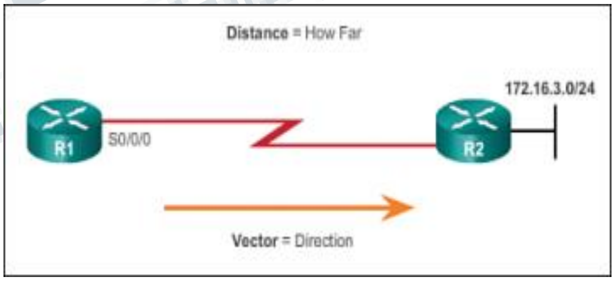


Figure 3: The Meaning of Distance Vector

A router using a ***distance vector routing protocol*** does not have the knowledge of the entire path to a destination network. Distance vector protocols use routers as sign posts along the path to the final destination. The only information a router knows about a remote network is the distance or metric to reach that network and which path or interface to use to get there. Distance vector routing protocols do not have an actual map of the network topology.

There are four distance vector IPv4 IGPs:

- **RIPv1**: First generation legacy protocol
- **RIPv2**: Simple distance vector routing protocol
- **IGRP**: First generation Cisco proprietary protocol (obsolete and replaced by EIGRP)
- **EIGRP**: Advanced version of distance vector routing

**Link-State Routing Protocols:**

In contrast to distance vector routing protocol operation, a router configured with a ***link-state routing protocol*** can create a complete view or topology of the network by gathering information from all of the other routers.

To continue our analogy of sign posts, using a link-state routing protocol is like having a complete map of the network topology. The sign posts along the way from source to destination are not necessary, because all link-state routers are using an identical map of the network. A link-state router uses the link-state information to create a topology map and to select the best path to all destination networks in the topology.

RIP-enabled routers send periodic updates of their routing information to their neighbours. Link-state routing protocols do not use periodic updates. After the network has converged, a link-state update is only sent when there is a change in the topology. For example, in Figure 4, the link-state update is sent when the 172.16.3.0 network goes down.

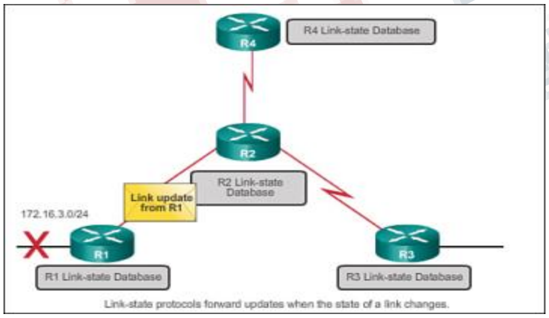


Figure 4: Link-State Protocol Operation

Link-state protocols work best in situations where:

- The network design is hierarchical, usually occurring in large networks
- Fast convergence of the network is crucial
- The administrators have good knowledge of the implemented link-state routing protocol

There are two link-state IPv4 IGPs:

- **OSPF**: Popular standards-based routing protocol
- **IS-IS**: Popular in provider networks

**Classful Routing Protocols:**

The biggest distinction between classful and classless routing protocols is that classful routing protocols do not send subnet mask information in their routing updates. Classless routing protocols include subnet mask information in the routing updates.

The two original IPv4 routing protocols developed were RIPv1 and IGRP. They were created when network addresses were allocated based on classes (i.e., class A, B, or C). At that time, a routing protocol did not need to include the subnet mask in the routing update, because the network mask could be determined based on the first octet of the network address.

To illustrate the shortcoming of classful routing, refer to the topology in Figure 5.

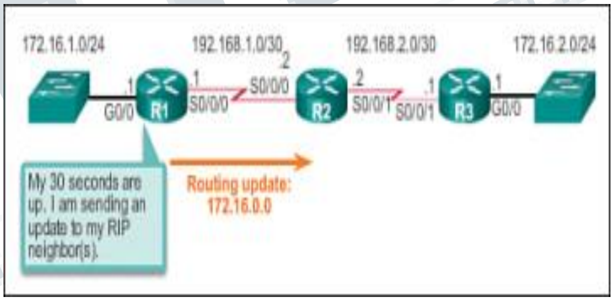
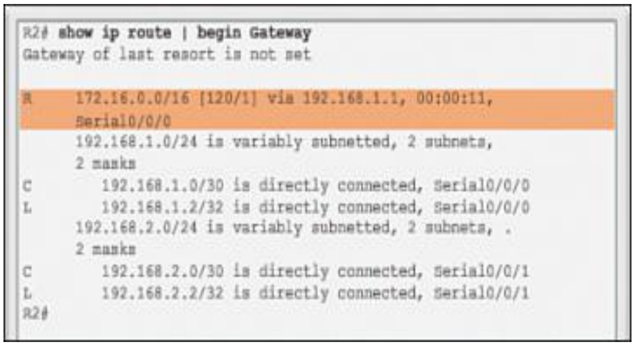


