

## PRACTICA 2: Protocolos IP, ICMP

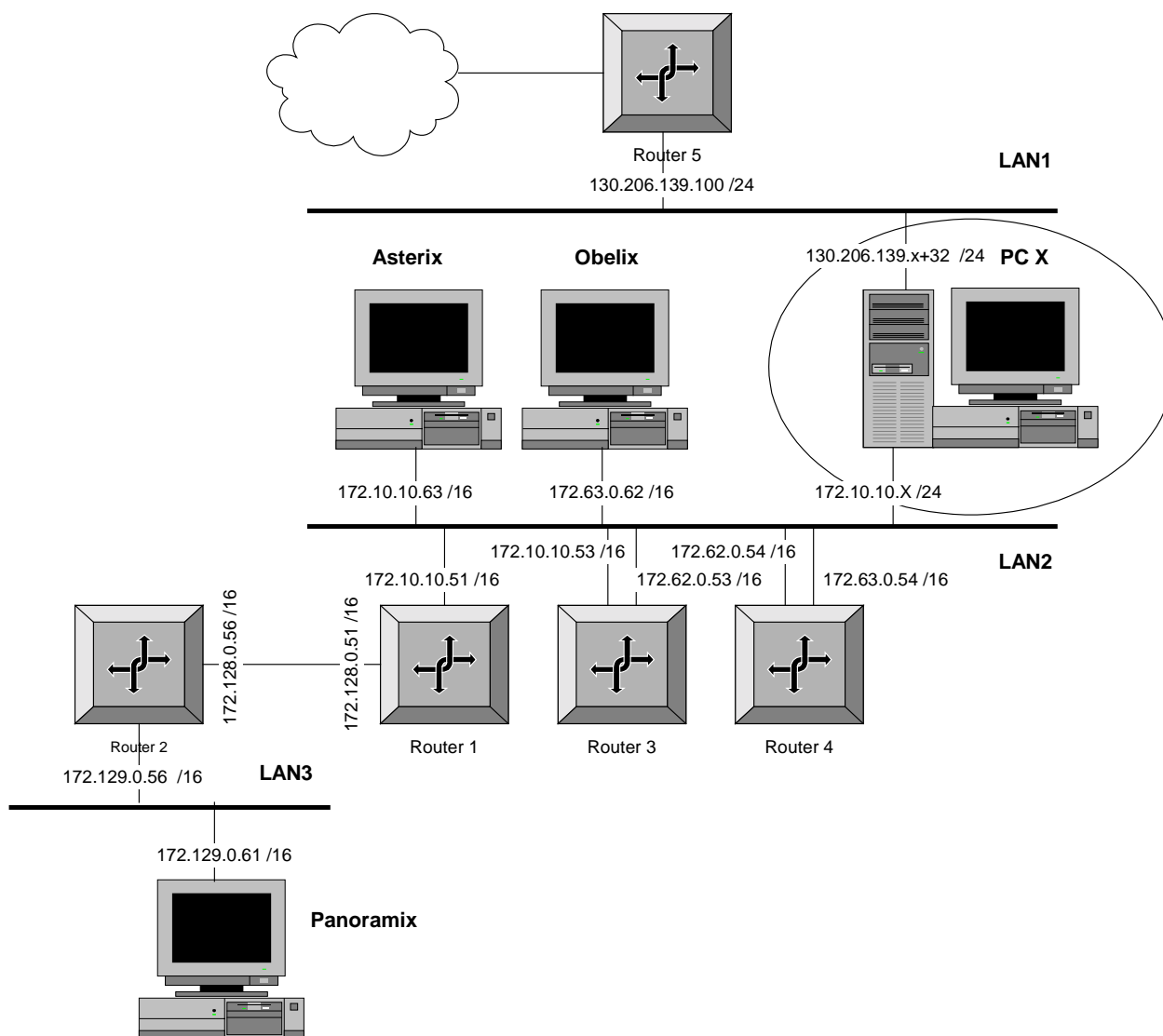
### 1. Objetivos de la práctica

Esta práctica tiene como objetivo primordial familiarizarse con los protocolos del conjunto TCP/IP: IP, e ICMP. Para ello se perseguirán tres objetivos concretos:

- Configurar el protocolo IP ( direcciones, máscara, tabla de encaminamiento ) en los interfaces Ethernet de un servidor Windows NT.
- Utilizar el monitor de red del System Management Server ( SMS ) de Microsoft para la captura y análisis del tráfico generado en la red, familiarizándose con sus opciones de captura y análisis.
- Estudiar la operación de los protocolos IP e ICMP.

