

Unidad de datos de protocolo.

Cáceres Pinzón Brian Sebastian, Rodriguez Gelves Sebastian Camilo.
{est.brian.caceres,est.sebastianc.rod2}@unimilitar.edu.co

Profesor David Martinez.

Resumen—En este documento se realiza el análisis de una simulación en cisco packet tracer donde se envían unidades de datos entre computadores y se busca entender estos protocolos de comunicación.

Palabras Claves- Pdu, Pc, Servidor, Red, Host.

I. INTRODUCCIÓN.

II. Trabajo previo

¿Qué es OSI?

OSI es una abreviatura de Open Systems Interconnection. A principios del 80, personas en varios comités de normalización en todo el mundo consideraron que había llegado el momento de desarrollar un conjunto de protocolos estándar. Esperan que algún día estos protocolos sustituyan la mayoría de las especificaciones dependientes del proveedor y que esto hará que la manera gratuita para una comunicación informática mundial sea fácil y flexible. Eso tomó casi una década antes de que se produjeran los primeros resultados: una modelo de referencia y un conjunto de estándares de capa de cable físico definiciones hasta bases de datos distribuidas y sistemas de información, junto con herramientas de gestión y seguridad. El proceso de estandarización aún no se ha terminado y probablemente no estará en el la próxima década, pero ya tenemos un poderoso conjunto de protocolos para las aplicaciones más importantes. Estas especificaciones han sido publicadas según las normas ISO y las recomendaciones del CCITT.

¿Cuál es el modelo de referencia OSI?

Un buen estándar internacional debe ser flexible y extensible. Para lograr este objetivo, parece una buena idea separar una estructura compleja como un protocolo de computadora en varios módulos.

Cada Módulo debe ser de tamaño manejable y, si se utilizan diferentes técnicas disponible para un cierto aspecto de un protocolo, luego la separación en los módulos hacen que sea bastante fácil cambiar esta parte de todo el sistema.(por ejemplo, la especificación del cable o la codificación de datos) sin tocar el resto de la especificación.

El modelo de referencia OSI (RM) definido en ISO 7498 divide el proceso de comunicación entre dos programas de aplicación en 7 capas intermedias. Cada capa proporciona un cierto tipo de servicio a la siguiente capa superior.

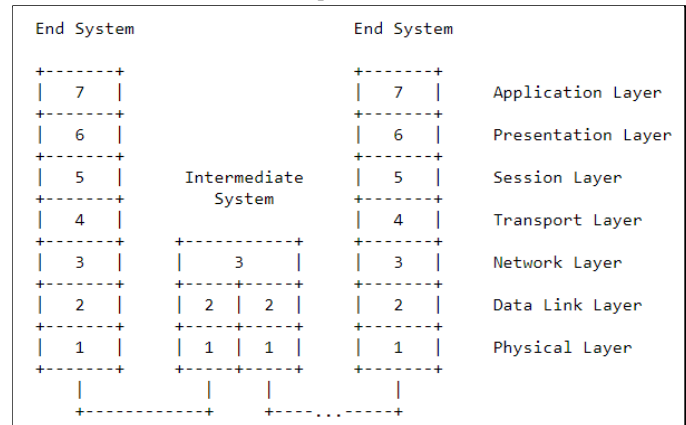
Este servicio se proporciona comunicándose con la entidad par en la misma capa del host remoto que usa el servicio proporcionada por la siguiente capa inferior. Algunas de las entidades de capa pueden ser implementadas en dispositivos físicos, algunos pueden ser parte de la operación sistema y algunos pueden estar incluidos en programas de aplicación.

La mayoría de las capas proporciona su servicio reenviando unidades de datos de protocolo al siguiente capa junto con un encabezado agregado o eliminado o realizando otras funciones y cambios de estado.

El modelo de referencia OSI solo define la noción abstracta de capas y no especifica si los límites entre las capas deben ser visibles y documentados en implementaciones.

Hay otros estándares que definen las interfaces del programa de

aplicación (API) entre los el sistema y la aplicación y estas API a menudo corresponden a una capa límite en el modelo de referencia OSI.El diagrama estándar clásico que se usa normalmente para describir el OSIRM tiene este aspecto:



¿Qué es ASN.1?

La mayoría de los protocolos se definen como conjuntos de unidades de datos de protocolo (PDU) que podrían intercambiarse entre dos hosts. Una PDU es una secuencia de bytes que un anfitrión usa para decirle al otro algo de acuerdo con las reglas del protocolo. Muy temprano en el proyecto OSI, se reconoció que se necesitaba una forma formal de definir la sintaxis de las PDU, es decir, algo como las conocidas gramáticas Backus-Naur sin contexto (BNF) se utilizan para definir la sintaxis de los lenguajes de programación. ASN.1 (sintaxis abstracta anotación número 1) juega el mismo papel en la definición de protocolos OSI que BNF juega en la definición de un lenguaje de programación: da una Especificación precisa y analizable cómo se estructuran las PDU y qué se permiten estructuras, pero no dice nada sobre el significado de una PDU. Esto todavía está definido en idioma inglés en los estándares OSI.

Un ejemplo de ello es:

```
NonsenseProtocol ::= CHOICE {
    testPDU [0] TestPDU, -- Our example
    getFile [1] GetFile -- another possible PDU
}
```

```
TestPDU ::= SEQUENCE {
    aNumber INTEGER,
    anotherNumber INTEGER,
    today UTCTime OPTIONAL,
    theText CHOICE {
        multilingualText ISO10646String,
        standardText VisibleString
    }
}
```

¿Qué estándares OSI existen?

Como dos organizaciones (ISO e ITU) han estado involucradas en el OSI proceso de estandarización, muchas de las especificaciones han sido publicadas como normas ISO y recomendaciones del CCITT (CCITT en el futuro, las recomendaciones se denominará recomendaciones del UIT-T).En estos casos, ambas versiones están "técnicamente alineadas" o una versiones un subconjunto del otro.El modelo de referencia OSI, como se define en ISO 7498-1 y CCITT

a recomendación X.200 describe los detalles del modelo de siete capas. Las otras tres partes de ISO 7498 describen la arquitectura de seguridad, Denominación y direccionamiento y marco de gestión. Los métodos de descripción de protocolos formales se definen en ISO 8807 (LOTOS, Lenguaje de especificación y ordenamiento temporal), ISO 9074 (ESTELLE) e ISO 9496 (CHILL). ISO 9646 estandariza los métodos de conformidad pruebas, p. ej. la notación combinada de árbol y tabular (TTCN) para la prueba suites. ISO TR 10167 (Directrices de aplicación para ESTELLE, LOTOS y SDL) incluye una serie de ejemplos de sistemas, mostrando cómo cada uno de ellos puede especificarse utilizando estos tres estándares.

