

PROJECT A

Advance Network Analytics



July 17, 2022

Harshiit MAMGAIN

10137780

**Network design:**

Diagram

Description automatically generated

**IP table:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP adress** | **Subnet Mask** | **Default Gateway** |
| PC1 | f0/2 | 172.16.24.2 | 255.255.255.0 | 172.16.24.1 |
| PC2 | f0/3 | 172.16.32.2 | 255.255.255.0 | 172.16.32.1 |
| PC3 | f0/0 | 172.16.40.2 | 255.255.255.0 | 172.16.40.1 |
| PC4 | f0/0 | 172.16.56.2 | 255.255.255.0 | 172.16.56.1 |
| Switch0 | VLAN10 |  |  |  |
|  | VLAN20 |  |  |  |
| R1 | g0/0 | 172.16.58.2 | 255.255.255.0 |  |
|  | s0/1/0 | 204.225.107.45 | 255.255.255.252 |  |
|  | s0/1/1 | 172.16.8.1 | 255.255.255.0 |  |
|  | Tunnel 1 | 172.16.48.2 | 255.255.255.252 |  |
| R2 | g0/0 | 172.16.56.1 | 255.255.255.0 |  |
|  | s0/1/0 | 204.225.107.182 | 255.255.255.252 |  |
|  | Tunnel 1 | 172.16.48.1 | 255.255.255.252 |  |
| R3 | g0/0.10 | 172.16.24.1 | 255.255.255.0 |  |
|  | g0/0.20 | 172.16.32.1 | 255.255.255.0 |  |
|  | s0/1/1 | 172.16.16.1 | 255.255.255.0 |  |
|  | s0/0/0 | 172.16.8.1 | 255.255.255.0 |  |
| R4 | s0/0/0 | 172.16.16.2 | 255.255.255.0 |  |
| Internet | g0/0 | 172.16.40.1 | 255.255.255.0 |  |
| Firewall | gig1/1 | 172.16.58.1 | 255.255.255.0 |  |
|  | gig1/2 | 172.16.66.2 | 255.255.255.0 |  |
| Server | f0/0 | 172.16.66.1 | 255.255.255.0 |  |

**WEEK 1 – Configuration of RIPv2 and Inter VLAN**

**Packet Tracer file name: WEEK-1**

**RIPv2** is an enhancement of RIPv1's features. RIPv1 is Classful routing protocol and RIPv2 Classless routing protocol. The subnet masks are NOT included in the routing update and In RIPv2 Subnet masks are included in the routing update.

RIPv2 multicasts the entire routing table to all adjacent routers at the address 224.0.0.9, as opposed to RIPv1 which uses broadcast (255.255.255.255). Unicast addressing is still allowed for special applications.

**Inter-VLAN routing** is the process of forwarding network traffic from one VLAN to another VLAN

Configuration Screenshots:

R1:

Graphical user interface, text, application, email

Description automatically generated

R2:

Graphical user interface, text, application, email

Description automatically generated

R3:

Graphical user interface, text, application, email

Description automatically generated

R4:

Graphical user interface, text, application, email

Description automatically generated

Text

Description automatically generated

Switch:

Text, letter

Description automatically generated

Text, letter

Description automatically generated

Table

Description automatically generated

Inter VLAN Routing on R3:

Text

Description automatically generated

Configuring RIPv2 on R3:

Text, letter

Description automatically generated

Text, letter

Description automatically generated

Ping Successful:

PC1 to PC3 and PC1 to PC2.

Graphical user interface, text

Description automatically generated

**WEEK 2: OSPF, GRE Tunnelling and Point to Point Protocol Implementation**

**Packet Tracer file name: WEEK-2**

**Generic routing encapsulation (GRE)** is a virtual point to point link that encapsulates data traffic in a tunnel. The below topics discusses the tunnelling of GRE, encapsulation, and de-capsulation process, configuring GREs and verifying the working of GREs.

**OSPF (Open Shortest Path First)** protocol is one of a family of IP Routing protocols and is an Interior Gateway Protocol (IGP) for the Internet, used to distribute IP routing information throughout a single Autonomous System (AS) in an IP network.

