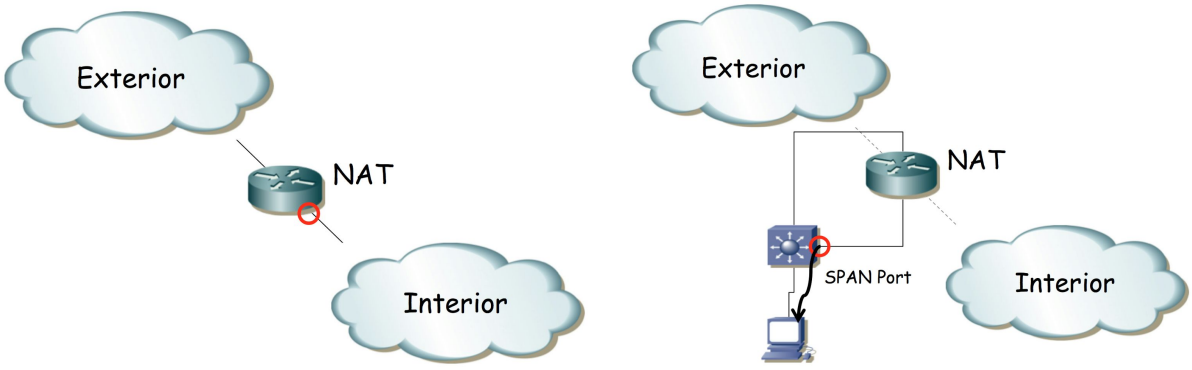
Práctica 2. Análisis de tráfico

Las trazas se han recogido de un router de salida del laboratorio (Fig. 1). Dicho router implementa también funcionalidades de NAT y está conectado a la red de la universidad. En las trazas se han borrado los datos contenidos a nivel superior al transporte por lo que no se puede analizar más allá de ese nivel.



a) Router/NAT y interfaz medida b) Configuración para realizar la medición

Fig. 1. Diagrama de la red

Se puede analizar la traza de acuerdo múltiples criterios. Aquí se enumeran algunos de ellos:

1. De acuerdo al tráfico a nivel de enlace. Estadísticas del número de tramas y su longitud.
2. Qué hosts hay presentes en la LAN (matrices de tráfico por direcciones MAC)
3. Flujo entrante al router y saliente del mismo. ¿Se satura su enlace? ¿De qué capacidad es?
4. Qué protocolos encapsula Ethernet: IPv4, IPv6, ARP, etc.
5. Qué protocolos de nivel de red están presentes. Si se detecta alguna anomalía.
6. Uso de puertos (a nivel TCP/UDP). Rango 1-1024 y con especial atención a: NFS, SSH, TELNET, NetBIOS, etc.
7. Por IPs (matrices de tráfico)
8. ¿Cuánto tráfico va dirigido a subredes de la UPNA y cuánto al exterior?
9. Conmutadores y routers: ¿Hay alguno?
10. Flujos principales a nivel de aplicación
11. Volumen de tráfico por servicios
12. Tráfico frente al tiempo de servidores o servicios destacados

Cada grupo tiene asignada una traza diferente por lo que los resultados no serán iguales. Se pide descargar dicha traza y analizarla de acuerdo a los criterios vistos en clase.

Entregables

- **Memoria (extensión máxima de 2000 palabras). Se valorará la cantidad y calidad de las conclusiones obtenidas así como la capacidad comunicativa y síntesis en el espacio limitado de texto que se os da.**