¿Cómo se relacionan OSI y TCP / IP?

TCP / IP es un conjunto de protocolos que ha sido desarrollado por los EE. UU. Departamento de Defensa y que se utilizan en Internet. Software del soporte de TCP / IP es parte de casi todas las distribuciones de UNIX en la actualidad.

TCP / IP no es un protocolo OSI y no encaja en la referencia OSI modelo. Sin embargo, el servicio proporcionado por IP es muy similar al servicio de red sin conexión proporcionado por CLNP, por lo que IP es generalmente llamado protocolo de capa 3. De manera similar, TCP se puede comparar con TP4 y puede verse como un protocolo de capa 4 en el modelo de referencia.

Las principales diferencias son el espacio de direcciones, que es una secuencia de 4 bytes. en IP y hasta 20 bytes en OSI, y el hecho de que TCP es un protocolo orientado a la transmisión que no proporciona ninguna unidad de datos de protocolo límites. Otros detalles son algunas características que faltan en TCP / IP como negociación de calidad de servicio y restricciones de enrutamiento.

¿Qué es mejor: TCP / IP y OSI?

Ninguno de los dos. En teoría, OSI tiene el conjunto de características más avanzadas, incluyendo protocolos de aplicación significativamente más sofisticados incluidos algunos para servicios que no están disponibles en absoluto en la suite TCP / IP.

En la práctica, TCP / IP se implementa y despliega mucho más ampliamente, por lo que es mucho más probable que encuentre productos TCP / IP que se adapten a sus necesidades, y normalmente a precios mucho más bajos que los productos OSI equivalentes.

III. Desarrollo de la práctica.

1. Realizar una simulación de envío y recepción sencilla y compleja en 2 redes interconectadas entre sí y un server

Se configuró una red con varios computadores como se observa a continuación, esta cuenta con 5 hosts los cuales son 4 pc's y un servidor, dos de los computadores están conectados por medio de un switch de igual forma los otros dos computadores y el servidor.

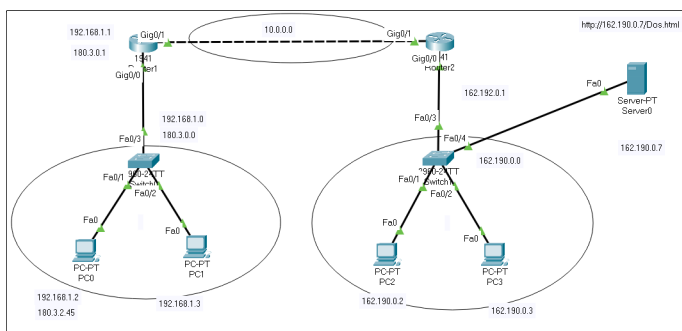


Figura 1. Esquema utilizado.

Se configuran los pcs y se les asigna una ip estática la cual es única para cada host, también se configura la máscara de red, que depende claramente del tipo de red.

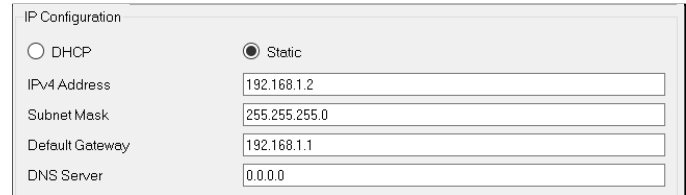


Figura 2. Configuración de host.

Para los routers se configuran las redes lan con las cuales interactúa el router estas son con otros routers y con el switch.

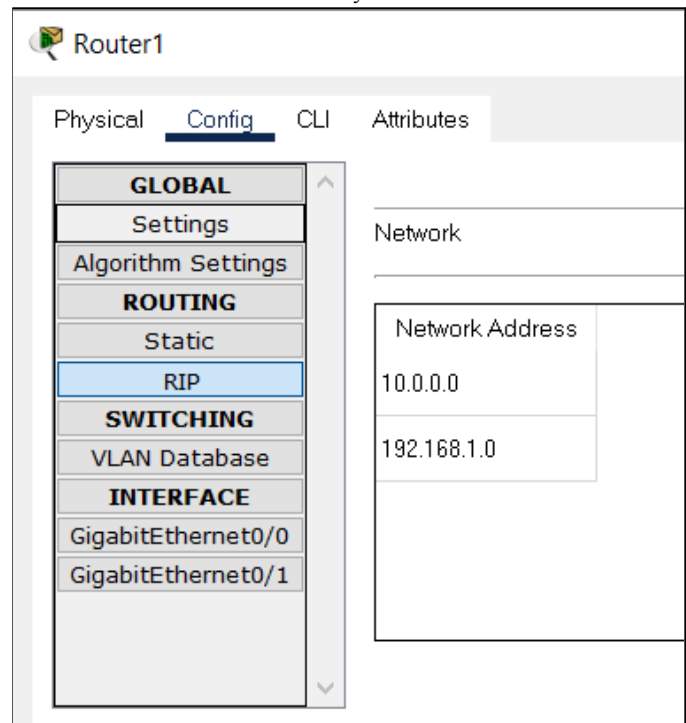


Figura 3. Configuración de los routers.

Se configura la red lan con el switch.

