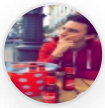


Juan94fran
www.wuolah.com/student/Juan94fran



# Ex. Enero 2019 RESUELTO.pdf

*Ex. Enero 2019 RESUELTO*

**3° Tecnologías Avanzadas de la Información**

**Grado en Ingeniería Informática - Tecnologías Informáticas**

**Escuela Técnica Superior de Ingeniería Informática**
**Universidad de Sevilla**

# Grado en Ingeniería Informática - Tecnologías de la Información
# Tecnologías Avanzadas de la Información - Evaluación continua 2019

*Apellidos, Nombre:*_____

**Cuestión 1.-** En el ámbito de la asignatura se ha optado por clasificar los ataques en función del objetivo, indique cuál es la clasificación propuesta y ponga un ejemplo de cada tipo de ataque. *(1 punto)*

**Cuestión 2.-** Indique las diferencias entre los ataques informáticos estructurados y los no estructurados. *(0.25 puntos)*

**Cuestión 3.-** Indique que tipo de ataque informático es un escaneo de puertos. No es un tipo de ataque. Se puede utilizar para realizar otro ataque *(0.25 puntos)*

**Cuestión 4.-** Los ataques DoS principalmente son de 2 tipos. Describa brevemente en que consisten ambos tipos. *(1 punto)*

**Cuestión 5.-** Un ataque típico en una red local es la inundación con paquetes UDP. En las redes IP los protocolos no tienen prioridad, entonces ¿por qué el efecto de la inundación UDP es la anulación del protocolo TCP? *(0.5 puntos)*

**Cuestión 6.-** OpenVPN utiliza las tecnologías indicadas. Describa brevemente cada una de ellas e indique para qué se utiliza en las VPNs *(1.5 puntos)*

- **(a)** Claves públicas y privadas RSA.
- **(b)** PKI: Certificados digitales, autoridades de certificación y firma electrónica.
- **(c)** Cifrado asimétrico.
- **(d)** Cifrado simétrico.
- **(e)** Túnel de red.
- **(f)** Protocolo TLS/SSL.

**Cuestión 7.-** En el ámbito de la seguridad informática las funciones HASH se utilizan: *(1 punto)*

- ☒ En los procesos de autenticación con contraseña.
- ☐ Para cifrar contraseñas.
- ☐ Para cifrar datos en una comunicación de red.
- ☒ En el proceso de firma electrónica.
- ☒ En la tecnología blockchain.
- ☒ En los certficados digitales usados en el protocolo SSL/TLS.

**Cuestión 8.-** Describa brevemente que es el Jitter e indique los principales motivos por los que aparece. *(0.5puntos)*

**Cuestión 9.-** La tecnología DIFFSERV tiene como objetivo dotar a Internet de QoS mediante el marcado de paquetes, responda brevemente: *(1 punto)*

- **(a)** ¿En que consiste el marcado de paquetes?
- **(b)** ¿Qué tecnología diferente al marcado de paquetes usa INTERSERV y por qué fracaso?

**Cuestión 10.-** Indique las métricas QoS estudiadas que más afectan a las siguientes aplicaciones: *(1 punto)*

**(a)** Skype R, J **(b)** Youtube A.B **(c)** Netflix A.B **(d)** Minecraft R, J

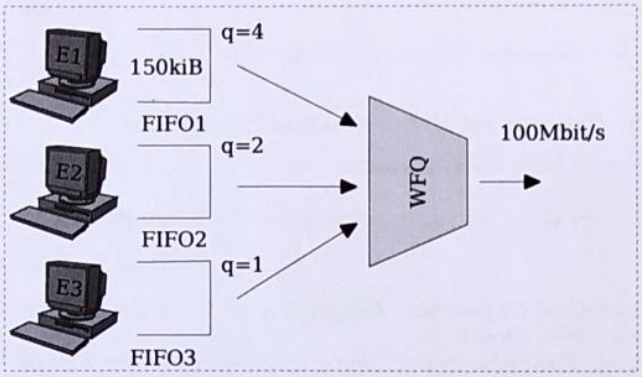
**(e)** FaceBook A.B **(f)** Gmail Nada **(g)** SFTP A.B **(h)** Canal de deportes IPTV R.