The OSPF protocol is a link-state routing protocol, which means that the routers exchange topology information with their nearest neighbours. The topology information is flooded throughout the AS, so that every router within the AS has a complete picture of the topology of the AS. This picture is then used to calculate end-to-end paths through the AS, normally using a variant of the Dijkstra algorithm. Therefore, in a link-state routing protocol, the next hop address to which data is forwarded is determined by choosing the best end-to-end path to the eventual destination.

**Point - to - Point Protocol (PPP)** is a communication protocol of the data link layer that is used to transmit multiprotocol data between two directly connected (point-to-point) computers. It is a byte - oriented protocol that is widely used in broadband communications having heavy loads and high speeds.

The main services provided by Point - to - Point Protocol are:

* Defining the frame format of the data to be transmitted.
* Defining the procedure of establishing link between two points and exchange of data.
* Stating the method of encapsulation of network layer data in the frame.
* Stating authentication rules of the communicating devices.
* Providing address for network communication.
* Providing connections over multiple links.
* Supporting a variety of network layer protocols by providing a range os services.

Point - to - Point Protocol is a layered protocol having three components:

* Encapsulation Component − It encapsulates the datagram so that it can be transmitted over the specified physical layer.
* Link Control Protocol (LCP) − It is responsible for establishing, configuring, testing, maintaining, and terminating links for transmission. It also imparts negotiation for set up of options and use of features by the two endpoints of the links.
* Authentication Protocols (AP) − These protocols authenticate endpoints for use of services. The two authentication protocols of PPP are –

1. Password Authentication Protocol (PAP)
2. Challenge Handshake Authentication Protocol (CHAP)

Configuration Screenshots:

Firewall:

Text

Description automatically generated

R1:

Text

Description automatically generated

Text, letter

Description automatically generated

Text

Description automatically generated with medium confidence

Internet:

Text

Description automatically generated

R2:

Text

Description automatically generated

Configuring GRE Tunnel:

R1:

Text, letter

Description automatically generated

R2:

Text, letter

Description automatically generated

PPP Implementation:

R1:

Text, letter

Description automatically generated

R2:

Text, letter

Description automatically generated

Applying OSPF protocol:

R1:

Text, letter

Description automatically generated

R2:



**WEEK 3:**

* **Setting up the firewall with DHCP, NAT and conduit**
* **Setup HTTP/FTP services on the servers**

**Dynamic Host Configuration Protocol (DHCP)** is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

**NAT** stands for network address translation. It’s a way to map multiple local private addresses to a public one before transferring the information. Organizations that want multiple devices to employ a single IP address use NAT.

There are three different types of NATs. People use them for different reasons, but they all still work as a NAT:

* Static NAT

When the local address is converted to a public one, this NAT chooses the same one. This means there will be a consistent public IP address associated with that router or NAT device.

* Dynamic NAT

Instead of choosing the same IP address every time, this NAT goes through a pool of public IP addresses. This results in the router or NAT device getting a different address each time the router translates the local address to a public address.

* PAT

PAT stands for port address translation. It’s a type of dynamic NAT, but it bands several local IP addresses to a singular public one. Organizations that want all their employees’ activity to use a singular IP address use a PAT, often under the supervision of a [network administrator](https://www.comptia.org/blog/your-next-move-network-administrator).

Inside and Outside Configurations on Firewall:

Text

Description automatically generated

Applying DHCP:



Verify DHCP request:

Graphical user interface, application

Description automatically generated

OSPF Configuration on R1:

Text

Description automatically generated with medium confidence

NAT:

Text

Description automatically generated with medium confidence

FTP:

Graphical user interface

Description automatically generated

HTTP:

Graphical user interface, table

Description automatically generated with medium confidence

**WEEK 4: Inter-domain IP route redistributions and testing inter-domain access**

**Packet Tracer File: WEEK-4**

**Redistribution:** The use of a routing protocol to advertise routes that are learned by some other means, such as by another routing protocol, static routes, or directly connected routes, is called redistribution. While running a single routing protocol throughout your entire IP internetwork is desirable, multi-protocol routing is common for several reasons, such as company mergers, multiple departments managed by multiple network administrators, and multi-vendor environments. Running different routing protocols is often part of a network design. In any case, having a multiple protocol environment makes redistribution a necessity.