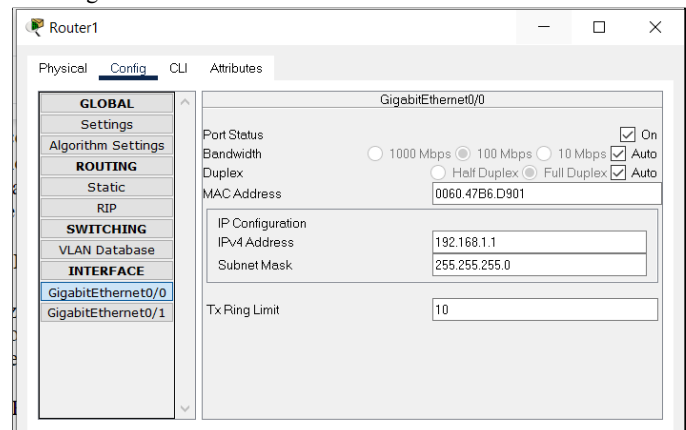


Figura 4. Configuración del router con switch.

Configuración red con el router.

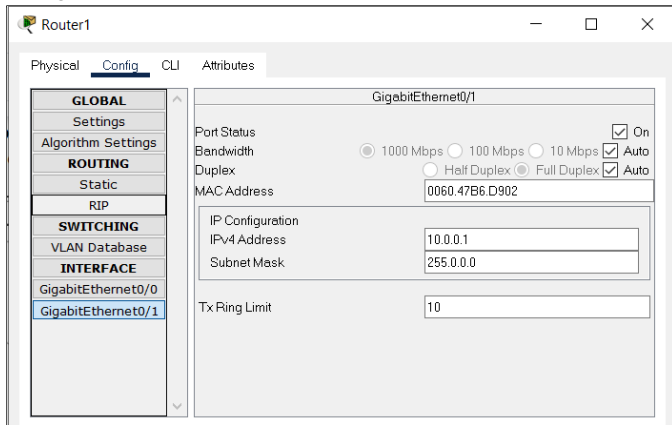


Figura 5. Configuración del router con routers.

Se configura el servidor, para el cual se le asigna una dirección ip.

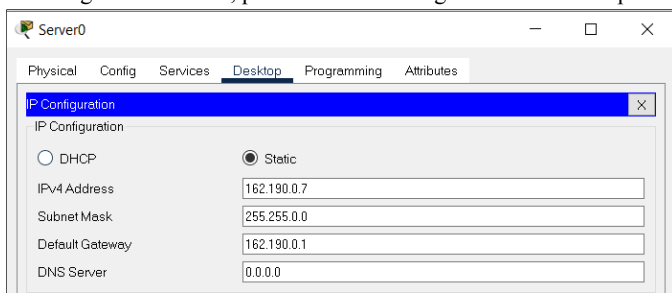


Figura 6. Configuración del servidor ip.

Se añade un servicio HTTPS para acceder desde un navegador en un host.

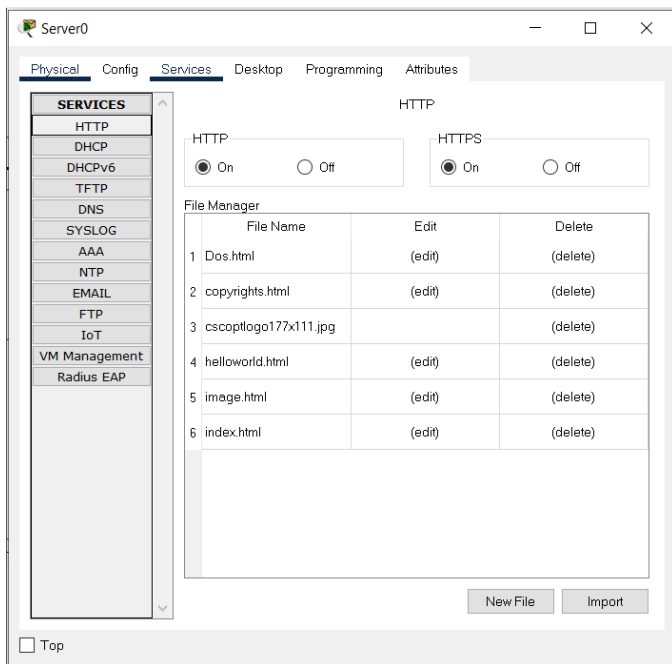


Figura 7. Configuración del servidor HTTPS.

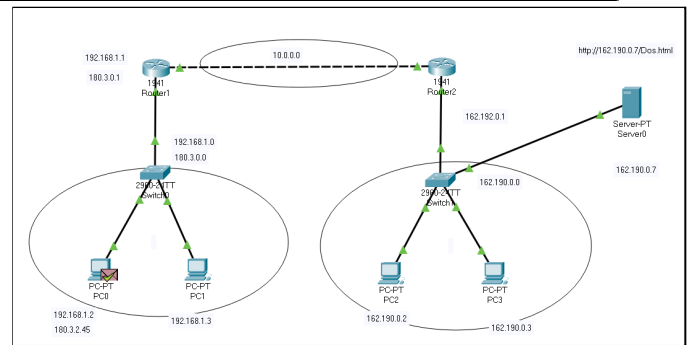


Figura 8. Esquema con mensaje completado.

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	—	PC0	ICMP
	0.001	PC0	Switch0	ICMP
	0.003	Switch0	Router1	ICMP
	0.006	Router1	Router2	ICMP
	0.007	Router2	Switch1	ICMP
	0.009	Switch1	PC3	ICMP
	0.011	PC3	Switch1	ICMP
	0.013	Switch1	Router2	ICMP
	0.015	Router2	Router1	ICMP
	0.018	Router1	Switch0	ICMP
	0.020	Switch0	PC0	ICMP

Figura 9. PDU simple.

PDU información, paso a paso:

En Time 0.000 en PC0 :

1. The Ping process starts the next ping request.
2. The Ping process creates an ICMP Echo Request message and sends it to the lower process.
3. The source IP address is not specified. The device sets it to the port's IP address.
4. The device sets TTL in the packet header.
5. The destination IP address 162.190.0.3 is not in the same subnet and is not the broadcast address.
6. The default gateway is set. The device sets the next-hop to default gateway.

1. The next-hop IP address is a unicast. The ARP process looks it up in the ARP table.
2. The next-hop IP address is in the ARP table. The ARP process sets the frame's destination MAC address to the one found in the table.
3. The device encapsulates the PDU into an Ethernet frame.