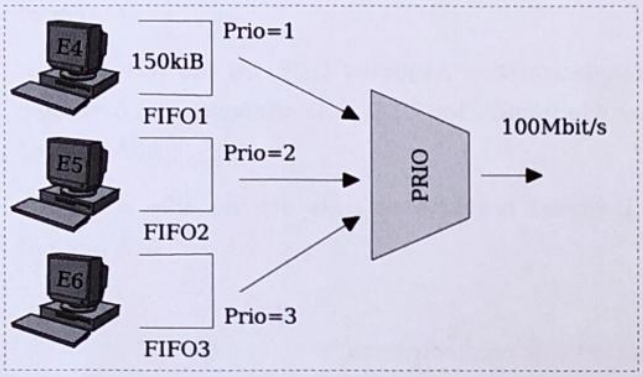
R = retraso

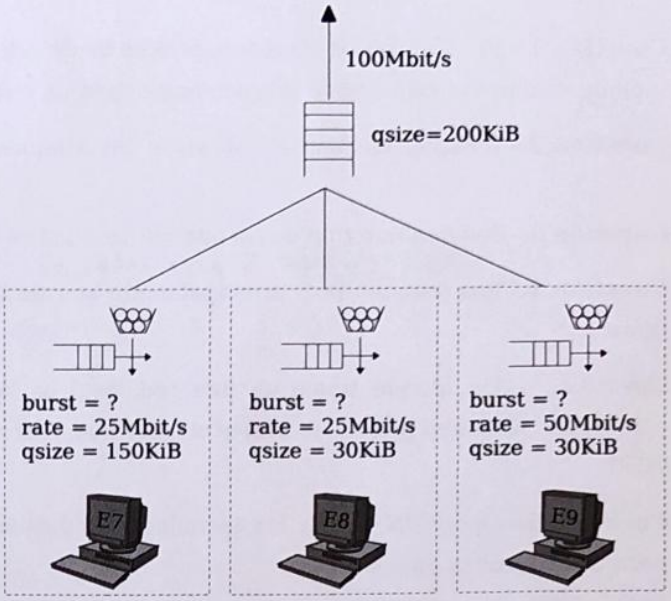
A.B = Ancho de banda

J = Jitter

**Cuestión 11.-** En la figura se muestran tres configuraciones: *(2 puntos)*




**(a)** Rellene la tabla indicando el mínimo caudal garantizado y la tasa pico usando las unidades correctas (G,M,K, etc.)

| Equipo | E1 | E2 | E3 | E4 | E5 | E6 | E7 | E8 | E9 |
|---|---|---|---|---|---|---|---|---|---|
| Caudal mínimo garantizado | 4/7·100 Mbit/s | 2/7·100 Mbit/s | 1/7·100 Mbit/s | 100Mbit/s | 0 | 0 | 25Mbit/s | 25Mbit/s | 50Mbit/s |
| Caudal máximo (tasa pico) | 100Mbit/s | 100Mbit/s | 100Mbit/s | 100Mbit/s | 100Mbit/s | 100Mbit/s | 100 ó 25 Mbit/s | 100 ó 25 Mbit/s | 100 ó 50 Mbit/s |

**(b)** Calcule el retraso máximo en los equipos E1 y E4.

**(c)** Calcule el tamaño de la cola del equipo E3 para que tenga un retraso máximo do 25ms. Utilice las unidades correctas en el resultado (KiB, MiB, GiB, etc.)

**(d)** Para la configuración con cubetas proponga una configuración para las ráfagas de cada equipo (parámetros burst) que no genere problemas de funcionamiento. ¿cual es la restricción existente cuando se configura el parámetro *burst*?

# Ex. Enero Alternativa 19

b) Retraso mínimo ($E_1$, $E_4$)

**$E_1$**

$N = 150 KiB$

1. Velocidad caudal

$\frac{4}{7} \cdot 100 = 57 \text{ Mbit/s}$

2. Retraso

$\frac{N}{V} = \text{retraso} \Rightarrow \frac{150 \cdot 10^3 \cdot 8 \text{ bit}}{57 \cdot 10^6 \text{ bit/s}} = 0'021 \text{ s} \rightarrow 21 \text{ ms}$

**$E_4$**

$N = 150 KiB$

1. Velocidad caudal

$100 \text{ Mbit/s}$

2. Retraso

$\frac{N}{V} = \text{retraso} \Rightarrow \frac{150 \cdot 10^3 \cdot 8 \text{ bit}}{100 \cdot 10^6 \text{ bit/s}} = 0'012 \text{ s} \rightarrow 12 \text{ ms}$

c) Tamaño cola $E_3$, retraso 25ms.