Figure 5: R1 Forwards a Classful Update to R2

Notice that the LANs of R1 (172.16.1.0/24) and R3 (172.16.2.0/24) are both subnets of the same class B network (172.16.0.0/16). They are separated by different classful network addresses (192.168.1.0/30 and 192.168.2.0/30). When R1 forwards an update to R2, RIPv1 does not include the subnet mask information with the update; it only forwards the class B network address 172.16.0.0. R2 receives and processes the update. It then creates and adds an entry for the class B 172.16.0.0/16 network in the routing table, as shown in Figure 6.



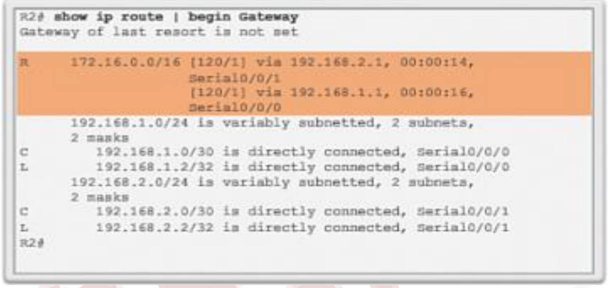
```
R2# show ip route | begin Gateway
Gateway of last resort is not set

R       172.16.0.0/16 [120/1] via 192.168.1.1, 00:00:11,
        Serial0/0/0
        192.168.1.0/24 is variably subnetted, 2 subnets,
        2 masks
C          192.168.1.0/30 is directly connected, Serial0/0/0
L          192.168.1.2/32 is directly connected, Serial0/0/0
        192.168.2.0/24 is variably subnetted, 2 subnets, .
        2 masks
C          192.168.2.0/30 is directly connected, Serial0/0/1
L          192.168.2.2/32 is directly connected, Serial0/0/1
R2#
```

Figure 6: R2 Adds the Entry for 172.16.0.0 via R1

When R3 forwards an update to R2, it also does not include the subnet mask information and therefore only forwards the classful network address 172.16.0.0.

R2 receives and processes the update and adds another entry for the classful network address 172.16.0.0/16 to its routing table, as shown in Figure 7. When there are two entries with identical metrics in the routing table, the router shares the load of the traffic equally among the two links. This is known as load balancing.



```
R2# show ip route | begin Gateway
Gateway of last resort is not set

R       172.16.0.0/16 [120/1] via 192.168.2.1, 00:00:14,
                      Serial0/0/1
                      [120/1] via 192.168.1.1, 00:00:16,
                      Serial0/0/0
        192.168.1.0/24 is variably subnetted, 2 subnets,
        2 masks
C          192.168.1.0/30 is directly connected, Serial0/0/0
L          192.168.1.2/32 is directly connected, Serial0/0/0
        192.168.2.0/24 is variably subnetted, 2 subnets,
        2 masks
C          192.168.2.0/30 is directly connected, Serial0/0/1
L          192.168.2.2/32 is directly connected, Serial0/0/1
R2#
```

Figure 7: R2 Adds the Entry for 172.16.0.0 via R3

Discontinuous networks have a negative impact on a network. For example, a ping to 172.16.1.1 would return "U.U.U" because R2 would forward the first ping out its Serial 0/0/1 interface toward R3, and R3 would return a Destination Unreachable (U) error code to R2. The second ping would exit out of R2's Serial 0/0/0 interface toward R1, and R1 would return a successful code (.). This pattern would continue until the **ping** command is done.

**Classless Routing Protocols:**

Modern networks no longer use classful IP addressing and the subnet mask cannot be determined by the value of the first octet. The classless IPv4 routing protocols (RIPv2, EIGRP, OSPF, and IS-IS) all include the subnet mask information with the network address in routing updates. Classless routing protocols support VLSM and CIDR.

IPv6 routing protocols are classless. The distinction whether a routing protocol is classful or classless typically only applies to IPv4 routing protocols. All IPv6 routing protocols are considered classless because they include the prefix-length with the IPv6 address.

Figures 9 through 11 Illustrate how classless routing solves the issues created with classful routing.