1. FastEthernet0 sends out the frame.

En Time 0.001 en Switch0:

1. FastEthernet0/1 receives the frame.

1. The frame source MAC address was found in the MAC table of Switch.
2. This is a unicast frame. Switch looks in its MAC table for the destination MAC address.

1. The outgoing port is an access port. Switch sends the frame out that port.

1. FastEthernet0/3 sends out the frame.

En Time 0.003 en Router 1:

1. GigabitEthernet0/0 receives the frame.
 1. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
 2. The device decapsulates the PDU from the Ethernet frame.
 1. The device looks up the destination IP address in the CEF table.
 1. The CEF table has an entry for the destination IP address.
 2. The device decrements the TTL on the packet.
 1. The next-hop IP address is in the adjacency table. The device sets the frame's destination MAC address to the one found in the table.
 2. The device encapsulates the PDU into an Ethernet frame.
 1. GigabitEthernet0/1 sends out the frame.

En Time 0.006 en Router 2:

1. GigabitEthernet0/1 receives the frame.
 1. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
 2. The device decapsulates the PDU from the Ethernet frame.
 1. The device looks up the destination IP address in the CEF table.
 1. The CEF table has an entry for the destination IP address.
 2. The device decrements the TTL on the packet.
 1. The next-hop IP address is in the adjacency table. The device sets the frame's destination MAC address to the one found in the table.
 2. The device encapsulates the PDU into an Ethernet frame.
 1. GigabitEthernet0/0 sends out the frame.

En Time 0.007 en Switch1:

1. FastEthernet0/3 receives the frame.
 1. The frame source MAC address was found in the MAC table of Switch.
 2. This is a unicast frame. Switch looks in its MAC table for the destination MAC address.
 1. The outgoing port is an access port. Switch sends the frame out that port.
1. FastEthernet0/2 sends out the frame.

En Time 0.009 en PC3:

1. FastEthernet0 receives the frame.
 1. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
 2. The device decapsulates the PDU from the Ethernet frame.
 1. The packet's destination IP address matches the device's IP address or the broadcast address. The device de-encapsulates the packet.
 2. The packet is an ICMP packet. The ICMP process processes it.
 3. The ICMP process received an Echo Request message.
 1. The ICMP process replies to the Echo Request by setting ICMP type to Echo Reply.
 2. The ICMP process sends an Echo Reply.
 3. The destination IP address 192.168.1.2 is not in the same subnet and is not the broadcast address.
 4. The default gateway is set. The device sets the next-hop to default gateway.

1. The next-hop IP address is a unicast. The ARP process looks it up in the ARP table.
2. The next-hop IP address is in the ARP table. The ARP process sets the frame's destination MAC address to the one found in the table.
3. The device encapsulates the PDU into an Ethernet frame.

1. FastEthernet0 sends out the frame.

En Time 0.011 en Switch1:

1. FastEthernet0/2 receives the frame.
 1. The frame source MAC address was found in the MAC table of Switch.
 2. This is a unicast frame. Switch looks in its MAC table for the destination MAC address.
 1. The outgoing port is an access port. Switch sends the frame out that port.

1. FastEthernet0/3 sends out the frame.

En Time 0.013 en Router 2:

1. GigabitEthernet0/0 receives the frame.
 1. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
 2. The device decapsulates the PDU from the Ethernet frame.
 1. The device looks up the destination IP address in the CEF table.
 1. The CEF table has an entry for the destination IP address.
 2. The device decrements the TTL on the packet.
 1. The next-hop IP address is in the adjacency table. The device sets the frame's destination MAC address to the one found in the table.
 2. The device encapsulates the PDU into an Ethernet frame.
 1. GigabitEthernet0/1 sends out the frame.

En Time 0.015 en Router 1:

1. GigabitEthernet0/1 receives the frame.
 1. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
 2. The device decapsulates the PDU from the Ethernet frame.
 1. The device looks up the destination IP address in the CEF table.
 1. The CEF table has an entry for the destination IP address.
 2. The device decrements the TTL on the packet.
 1. The next-hop IP address is in the adjacency table. The device sets the frame's destination MAC address to the one found in the table.
 2. The device encapsulates the PDU into an Ethernet frame.
 1. GigabitEthernet0/0 sends out the frame.

1. The next-hop IP address is in the adjacency table. The device sets the frame's destination MAC address to the one found in the table.
2. The device encapsulates the PDU into an Ethernet frame.

1. GigabitEthernet0/0 sends out the frame.

En Time 0.018 en Switch0:

1. FastEthernet0/3 receives the frame.
 1. The frame source MAC address was found in the MAC table of Switch.
 2. This is a unicast frame. Switch looks in its MAC table for the destination MAC address.
 1. The outgoing port is an access port. Switch sends the frame out that port.

1. FastEthernet0/1 sends out the frame.

En Time 0.020 en PC0:

1. FastEthernet0 receives the frame.

1. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
2. The device decapsulates the PDU from the Ethernet frame.

1. The packet's destination IP address matches the device's IP address or the broadcast address. The device de-encapsulates the packet.
2. The packet is an ICMP packet. The ICMP process processes it.
3. The ICMP process received an Echo Reply message.
4. The Ping process received an Echo Reply message.

ICMP:

PDU COMPLEJA.

La pdu compleja se puede configurar por medio de la ventana crear pdu compleja, desde allí configuramos el protocolo, las ip la cuales deben ser las de destino y la de origen, también se configura la secuencia de números a enviar y el tiempo que se requiere para que se haga el envío.