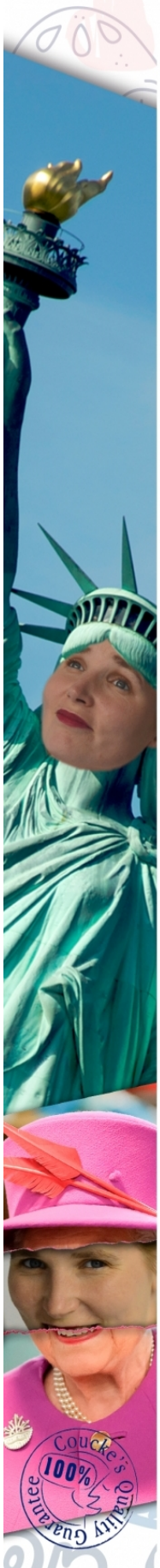
1. Velocidad caudal $E_3$

$\frac{1}{7} \cdot 100 = 14 \text{ Mbit/s}$

$\frac{N}{14 \cdot 10^6 \text{ bit/s}} = 25 \cdot 10^{-3} \text{ s}$

$N = 44 KiB$

* Al resultado anterior lo dividimos entre 8 y 1024 para tener KiB




d) La restricción para configurar las ráfagas (burst) es que no superen el tamaño de paquetes del enlace.

En este caso tenemos $q_{size} = 200K \cdot B$, pues los burst tener que sumar dicha cantidad: $burst_1 = 50\,K \cdot B$

$burst_2 = 50\,K \cdot B$

$burst_3 = 100\,K \cdot B$

---

Cuestión 1

- Ataques de confidencialidad: obtiene información o acceso privilegiado a un sistema. Sniffing desactiva el filtro de verificación de direcciones, todos los paquetes enviados a la red sean capturados.
- Ataques de autenticidad: Engañar a un sistema víctima. Spoofing que consiste en la suplantación de identidad.
- Ataques de Disponibilidad: inhabilitar el acceso a un servicio. Como ejemplo el Spam masivo.
- Ataques de integridad: Modificación o destrucción de datos. Exploits.

## Cuestion 2

No estructurados: no se define un objetivo específico, suelen ser fácilmente reconocibles.

Estructurados: se dirigen contra con objetivo concreto planificando y intentando evitar dejar huellas tras el ataque.

## Cuestión 4

- Denegación de servicio de aplicación: se volverá inaccesible por bloqueo de los recursos de la máquina o por un bloqueo completo de ésta.

- Denegación de servicio de red: buscan impedir que los usuarios de cierta red puedan hacer uso de los servicios de ella.

## Cuestión 5

Por el control de flujo, TCP necesita recibir una respuesta de los paquetes anteriores, si tenemos una inundación de UDP, los paquetes se perderán.

## Cuestión 8

Jitter: variación de tiempo entre dos paquetes consecutivos y aparece por colas saturadas en los routers

## Cuestión 6

La privacidad en VPN se consigue mediante técnicas criptográficas. Utiliza el cifrado simétrico que contiene una única clave y mucho más rápido y el cifrado asimétrico lo utiliza para compartir con mayor seguridad la clave del cifrado simétrico, donde dicha clave tiene que cambiarla cada cierto tiempo para mayor seguridad.

Para asegurar el intercambio de clave pública aparecen las infraestructuras PKI:

Además nos encontramos con las autoridades de certificación que firma las claves públicas, certificando la identidad de quien dice ser. El certificado digital archivo firmado con clave privada de la autoridad. Firma electrónica asegura que no sufre cambios.

Tunel de red, es un canal de comunicación que permite encapsular un protocolo dentro de otro, y lo empleamos en VPN para el acceso virtual seguro de usuarios remotos.

Los protocolos SSL/TLS son protocolos de seguridad y lo utilizamos en VPN para tener una seguridad en nuestra red ~~virtual~~ privada.

## Cuestión 9

a) • Marcado de paquetes: Alteración de los campos asignados para QoS para que sean ~~asignados~~ procesados. Puede ser: En Onjon, si se considera seguro o en frontera, se ignora el marcado onjon.

b) Interserv: garantiza estrictamente la reserva ancho de banda y fracaso por su mecanismo complejo y costoso.