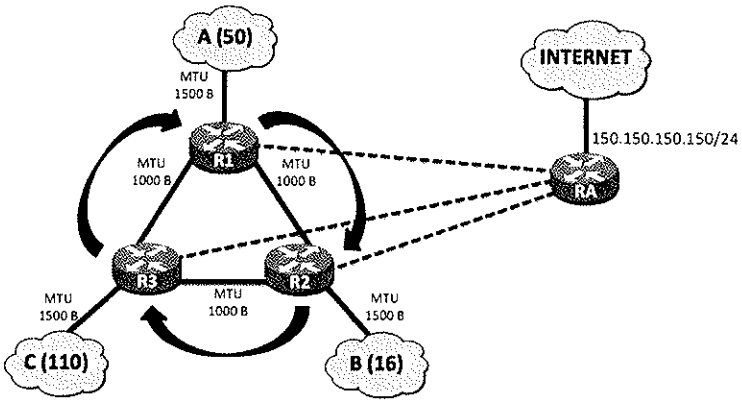
TRANSMISIÓN DE DATOS Y REDES DE COMPUTADORES II

Examen de Teoría[1]

Septiembre de 2011

APELLIDOS, NOMBRE: JORGE NAVARRO ORTIZ **GRUPO:**

1. (*2.5 puntos*) La siguiente figura muestra la topología de red de una empresa, que tiene contratado con su ISP el rango de direcciones 15.16.17.0/24. El número de ordenadores conectados a las redes A, B y C están indicados en la figura entre paréntesis.



a) Realice la asignación de direcciones IP tanto de equipos como de routers (incluyendo las redes entre los routers), utilizando direcciones públicas siempre que sea posible.

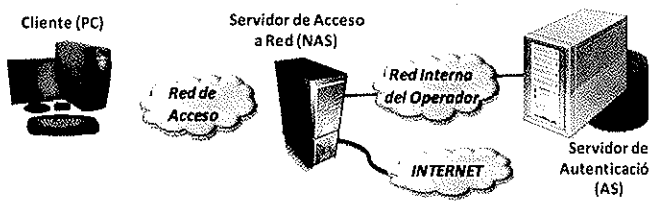
b) Indique las tablas de encaminamiento de todos los routers de forma que, para el tráfico entre las redes A, B y C, se encamine de acuerdo a las flechas en la figura). Debe haber conectividad completa entre estas redes y hacia Internet.

c) Suponga que el router R_A tiene funcionalidad de servidor DNS. Describa el intercambio de tramas si un ordenador de la red A quiere enviar un *ping* a un ordenador de la red C a través de su nombre de dominio (petición y respuesta con tamaño inferior a 1000 bytes). Tanto el mensaje de petición como el de respuesta del *ping* tienen un tamaño de 2000 bytes (incluyendo las cabeceras del nivel de red). Indique (si procede): direcciones físicas de origen y destino, direcciones IP de origen y destino, protocolo, puertos de origen y destino, flags, números de secuencia y acuse, y el tipo de mensaje.

2. (*2 puntos*) Explique las diferencias en objetivos y funcionamiento entre el control de flujo y el control de congestión en TCP. ¿Cómo ayudan los routers en el control de congestión de TCP? ¿Y en el control de flujo?

3. (*2.5 puntos*) La figura y mensajes siguientes describen un protocolo utilizado para permitir el acceso de un cliente a Internet a través de un Servidor de Acceso a Red (NAS). El Servidor de Autenticación (AS) guarda en una base de datos las claves secretas que se solicita a los usuarios para poder acceder a Internet.