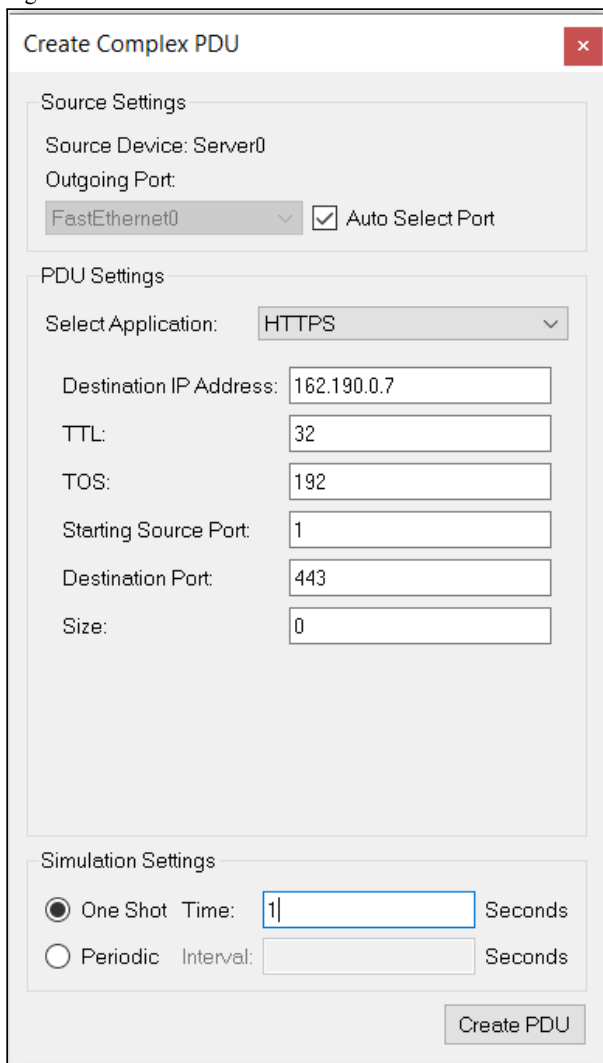


Figura 10. Configuración del servidor PDU compleja.

En la siguiente imagen se observa cuando ya finaliza la recepción de los datos en el servidor y el pc envía aviso de recibido.

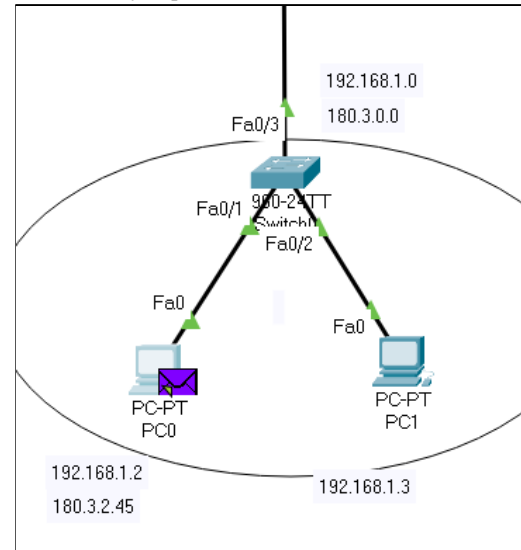


Figura 11. PDU compleja por HTTP.

Al hacer la pdu compleja el panel de simulación muestra los siguientes eventos los cuales se describen a continuación.

Simulation Panel				
Event List				
Vis.	Time(sec)	Last Device	At Device	Type
	450.783	—	PC0	HTTP
	450.784	—	PC0	HTTP
	450.785	PC0	Switch0	HTTP
	450.786	Switch0	Router1	HTTP
	450.787	Router1	Router2	HTTP
	450.788	Router2	Switch1	HTTP
	450.789	Switch1	Server0	HTTP
	450.790	Server0	Switch1	HTTP
	450.791	Switch1	Router2	HTTP
	450.792	Router2	Router1	HTTP
	450.793	Router1	Switch0	HTTP
	450.794	Switch0	PC0	HTTP

Figura 12. PDU compleja por HTTP lista de eventos.

Tiempo 450.783

1. The HTTP client sends a HTTP request to the server.

1. Sent segment information: the sequence number 1, the ACK number 1, and the data length 108.

1. The destination IP address 162.190.0.7 is not in the same subnet and is not the broadcast address.

2. The default gateway is set. The device sets the next-hop to default gateway.

1. The next-hop IP address is a unicast. The ARP process looks it up in the ARP table.

2. The next-hop IP address is in the ARP table. The ARP process sets the frame's destination MAC address to the one found in the table.

3. The device encapsulates the PDU into an Ethernet frame.

1. The port FastEthernet0 is sending another frame at this time. The device buffers the frame to be sent later.

Tiempo 450.784

1. The device takes out this frame from the buffer and sends it.
2. FastEthernet0 sends out the frame.

Tiempo 450.785

1. FastEthernet0/1 receives the frame.
1. The frame source MAC address was found in the MAC table of Switch.
2. This is a unicast frame. Switch looks in its MAC table for the destination MAC address.
1. The outgoing port is an access port. Switch sends the frame out that port.
1. FastEthernet0/3 sends out the frame.

Tiempo 450.786

1. GigabitEthernet0/0 receives the frame.
1. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
2. The device decapsulates the PDU from the Ethernet frame.
1. The device looks up the destination IP address in the CEF table.
1. The CEF table has an entry for the destination IP address.
2. The device decrements the TTL on the packet.
1. The next-hop IP address is in the adjacency table. The device sets the frame's destination MAC address to the one found in the table.
2. The device encapsulates the PDU into an Ethernet frame.
1. GigabitEthernet0/1 sends out the frame.

Tiempo 450.787

1. GigabitEthernet0/1 receives the frame.
1. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
2. The device decapsulates the PDU from the Ethernet frame.
1. The device looks up the destination IP address in the CEF table.
1. The CEF table has an entry for the destination IP address.
2. The device decrements the TTL on the packet.
1. The next-hop IP address is in the adjacency table. The device sets the frame's destination MAC address to the one found in the table.
2. The device encapsulates the PDU into an Ethernet frame.
1. GigabitEthernet0/0 sends out the frame.

Tiempo 450.788

1. FastEthernet0/3 receives the frame.
1. The frame source MAC address was found in the MAC table of Switch.
2. This is a unicast frame. Switch looks in its MAC table for the destination MAC address.
1. The outgoing port is an access port. Switch sends the frame out that port.
1. FastEthernet0/4 sends out the frame.

Tiempo 450.789

1. FastEthernet0 receives the frame.

1. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
2. The device decapsulates the PDU from the Ethernet frame.

1. The packet's destination IP address matches the device's IP address or the broadcast address. The device de-encapsulates the packet.

1. The device receives a TCP PUSH+ACK segment on the connection to 192.168.1.2 on port 1064.
2. Received segment information: the sequence number 1, the ACK number 1, and the data length 108.
3. The TCP segment has the expected peer sequence number.
4. TCP processes payload data.
5. TCP reassembles all data segments and passes to the upper layer.