### 2. Descripción del entorno

El entorno de red sobre el que se desarrollará la práctica aparece representado en la Figura 1 y está compuesto por:



- Un puesto de trabajo del alumno: PC-X (donde X es el número de puesto que irá de 1 a 18), dotado de dos interfaces Ethernet y con Windows NT Server 4.0.
- Cinco routers, conectados tal y como aparece en la Figura. Uno de ellos ( Router 5 ) proporciona acceso a la red de la UD, externa al laboratorio ( y por lo tanto a RedIris e Internet ).
- Tres redes Ethernet LAN1, LAN2 y LAN3. Cada PC está conectado a una toma de la mesa de trabajo correspondiente a la LAN1, y además, en cada mesa del laboratorio hay un hub que permite conectar el PC a la LAN2.
- Tres servidores ( Asterix, Obelix y Panoramix ) conectados como indica la figura.

El PC de cada uno de los puestos de trabajo ( PC-X ) debe conectarse a las redes LAN1 y LAN2 indicadas en la figura con las direcciones IP y máscaras correspondientes pero sin hacer routing entre ellas.

Como puede verse en la figura sobre la misma red física LAN2 se han creado varias redes lógicas. El propósito es que el monitor de red del PC-X pueda capturar los datagramas que circulan por todas las redes lógicas soportadas sobre LAN2.

### 3. GUIÓN DE LA PRACTICA

Se describen a continuación los pasos a seguir para realizar la práctica.

#### 3.1 Configuración de los interfaces Ethernet

Arrancar el PC en el modo preparado para el Laboratorio de Redes de Ordenadores (Windows NT Server 4.0 ) y configurar los dos interfaces Ethernet de la estación de trabajo con las direcciones IP indicadas en la tabla siguiente.


	Dirección	Máscara
Adapter 1	130.206.139.X+32	255.255.255.0
Adapter 2	172.10.10.X	255.255.0.0

La estación no deberá hacer routing entre sus interfaces y deberá utilizar al Router 5 como router (gateway) por defecto. Deberán incluirse manualmente en la tabla de encaminamiento de PC-X, mediante el comando *route*, todas las rutas que sean necesarias para que pueda accederse a todas las redes de la plataforma indicada en la figura.


Una vez terminada la configuración, puede comprobarse que la instalación realizada funciona haciendo ping a una dirección IP de cada una de las redes indicadas en la figura.

#### 3.2 Fragmentación de datagramas IP

1. Identificar, haciendo uso de mensajes ICMP la MTU del camino hasta el nodo PANORAMIX, así como la red en la cual dicho valor es mínimo estableciendo la MTU del camino.


	<ul style="list-style-type: none"> <li>• Explicar el procedimiento seguido para averiguar este valor.</li> <li>• Indicar la red que posee esta valor de MTU..</li> </ul>
---	--

2. Provocar la fragmentación de un datagrama en algún router (!NO EN EL NODO EMISOR SINO EN ALGÚN ROUTER EN LA RUTA HACIA UN DESTINO!) y capturar todos los fragmentos del mismo. (sugerencia: realizar *ping* a PANORAMIX con un tamaño del campo de datos que produzca fragmentación del datagrama, de este modo podrán capturarse los fragmentos del mensaje de respuesta ). Incluir la captura con el nombre *captura1.cap*.

	<ul style="list-style-type: none"> <li>• Indicar el modo en que se ha conseguido filtrar la captura para que SÓLO se visualicen las tramas que contienen los fragmentos de datagrama en cuestión.</li> <li>• Indicar los valores del campo desplazamiento del fragmento de cada uno de los octetos. Como sugerencia, comprobar que los valores obtenidos corresponden con los que el alumno esperaría obtener ( y si no es así cuestionarse el porqué ).</li> <li>• Identificar qué router ha fragmentado el datagrama ( el alumno debería ser capaz de explicar su respuesta).</li> </ul>
---	--


### 3.3 Encaminamiento

1. Enviar un datagrama que pase por varios routers hacia su destino atravesando varias redes lógicas que se encuentren configuradas sobre la misma red física (hacer *ping* a un nodo de la misma red física que PC X pero en diferente red lógica, por ejemplo OBELIX de modo que el datagrama atravesase las redes 172.10.0.0, 172.62.0.0 y 172.63.0.0, todas ellas sobre la misma red LAN2 ). Capturar ( *captura2.cap* ) las sucesivas transmisiones de un mismo datagrama con diferentes valores de TTL, es decir, en sucesivas retransmisiones del mismo en camino hacia su destino.