PC → NAS: $Kpub_{NAS}$ (peticion_acceso + usuario)
NAS → PC: desafio
PC → NAS: $Kpub_{NAS}$(MD5(usuario:K_{PC-AS}:desafio))
NAS → AS: peticion_autenticacion + usuario + desafio + MD5(usuario:K_{AS-PC}:desafio))
AS → NAS: peticion_aceptada + $Ksesion_{PC-NAS}$ + K_{PC-AS}($Ksesion_{PC-NAS}$)
(ó peticion_rechazada)
NAS → PC: $Kpriv_{NAS}$ (peticion_aceptada + K_{PC-AS}($Ksesion_{PC-NAS}$))
(ó $Kpriv_{NAS}$ (peticion_rechazada))
PC → NAS: $Ksesion_{PC-NAS}$ (datos_a_enviar)
NAS → hacia Internet: datos_a_enviar
Desde Internet → NAS: datos_de_respuesta
NAS → PC: $Ksesion_{PC-NAS}$ (datos_de_respuesta)



Siendo:

- $Kpub_X$ cifrado con la clave pública de X
- $Kpriv_X$ cifrado con la clave privada de X
- K_{X-Y} la clave secreta entre X e Y
- MD5 es una función *hash*

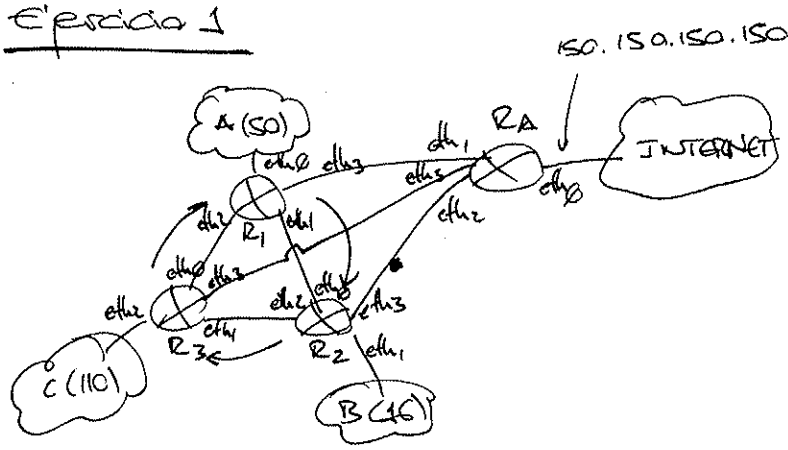
Suponiendo que las claves públicas corresponden a certificados digitales emitidos por una autoridad reconocida,

a) ¿Qué servicios de seguridad se proporcionan en el protocolo descrito?
b) ¿Qué debilidades presenta el esquema propuesto? En su caso, ¿cómo podrían evitarse?

[1] Esta prueba supone el 70% de la calificación final de la asignatura.

EXAMEN DE SEPTIEMBRE 2011 DE TDRC2

Ejercicio 1



* ISP proporciona el rango 15.16.17.0/24

a) Asignación de direcciones IP tanto de equipos como routers usando IPs públicas (si es posible).

Para evitar definir subredes con bits a 1 en la parte de equipo, es más sencillo empezando por las redes de mayor tamaño.

Red C → 110 equipos + 1 router + dir. subred + dir. difusión = 113 direcciones
→ potencia de 2 inmediatamente superior ⇒ $128 \geq 113$
→ rango 15.16.17.0/25 → de 15.16.17.0 a 15.16.17.127
(dir. subred; dir. difusión)

Red A ⇒ 50 equipos + 1 router + dir. subred + dir. difusión = 53
→ potencia de 2 inmediatamente superior → $64 \geq 53$
→ rango 15.16.17.128/26 → de 15.16.17.128 a 15.16.17.191
(dir. subred; dir. difusión)

Red B → 16 equipos + 1 router + dir. subred + dir. difusión = 19
→ potencia de 2 superior (o igual) → $32 \geq 19$
→ rango 15.16.17.192/27 → de 15.16.17.192 a 15.16.17.223
(dir. subred; dir. difusión)

Faltan las redes entre routers:

6 subredes × 4 direcciones (potencia de 2 mayor o igual que 2 routers + dir. subred + dir. difusión = 4)

= 24 direcciones

↳ caben sin problema (255 − 223 = 32 direcciones que quedan tras asignar las redes A, B y C).