1. The server receives a HTTP request.

1. The server sends back a HTTP reply to the client.

1. Sent segment information: the sequence number 1, the ACK number 109, and the data length 233.

1. The destination IP address 192.168.1.2 is not in the same subnet and is not the broadcast address.
2. The default gateway is set. The device sets the next-hop to default gateway.

1. The next-hop IP address is a unicast. The ARP process looks it up in the ARP table.
2. The next-hop IP address is in the ARP table. The ARP process sets the frame's destination MAC address to the one found in the table.
3. The device encapsulates the PDU into an Ethernet frame.

1. FastEthernet0 sends out the frame.

Tiempo 450.790

1. FastEthernet0/4 receives the frame.
1. The frame source MAC address was found in the MAC table of Switch.
2. This is a unicast frame. Switch looks in its MAC table for the destination MAC address.
1. The outgoing port is an access port. Switch sends the frame out that port.
1. FastEthernet0/3 sends out the frame.

Tiempo 450.791

1. GigabitEthernet0/0 receives the frame.
1. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
2. The device decapsulates the PDU from the Ethernet frame.
1. The device looks up the destination IP address in the CEF table.
1. The CEF table has an entry for the destination IP address.
2. The device decrements the TTL on the packet.
1. The next-hop IP address is in the adjacency table. The device sets the frame's destination MAC address to the one found in the table.
2. The device encapsulates the PDU into an Ethernet frame.

1. GigabitEthernet0/1 sends out the frame.

Tiempo 450.792

1. GigabitEthernet0/1 receives the frame.

1. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
2. The device decapsulates the PDU from the Ethernet frame.

1. The device looks up the destination IP address in the CEF table.

1. The CEF table has an entry for the destination IP address.
2. The device decrements the TTL on the packet.

1. The next-hop IP address is in the adjacency table. The device sets the frame's destination MAC address to the one found in the table.
2. The device encapsulates the PDU into an Ethernet frame.

1. GigabitEthernet0/0 sends out the frame.

Tiempo 450.793

1. FastEthernet0/3 receives the frame.

1. The frame source MAC address was found in the MAC table of Switch.
2. This is a unicast frame. Switch looks in its MAC table for the destination MAC address.

1. The outgoing port is an access port. Switch sends the frame out that port.

1. FastEthernet0/1 sends out the frame.

Tiempo 450.794

1. FastEthernet0 receives the frame.

1. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
2. The device decapsulates the PDU from the Ethernet frame.

1. The packet's destination IP address matches the device's IP address or the broadcast address. The device de-encapsulates the packet.

1. The device receives a TCP PUSH+ACK segment on the connection to 162.190.0.7 on port 80.
2. Received segment information: the sequence number 1, the ACK number 109, and the data length 233.
3. The TCP segment has the expected peer sequence number.
4. The TCP segment has the expected ACK number. The device pops the last sent segment from the buffer.
5. TCP processes payload data.
6. TCP reassembles all data segments and passes to the upper layer.

1. The HTTP client receives a HTTP reply from the server. It displays the page in the web browser.

CEF: Cisco Express Forwarding, CEF es un modo de conmutación de tráfico más rápido que otros disponibles.

ARP: Address Resolution Protocol, es un protocolo de resoluciones en la capa de datos, responsable de encontrar la dirección de hardware (Ethernet MAC) que corresponde a una determinada dirección IP.

La cabecera TCP contiene 6 “flags” para influenciar el flujo de datos:

SYN. Solicita la conexión

ACK. Reconoce (Acknowledge) la conexión

FIN. Finaliza la conexión

RST. Aborta una conexión, por motivos diversos

PSH: Enviar y rellenar el mensaje actual para enviar

inmediatamente.

URG: Informa al receptor sobre un segmento urgente que debe ser priorizado.

ANÁLISIS DE RESULTADOS.

Se observa que existen demasiados protocolos de comunicación como se muestra a continuación, y por ello es necesario filtrarlos, para obtener los que se desean analizar.



Figura 13. Protocolos disponibles.

Se aprecia como las banderas del protocolo TCP aparecen en ciertas líneas indicando cierto flujo que va a tomar ese mensaje, por ejemplo en “ The device receives a TCP PUSH+ACK segment on the connection to 162.190.0.7 on port 80. en tiempo 450.794 ” utilizando la bandera de PUSH y ACK

REDES DE DATOS PRACTICA 4

Para la práctica de laboratorio desarrollada se generan diversas redes locales LAN (Conectadas por un mismo switch). Las clases de las direcciones son de Clase C así mismo estas se conectan a un router para cada una de las clases ser conectadas finalmente entre sí.

En una de las redes se configura una conexión inalámbrica (wifi)

TABLA I

Direcciones de las redes WAN

RED	DIRECCIÓN IP	Mascara de subred
WAN 1	200.10.10.0	255.255.255.0
WAN 2	200.10.20.0	255.255.255.0
WAN 3	200.10.30.0	255.255.255.0

TABLA II

Direcciones de las redes LAN

RED	DIRECCIÓN IP	Mascara de subred
LAN 1	192.168.1.0	255.255.255.0
LAN 2	192.168.2.0	255.255.255.0
LAN 3	193.168.1.0	255.255.255.0
LAN 4	192.168.3.0	255.255.255.0

TABLA III

Direcciones de las Interfaces Router Bogotá

RED	Enlace	DIRECCIÓN IP	Mascara de subred
FastEthernet	LAN 4	192.168.3.1	255.255.255.0
Serial 2/0	WAN 1	200.10.10.2	255.255.255.0
Serial 3/0	WAN 2	200.10.20.1	255.255.255.0

TABLA IV

Direcciones de las Interfaces Router Medellin

RED	Enlace	DIRECCIÓN IP	Mascara de subred
FastEthernet	LAN 1	192.168.1.1	255.255.255.0
Serial 2/0	WAN 1	200.10.10.1	255.255.255.0
Serial 3/0	WAN 3	200.10.30.2	255.255.255.0

TABLA V

Direcciones de las Interfaces Router Cali

RED	Enlace	DIRECCIÓN IP	Mascara de subred
FastEthernet	LAN 2	192.168.2.1	255.255.255.0
FastEthernet	LAN 3	193.168.1.1	255.255.255.0
Serial 2/0	WAN 3	200.10.30.1	255.255.255.0
Serial 3/0	WAN 2	200.10.20.2	255.255.255.0

A cada uno de los routers se configura su dirección IP según la red LAN que pertenece donde debe coincidir con el segmento de red al que este pertenece, como se muestra en las tablas I-II, además se debe prender el puerto de red del router para que exista una comunicación. Finalmente ser probado con un ping que identifica este dispositivo en la red.