Differences in routing protocol characteristics, such as metrics, administrative distance, classful and classless capabilities can affect redistribution. Consideration must be given to these differences for redistribution to succeed.

Configuring Redistribution on R3 and R1:

Text

Description automatically generated

Text, letter

Description automatically generated

**Analysis Tasks:**

1. **Analyze the GRE Tunneling**:

Tunneling is the process of wrapping packets inside of other packets. Typically, two routers are used to configure GRE tunnels, with each router serving as one end of the tunnel. The routers are set up to send and receive GRE packets directly to each other. Any routers in between those two routers will only refer to the headers surrounding the encapsulated packets in order to forward them; they won't open the packets.

Although GRE is not the only tunnelling technique, it does have some benefits over some other approaches such as:

1. It can be supported by any vendor because it is defined in RFC2784. Additionally, because it accepts multicast packets, it can be used with dynamic routing systems (unlike IPSec tunnels for example).
2. GRE is also relatively simple to configure and is lightweight because it lacks built-in encryption. It is simple to add an additional layer of IPSec to the tunnel if encryption is required. In doing so, the benefits of IPSec and GRE are combined.
3. GRE tunnels encase multiple protocols over a single-protocol backbone.
4. They provide workarounds for networks with limited hops.
5. They connect discontinuous sub-networks and allow VPNs across wide area networks (WANs).

**Disadvantage of GRE tunneling**:

The main disadvantage of GRE tunneling is that it does not support data encryption. Because of this, the network security cannot be ensured.

To offer network security, it must be combined with other secure tunnelling protocols like IPSec. Due to the manual nature of defining GRE tunnels, the GRE protocol is less scalable.

1. **Analyze the OSPF protocol:**

The OSPF (Open Shortest Path First) protocol is a link-state routing protocol, which means that the routers exchange topology information with their nearest neighbors. Every router in the AS has access to the topology data, giving every router in the AS a complete understanding of the topology of the AS. The end-to-end pathways through the AS are then calculated using this image, typically using a Dijkstra algorithm version. In a link-state routing system, the optimal end-to-end path to the final location is chosen to identify the next hop address to which data is passed.

Large enterprise networks that employ routing apparatus from many suppliers frequently employ OSPF. Additionally, OSPF is employed in businesses that have a policy of using an open standard protocol for routing since it allows them flexibility when they need to add or replace routers.

**Advantage of OSPF protocol:**

1. The fundamental benefit of a link state routing protocol like OSPF is that it enables routers to calculate routes that meet specific requirements since they have comprehensive topology knowledge. This is beneficial for traffic engineering since it allows routes to be restricted to satisfy specific quality of service standards.
2. It is based on an open standard. It can run on most routers.
3. It uses the SPF algorithm to provide a loop-free topology.
4. It uses both trigger updates and incremental updates to provide fast convergence.
5. It supports VLSM and route summarization for a hierarchical design.
6. It supports both versions of IP protocol. OSPFv2 supports IPv4 and OSPFv3 supports IPv6.
7. It supports load balancing with equal-cost routes for the same destination.
8. It supports networks of all sizes.