* Red entre R_1 y R_2 → 4 direcciones → 15.16.17.224/30
  ↓ .225 ↓ .226
  ↳ de 15.16.17.224 a 15.16.17.227

* Red entre R_2 y R_3 → 4 direcciones → 15.16.17.228/30
  ↓ .229 ↓ .230
  ↳ de 15.16.17.228 a 15.16.17.231

* Red entre R_1 y R_3 → 4 direcciones → 15.16.17.232/30
  ↓ .233 ↓ .234
  ↳ de 15.16.17.232 a 15.16.17.235

* Red entre R_A y R_1 → 4 direcciones → 15.16.17.236/30
  ↓ .237 ↓ .238
  ↳ de 15.16.17.236 a 15.16.17.239

* Red entre R_A y R_2 → 4 direcciones → 15.16.17.240/30
  ↓ .241 ↓ .242
  ↳ de 15.16.17.240 a 15.16.17.243

* Red entre R_A y R_3 → 4 direcciones → 15.16.17.244/30
  ↓ .245 ↓ .246
  ↳ de 15.16.17.244 a 15.16.17.247

b) Tablas de encaminamiento de los routers

NOTA: Los equipos de las redes A, B y C tendrán como pasarela por defecto sus respectivos routers (R_1, R_2 y R_3).

* TABLA DE R_1

	Destino	Máscara	Siguiente salto	Interfaz	
Red A ←	15.16.17.128	/26	*	eth0	rutas directas
	15.16.17.224	/30	*	eth1	
	15.16.17.232	/30	*	eth2	
	15.16.17.236	/30	*	eth3	
Red C ←	15.16.17.0	/25	15.16.17.226 (R_2)	eth1	
Red B ←	15.16.17.192	/27	15.16.17.226 (R_2)	eth1	
INTERNET ←	default	0.0.0.0	15.16.17.237 (R_A)	eth3	

* TABLA DE R_2

	Destino	Máscara	Sig. salto	Interfaz
Red B ←	15.16.17.192	/27	*	eth1
	15.16.17.224	/30	*	eth0
	15.16.17.228	/30	*	eth2
	15.16.17.240	/30	*	eth3
			15.16.17.230 (R_3)	eth2
Red A ←	15.16.17.128	/26	15.16.17.230 (R_3)	eth2
Red C ←	15.16.17.0	/25	15.16.17.241 (R_A)	eth3
INTERNET ←	~~15.16.17.~~ default	0.0.0.0		

* TABLA DE R_3

	Destino	Máscara	Sig. salto	Interfaz
Red C ←	15.16.17.0	/25	*	eth_2
	15.16.17.232	/30	*	eth_0
	15.16.17.228	/30	*	eth_1
	15.16.17.244	/30	*	eth_3
Red A ←	15.16.17.128	/26	15.16.17.233 (R_1)	eth_0
Red B ←	15.16.17.192	/27	15.16.17.233 (R_1)	eth_0
INTERNET ←	default	0.0.0.0	15.16.17.245 (R_A)	eth_3

* TABLA DE RA

	Destino	Máscara	Sig. salto	Interfaz
	150.150.150.0	/24	*	eth_0
	15.16.17.236	/30	*	eth_1
	15.16.17.240	/30	*	eth_2
	15.16.17.244	/30	*	eth_3
RED A ←	15.16.17.128	/26	15.16.17.238 (R_1)	eth_1
RED B ←	15.16.17.192	/27	15.16.17.242 (R_2)	eth_2
RED C ←	15.16.17.0	/25	15.16.17.246 (R_3)	eth_3
INTERNET ←	default	0.0.0.0	150.150.150.xx (IP del gateway del ISP)	eth_0

c) Tramas para hacer un ping de un equipo de la red A a uno de la red C, usando el DNS ubicado en RA.