Para realizar la conexión de las dos redes se debe configurar en los routers de la red LOCAL el protocolo de enrutamiento, este proceso es mostrado en las tablas III-V. Esto se logra configurando dentro del apartado de la configuración del router la opción RIP, donde se agregan las direcciones IP a las que se desea brindar acceso desde el router.

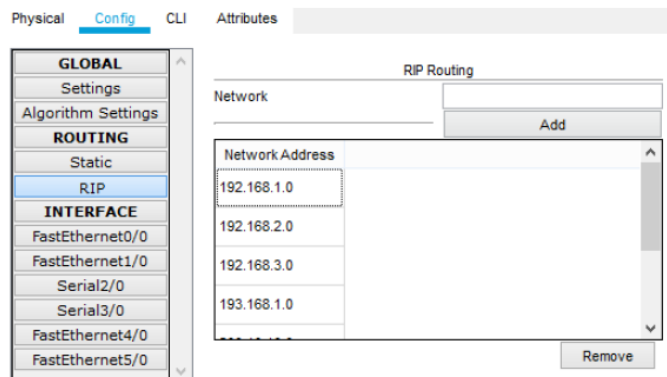


Figura 2. Configuración RIP del Router.

Finalmente se conecta a una de las redes un servidor que permite acceder desde los otros dispositivos de las distintas redes locales a los servicios en la página web. Esto se realiza programando un código HTTP, donde para acceder a

él, se ingresa la dirección IP asignada al servidor en su red LAN, en este caso es 192.168.3.4.

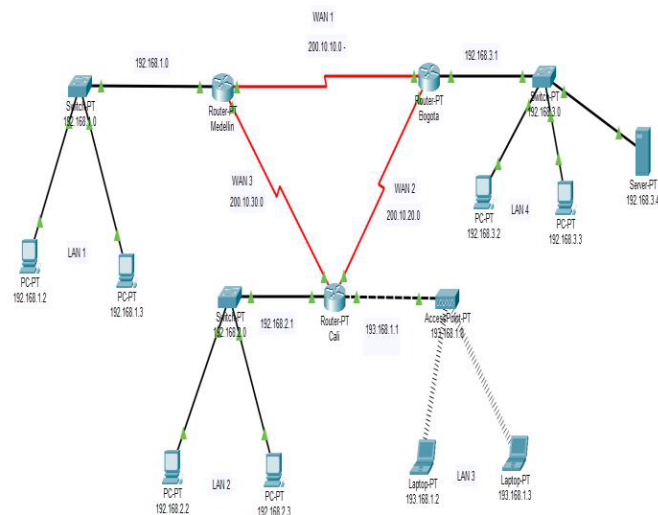


Figura 3. Esquema montaje.

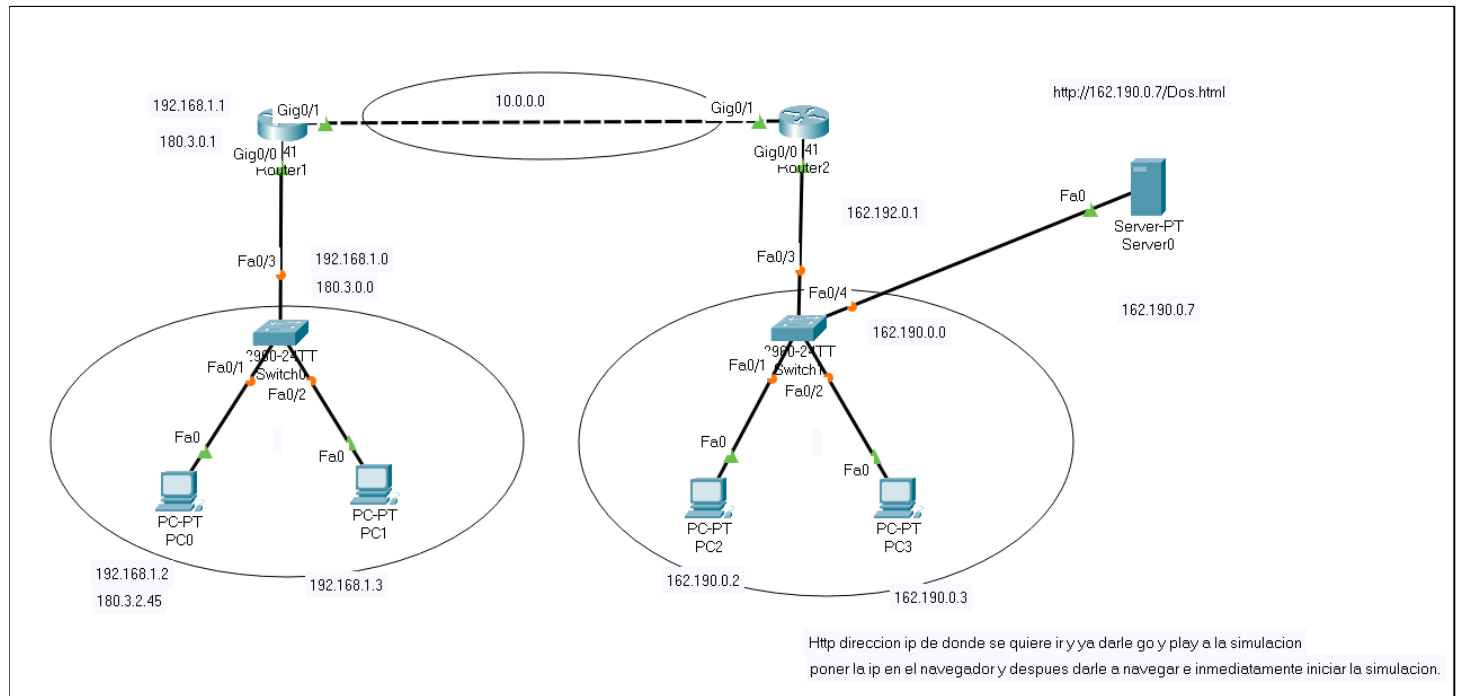
CONCLUSIONES.