**Disadvantage of OSPF protocol**

1. A link state routing protocol's key drawback is that it struggles to grow as more routers are added to the routing domain. The quantity and frequency of topology changes, as well as the time it takes to generate end-to-end routes, grow as the number of routers increases. IGPs only route traffic within a single AS because link state routing protocols lack the scale necessary for routing over the entire Internet.
2. It needs lots of information to calculate the best route for each destination. To store this information, OSPF consumes more memory than other routing protocols.
3. To calculate the best route, it runs the SPF algorithm that requires extra CPU processing.
4. It is complex to configure and difficult to troubleshoot. In a large network, only experienced network administrators can configure it.
5. **Analyze the RIPv2 Protocol**

***Routing Information Protocol (RIP):***

In an autonomous system, the Routing Information Protocol (RIP) protocol is the intradomain (interior) routing protocol that is based on distance vector routing. Nodes are routers and network connections. The destination address appears in the routing table's first column. The hop count, or number of networks that must be passed in order to reach the target, is the cost of measure in this protocol. In this case, since infinity is specified by a fixed number of 16, a network using a rip cannot have more than 15 hops.

***RIP Version 2:***

In 1993, RIP version 2 was created because of various shortcomings in the original RIP specification. It can transmit subnet information and enables classless inter-domain routing (CIDR). Its metric is also hop count, and its maximum hop count of 15 is same to that of rip version 1. Subnetting, multicasting, and authentication are all supported. Every router has an auto summary feature. Subnet masks are part of the routing update in RIPv2. As opposed to RIPv1, which employs broadcast, RIPv2 multicasts the whole routing table to all nearby routers at the address 224.0.0.9. (255.255.255.255).

**Advantages of RIPv2:**

1. It’s a standardized protocol.
2. It’s VLSM compliant.
3. Provides fast convergence.
4. It sends triggered updates when the network changes.
5. Works with snapshot routing – making it ideal for dial networks.

**Disadvantage of RIPv2:**

1. Max hop count of 15, due to the ‘count-to-infinity’ vulnerability.
2. No concept of neighbors.
3. Exchanges entire table with all neighbours every 30 seconds (except in the case of a triggered update).
4. **Analyze the security options**

A firewall is a type of network security device that keeps track of incoming and outgoing network traffic and makes decisions about which traffic to allow or deny in accordance with a set of security rules. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet. A firewall can be hardware, software, or both.

Firewall keeps track of attempts to access your operating system and stops unwanted or unknown activity. A firewall acts as a traffic guard at the port, or entrance point, of your computer. Only reputable IP addresses or sources are permitted. In the same way that your postal address indicates where you live, IP addresses are significant since they identify a machine or source.

Types of Firewalls:

1. *Pocket Filtering Firewalls*

A management tool called a packet-filtering firewall can stop network traffic using the IP protocol, an IP address, and a port number. This kind of firewall is designed for smaller networks and offers the most fundamental level of security.

1. *Proxy Service Firewalls:*

By filtering communications at the application layer, the proxy service firewall is a solution that can help to safeguard the security of your network. In essence, it acts as a bridge or middleman between your internal network and external web servers. It is more secure because it employs stateful and deep packet inspection technology to examine incoming traffic. This firewall is sometimes referred to as a gateway firewall.

1. *Stateful multi-layer inspection (SMLI) firewalls*

The stateful multi-layer inspection firewall monitors connections that have already been made and provides basic firewall features. In addition to administrator-defined rules and context, it filters traffic based on state, port, and protocol. Data from previous connections as well as packets from the current connection are used in this.

1. *Unified threat management (UTM) firewalls*

A programme known as a unified threat management firewall combines the SMLI firewall's capabilities with intrusion prevention and antivirus. The UTM umbrella of services may also cover other services like cloud management.

1. *Next-generation firewalls (NGFW)*

Next-generation firewalls are more advanced than stateful inspection and packet filtering firewalls. They offer higher degrees of security by doing full packet inspection in addition to the usual packet filtering. This entails looking into a packet's contents and source in addition to its header. Advanced malware can be blocked by NGFW, which can handle increasingly complex and changing security threats.

1. *Network address translation (NAT) firewalls*

Internet traffic can be analysed by a NAT firewall, and unwanted communications can be stopped. It only permits inbound web traffic, in other words, if a device on your private network requested it.

1. *Virtual firewalls*

A virtual firewall is an appliance used in a cloud-based system, both private and public. This type of firewall is used to assess and manage internet traffic over both physical and virtual networks.