→ petición y respuesta DNS < 1000 Bytes → sin fragmentación
→ petición y respuesta del PING = 2000 Bytes → con fragmentación

Petición DNS → sobre UDP (puerto 53)
↳ sin flags ni nºs seq y acuse

PC → R_A → RA
PC ← R_1 ← RA

	Dir. física Origen	Dir. física Destino	Dir. IP Origen	Dir. IP Destino	Protocolo	Puerto origen	Puerto Destino	Tipo de mensaje
	MAC_PC_1	$MAC\_R_1\text{-}eth_0$	15.16.17.129 (PC)	15.16.17.237 (R_A)	UDP	*1 dado por S.O.	53	petición DNS
	$MAC\_R_1\text{-}eth_3$	$MAC\_R_A\text{-}eth_1$	"	"	"	"	"	"
	$MAC\_R_A\text{-}eth_1$	$MAC\_R_1\text{-}eth_3$	15.16.17.237 (R_A)	15.16.17.129 (PC)	UDP	53	*2 (igual que *1)	respuesta DNS
	$MAC\_R_1\text{-}eth_0$	MAC_PC_1	"	"	"	"	"	"

PING → protocolo ICMP sobre IP → no hay nivel de transporte, por lo que no hay puertas, flags ni nºs seq. o acuse.

PC →

Dir. física origen	Dir. física Destino	Dir IP origen	Dir IP destino	Protocolo	Tipo de mensaje
MAC_PC	MAC_R1-eth0	15.6.17.129 (PC_1)	15.6.17.1 (PC_2)	ICMP	ICMP echo-request
					1er fragmento (MF=1) (1480B datos + 20B cabecera)
					2º fragmento (MF=0) (2000B - 1480 = 520B datos + 20B cabecera)
MAC_R1-eth1	MAC_R2-eth0				ICMP echo-request
					fragmento 1a → 980B + 20B (MF=1)
					fragmento 1b → 500B + 20B (MF=1)
					fragmento 2 → 520B + 20B (MF=0)
MAC_R2-eth2	MAC_R3-eth1				fragmento 1a
					fragmento 1b
					fragmento 2
MAC_R3-eth2	MAC_PC2				fragmento 1a
					fragmento 1b
					fragmento 2

La vuelta (ICMP echo-reply) sería igual pero en el orden inverso, empezando por $PC_2 \rightarrow R_3 \rightarrow R_2 \rightarrow R_1 \rightarrow PC_1$.
La fragmentación sería también similar.

Ejercicio 2 Objetivos y funcionamiento de los controles de congestión y de flujo. (de TCP)

Control de flujo

* Objetivo: evitar que el receptor descarte paquetes (en su buffer de recepción) por no ser capaz de seguir el ritmo al emisor (la aplicación no consume datos tan rápidamente como llegan).

* Funcionamiento: el receptor envía una ventana ofertada al emisor en los ACKs de TCP, indicándole el nº bytes que tiene libre en su buffer de recepción. El emisor tiene en cuenta los datos aún no confirmados para calcular una ventana útil = ofertada - bytes en tránsito.

  Y no envía más datos que esa $V_{útil}$ (que se actualizará al recibir nuevas ACKs).

Control de congestión

* Objetivo: adaptarse a la capacidad real del canal, evitando/reduciendo el nº de paquetes descartados en los buffers de los routers (situación de congestión)

* Funcionamiento: depende de la versión de TCP. Suponiendo Tahoe, el emisor actualiza la ventana de congestión en base a los ACKs recibidos (e.g. inicio lento, prevención de la congestión). La falta de un ACK (expira su temporizador) se considera que se debe a la congestión y se reduce la ventana de congestión (máx. nº de bytes que el emisor puede enviar sin recibir confirmación, según este mecanismo).

El emisor puede transmitir el mínimo entre la ventana útil (control de flujo) y la ventana de congestión (control de congestión). (3)

Como se ha descrito, tienen objetivos y funcionamientos diferentes; cuando el emisor ha de considerar ambos para ver cuál limita su transmisión.

¿Cómo ayudan los routers en el control de congestión de TCP?

En las versiones originales de TCP no hay ningún mecanismo por el que los routers hagan algo para evitar la congestión.

¿y en el control de flujo?

Igualmente, en las versiones originales de TCP, no hay ningún mecanismo. Máxime cuando es el receptor, y no los routers, el que controla/gestiona el control de flujo.

Ejercicio 3

Este ejercicio se puso en el examen de Septiembre de 2010 y está resuelto en el material colgado en la web de la asignatura.