- Se aplicó correctamente la implementación de una pdu simple y una pdu compleja para una red de routers y un servidor en el cual se implementan distintos protocolos como HTTP protocolo de transferencia de hipertexto, para páginas web e ICMP el cual es internet control message protocol, se logró establecer comunicación entre estos hosts de diferentes redes.
- La implementación de redes de datos permite la conectividad entre distintos componentes, es por esto, que es importante definir el modo por el cual estos se comunicaran, ya que de no ser así la comunicación fallará.
- Es fundamental tener presente la velocidad a la cual se hace el envío de datos, de no ser las misma la velocidad de transmisión con la de recepción, es posible que se produzcan fallos en la recepción del mensaje.
- Las direcciones IP son los destinos de un dato, es fundamental tener presente a qué clase pertenece cada uno de los dispositivos, esto permitirá que la comunicación se dé de manera efectiva.
- La implementación de redes de datos permite la conectividad entre distintos componentes, es por esto, que es importante definir el modo por el cual estos se comunicaran, ya que de no ser así la comunicación fallará.
- Las direcciones IP son los destinos de un dato, es fundamental tener presente a qué clase pertenece cada uno de los dispositivos, esto permitirá que la comunicación se dé de manera efectiva.
- Es fundamental tener presente la velocidad a la cual se hace el envío de datos, de no ser las misma la velocidad de transmisión con la de recepción, es posible que se produzcan fallos en la recepción del mensaje.

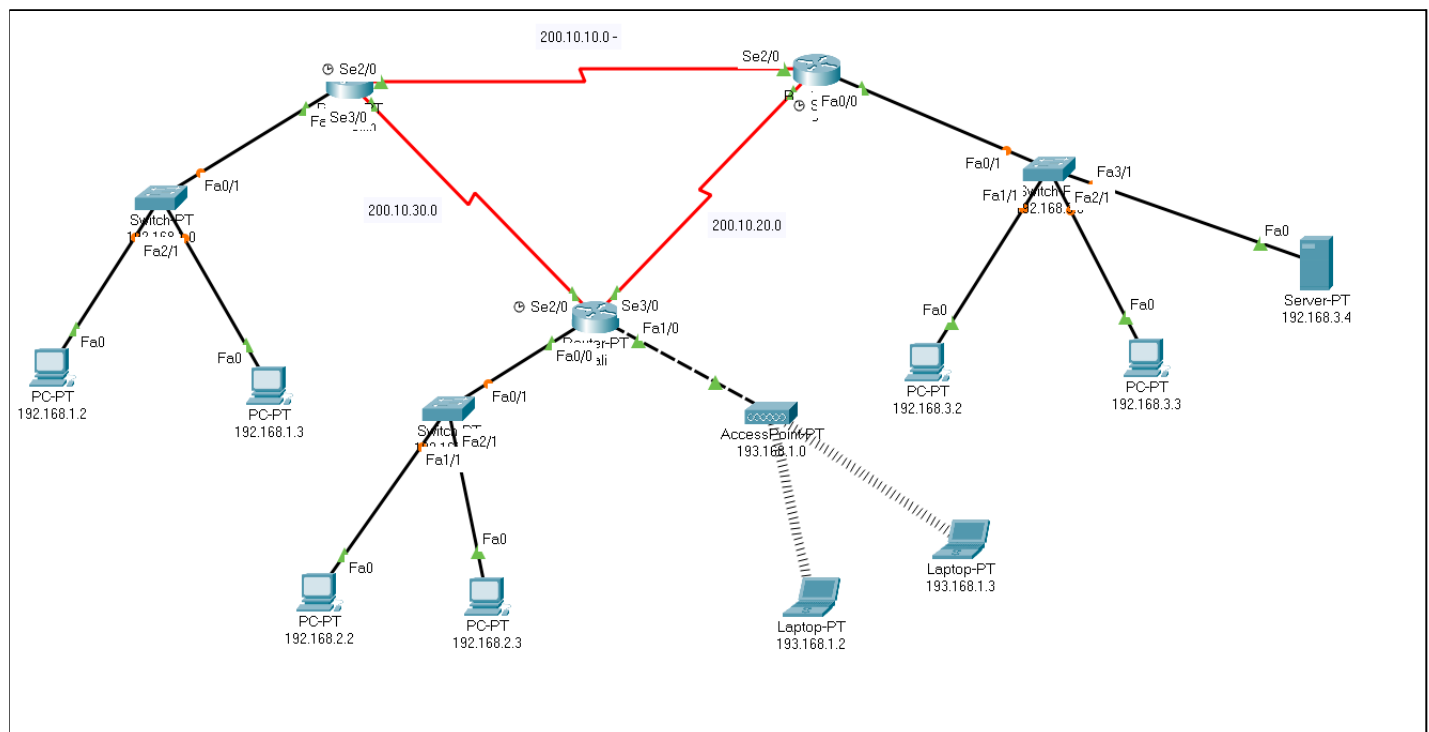
REFERENCIAS.

- [1]Cisco System, Interconexión de dispositivos de red, FinePrint, HispaLinux, 2012.
- [2]N. Sharadha, S. Anitha y J. Pushpanjali, «Developing an Ethernet Interface using a General Purpose Microcontroller and Ethernet Controller for power amplifier,» International Conference on Communication and Signal Processing (ICCSP), Chennai, 2018.
- [3]T. Nguyen Xuan, K. Semog , R. Jong Myung y P. Sang Yoon, «Novel Traffic Technique for the Redundancy Protocol for Ethernet (RPE),» IEEE, International Conference.

ANEXOS



Anexo 1. Montaje utilizado para las 2 PDU, simple y compleja.



Anexo 2. Montaje red de datos.