**Advantages of Firewall**

**1. Monitor Traffic**

Monitoring the traffic that passes through a firewall is one of its main responsibilities. Any data passing over a network is done so in the form of packets. Each of these packets is examined by the firewall for potential dangers. If the firewall by chance discovers them, it will stop them right away.

**2. Protection against Trojans**

Trojan-type malware is very harmful for users. A Trojan horse lurks on your computer, quietly watching everything you do on it. Whatever data they collect will be transmitted to a web server. Of course, you won't be aware of their presence until your machine starts acting strangely. In this case, a firewall will instantly stop Trojans before they can harm your system.

**3. Prevent Hackers**

Internet hackers are always looking for machines to use for their illicit purposes. When hackers come upon such machines, they begin to engage in even more nefarious actions, such spreading malware. In addition to such hackers, there may be other unidentified individuals searching for an open internet connection, including the neighbours. Therefore, having firewall protection is a smart concept in order to stop such invasions.

**4. Access Control**

A firewall's access policy can be applied to particular hosts and services. The attackers' ability to exploit some hosts is available. Therefore, it is best to prevent such hosts from using the system. This access policy can be applied if a user feels that they need to be protected from these kinds of unauthorised access.

**5. Better Privacy**

One of a user's main concerns is privacy. Hackers are continually on the lookout for privacy information to gather user-related information. However, a firewall can be used to restrict several of a website's services, including the domain name service and the finger. Therefore, the hackers have no prospect of obtaining private information. Firewalls can also prevent access to the site system's DNS information. As a result, the attackers won't be able to see the names or the IP address.

**Disadvantages of Firewall:**

**1.**      **Cost**

Depending on the kind, firewalls do require an investment. Generally speaking, hardware firewalls cost more than software firewalls. Hardware firewalls also need to be installed and maintained, which can be expensive. Without the assistance of a skilled IT professional, these setups cannot be made. When compared to a software firewall, there isn't much investment required, and the deployment is simple enough for the typical user.

**2.**      **User Restriction:**

Without a doubt, firewalls stop illegal network access to your machine. While the typical user may benefit from this, huge companies may find it to be a problem. The firewall's policies must be stringent enough to bar personnel from performing particular tasks. This could have a significant impact on the company's overall productivity. Employees may occasionally be discouraged from employing backdoor attacks as a result. However, since the data transmitted through these backdoor attacks is not thoroughly analysed, this may cause security issues.

3.      **Performance**:

Firewalls, particularly those that are software-based, have the potential to reduce the overall performance of your computer. The computer's total performance is determined by a number of elements, including the processing speed and RAM capacity. Software firewalls use more processing and RAM resources when they are continuously running in the background. This can result in decreased system performance. Hardware firewalls, however, don't affect system performance because they don't use computer resources.

**4.**      **Malware Attacks**

Although firewalls are able to stop the most common types of trojans, it has been shown that they are powerless against other varieties of malware. These virus varieties can infiltrate your system by taking the form of reliable data. Therefore, having an anti-malware programme installed on your computer is still advised even if you have a firewall. since an anti-malware scan is the only way to get rid of them.

**5.**       **Complex Operations**

Although firewall maintenance is simple for small enterprises, it is undoubtedly difficult for huge organisations. Large enterprises need a distinct team to manage their firewalls. These individuals guarantee that the firewall is secure enough to keep outsiders out of the network.

**CONCLUSION:**

**On completion of Project, I have come out with a better understanding of OSPF, RIPv2 and Inter VLAN routing configurations. Critical knowledge of GRE tunneling and implementing Firewall security protocols.**

**References:**

1. <https://www.hitechwhizz.com/2020/03/5-advantages-and-disadvantages-drawbacks-benefits-of-firewall.html>

2. <https://www.cloudflare.com/en-ca/learning/network-layer/what-is-gre-tunneling/>

3. <https://www.orbit-computer-solutions.com/ripv2/>

4. <https://www.metaswitch.com/knowledge-center/reference/what-is-open-shortest-path-first-ospf>

5.<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-16/iro-xe-16-book/iro-cfg.html>