	<ul style="list-style-type: none"> <li>• Indicar cuántas veces se ha capturado el datagrama.</li> <li>• Indicar, para cada ocasión en que se ha capturado el datagrama el valor del campo TTL, explicando a qué salto corresponde ( entre qué routers o nodo-router se intercambia ).</li> <li>• Dar una explicación a los valores TTL obtenidos.</li> </ul>
---	--

### 3.4 Registro de ruta

1. Identificar, haciendo uso del comando *ping* y de mensajes ICMP con la opción de registro de ruta (RR), el camino que sigue un datagrama hasta OBELIX. Capturar las distintas transmisiones de este datagrama (teniendo en cuenta que los routers situados entre PC X y OBELIX comparten la misma red LAN2 ). Incluir la captura *captura3.cap*.

	<ul style="list-style-type: none"> <li>• Identificar la ruta seguida por los datagramas que contienen el "echo request" y el "echo reply" respectivamente ( mediante los nombres de los nodos/router que atraviesan ) a partir de la información proporcionada por el propio comando <i>ping</i>.</li> <li>• Explicar a partir de las tramas capturadas COMO CAMBIA el tamaño de la cabecera y el contenido de la opción RR en cada retransmisión del datagrama que contiene el mensaje ICMP.</li> </ul>
---	--


2. Identificar haciendo uso de la herramienta *tracert* ( comando *tracert* ) la misma ruta que en el ejercicio anterior, capturando las tramas generadas al ejecutar dicho comando y las respuestas correspondientes.

	<ul style="list-style-type: none"> <li>• Explicar a partir de las tramas capturadas el procedimiento que sigue el comando <i>tracert</i> para averiguar la ruta hasta un destino ( qué mensajes envía ... ). Aunque este procedimiento es fácil de encontrar en la bibliografía, el propósito es que el alumno sea capaz de descubrir a través del examen de las tramas qué es lo que está ocurriendo en un momento dado.</li> </ul>
---	--


3. Comprobar el funcionamiento del encaminamiento estricto y flexible en el comando *ping*, enviando datagramas con destino al nodo PANORAMIX con la opción encaminamiento estricto desde el origen y encaminamiento flexible desde el origen respectivamente. El alumno debe ser capaz de plantear un ejemplo con éxito y sin él en ambos casos de tipo de encaminamiento y explicar el motivo del fallo en su caso.

### 3.5 Mensajes de error ICMP

1. Utilizar el comando *ping* para generar tramas ICMP de destino no alcanzable (y capturarlas) de los siguientes tipos:
  - a) Red no alcanzable
  - b) Nodo no alcanzable
  - c) Fragmentación necesaria y bit de no fragmentación activado
  - d) Fallo en la ruta desde el origen


	<ul style="list-style-type: none"> <li>Indicar en cada caso el comando utilizado para conseguir el mensaje ICMP y quién ha devuelto la contestación.</li> </ul>
---	---

2. Generar y capturar una trama ICMP de Tiempo expirado durante el tránsito.

	<ul style="list-style-type: none"> <li>Indicar el comando utilizado para conseguir el mensaje ICMP y justificar quién ha enviado el mensaje ICMP.</li> </ul>
---	--

### 3.6 Mensajes de redirección ICMP

1. Generar y capturar mediante el comando *ping* un mensaje ICMP de redirección. Para ello deberá actuarse sobre la tabla de encaminamiento de PC-X modificando las entradas de su tabla de encaminamiento de modo que se produzca la emisión de un mensaje del tipo indicado.

	<ul style="list-style-type: none"> <li>Visualizar el contenido de la tabla de encaminamiento antes de ejecutar el comando ping (no es preciso incluirla en la memoria).</li> <li>Indicar el comando utilizado para conseguir que aparezca el mensaje ICMP de redirección.</li> <li>Justificar cómo se sabe que se ha enviado un mensaje ICMP de redirección, quién lo ha enviado y la lógica del hecho ( como sugerencia pueden capturarse las tramas y localizar la trama deseada o bien inferirlo a partir del contenido de la tabla de encaminamiento ).</li> <li>Visualizar el contenido de la tabla de encaminamiento después de ejecutar el comando ping e incluir en la memoria la ruta(s) nueva(s) aparecida(s).</li> </ul>
---	---