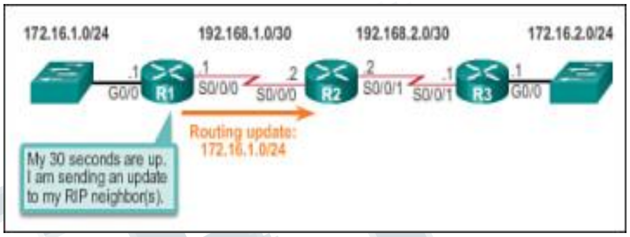
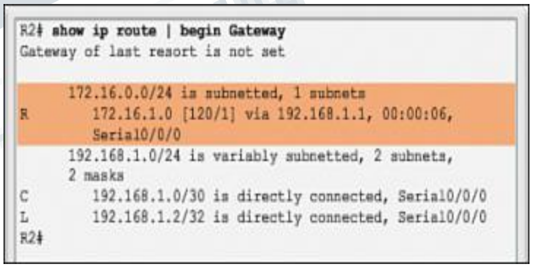


*Figure 8: R1 Forwards a Classless Update to R2*

In the *discontinuous network* design of Figure *9*, the classless protocol RIPv2 has been implemented on all three routers. When R1 forwards an update to R2, RIPv2 includes the subnet mask information with the update 172.16.1.0/24.

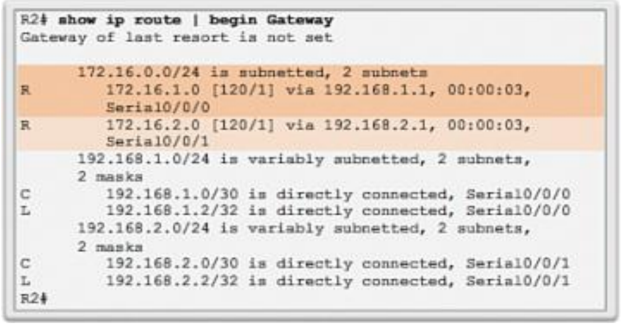


```
R2# show ip route | begin Gateway
Gateway of last resort is not set

        172.16.0.0/24 is subnetted, 1 subnets
R          172.16.1.0 [120/1] via 192.168.1.1, 00:00:06,
           Serial0/0/0
        192.168.1.0/24 is variably subnetted, 2 subnets,
        2 masks
C          192.168.1.0/30 is directly connected, Serial0/0/0
L          192.168.1.2/32 is directly connected, Serial0/0/0
R2#
```

Figure 9: R2 Adds the Entry for the 172.16.1.0/24 Network via R1

In Figure 10, R2 receives, processes, and adds two entries in the routing table. The first line displays the classful network address 172.16.0.0 with the /24 subnet mask of the update. This is known as the parent route. The second entry displays the VLSM network address 172.16.1.0 with the exit and next-hop address. This is referred to as the child route. Parent routes never include an exit interface or next-hop IP address.



```
R2# show ip route | begin Gateway
Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 2 subnets
R        172.16.1.0 [120/1] via 192.168.1.1, 00:00:03,
         Serial0/0/0
R        172.16.2.0 [120/1] via 192.168.2.1, 00:00:03,
         Serial0/0/1
      192.168.1.0/24 is variably subnetted, 2 subnets,
      2 masks
C        192.168.1.0/30 is directly connected, Serial0/0/0
L        192.168.1.2/32 is directly connected, Serial0/0/0
      192.168.2.0/24 is variably subnetted, 2 subnets,
      2 masks
C        192.168.2.0/30 is directly connected, Serial0/0/1
L        192.168.2.2/32 is directly connected, Serial0/0/1
R2#
```

Figure 10: Entry for the 172.16.2.0/24 Network via R3

When R3 forwards an update to R2, RIPv2 includes the subnet mask information with the update 172.16.2.0/24. R2 receives, processes, and adds another child route entry 172.16.2.0/24 under the parent route entry 172.16.0.0, as shown in Figure 11. A ping from R2 to 172.16.1.1 would now be successful.

## CONCLUSION:

In this Paper IPSec protocol is used to implement the security between two companies. Although there are different protocols can be used to implement it. Due to its various advantages it can used to transfer secure data

### FUTURE SCOPE:

Due to various advantages of IPSec protocol still there is a research is going to improve it so that used for further applications like military applications in which there is need to transfer data securely to communicate with military Systems.

### REFERENCES:

[1]. Munasinghe K. S. and Shahrestani S. A., "Evaluation of an IPSec VPN over a Wireless Infrastructure," in Proceedings of The Australian Telecommunication Networks and Applications Conference (ATNAC 2004), pp. 315-320, December 2004a.

[2]. TCP/IP Illustrated, Volume 1: The Protocols (2nd Edition) (Addison-Wesley Professional Computing Series) 2nd Edition

[3].The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference 1st Edition

[4]. Cisco TCP/IP Routing Professional Reference 3rd Edition

[5]. Routing Protocols Companion Guide Kindle Edition By Cisco Networking Academy.