Arquitectura TCP/IP

Bloque IV. Tema 10

Gestión de Sistemas e Informática

Curso 2017 - 18

Juan José Aguado Gil

02 Febrero 2018

1. PDU: Protocol Data Unit

La información básica que manejan los protocolos se conoce como **PDU**. Las PDUs utilizadas en los diferentes niveles de OSI son:

Nivel	**PDU**
1	Bits
2	Trama (frame)
3	Paquete
4	Segmento; TPDU
5	SPDU
6	PPDU
7	Mensaje; APDU

2. MTU: Maximum Transmission Unit

MTU is the size of the largest network layer protocol data unit that can be communicated in a single network transaction. Fixed MTU parameters usually appear in association with a communications interface or standard. Some systems may decide MTU at connect time. The MTU relates to, but is not identical with the maximum frame size that can be transported on the data link layer, e.g. Ethernet frame.

Larger MTU is associated with reduced overhead. Smaller values can reduce network delay. In many cases MTU is dependent on underlying network capabilities and must be or should be adjusted manually or automatically so as not to exceed these capabilities.

2.1. Path MTU Discovery

The Internet Protocol defines the "Path MTU" of an Internet transmission path as the smallest MTU of any of the IP hops of the "path" between a source and destination. Put another way, the path MTU is the largest packet size that can traverse this path without suffering fragmentation.

3. Puertos y Sockets

Cada proceso que se comunica con otro proceso se identifica a sí mismo a la familia de protocolos TCP/IP por uno o más puertos. Un puerto es un número de 16 bits, usado por el protocolo host-a-host para identificar a qué protocolo de más alto nivel o programa de aplicación (proceso) debe entregar los mensajes de entrada.

Como algunos programas de más alto nivel son protocolos por sí mismos, estandarizados en la familia de protocolos TCP/IP, tales como telnet y ftp, usan el mismo número de puerto en todas las realizaciones de TCP/IP. Aquellos números de puerto "asignados" se denominan puertos bien-conocidos y las aplicaciones estándares servicios bien-conocidos.

Los **puertos bien-conocidos** los controla y asigna la Autoridad de Números Asignados de Internet (IANA) y en la mayoría de los sistemas sólo pueden usarlo los procesos del sistema o programas ejecutados con privilegios de usuario. Los puertos bien-conocidos asignados ocupan números de puerto en el rango de 0 a 1023.

3.1. Sockets

Socket designa un concepto abstracto por el cual dos programas (posiblemente situados en computadoras distintas) pueden intercambiar cualquier flujo de datos, generalmente de manera fiable y ordenada.

Los sockets constituyen el mecanismo para la entrega de paquetes de datos provenientes de la tarjeta de red a los procesos o hilos apropiados. Un socket queda definido por una de **dirección IP**, un **protocolo de transporte** y un **número de puerto**.

Primitivas en las comunicaciones a través de sockets:

- Primitivas de llamada a los sockets:
  - **socket**: crea un uevo punto terminal de conexión.

Puerto	Nombre	Descripción
20	ftp-data	FTP File Transfer Protocol - Datos
21	ftp-cmd	FTP File Transfer Protocol - Control
22	ssh	SSH (Secure Shell), scp, SFTP
67	bootps	BOOTP servidor y DHCP
68	bootpc	BOOTP cliente y DHCP
69	tftp	TFTP Trivial File Transfer Protocol
80	http	HTTP HyperText Transfer Protoco
88	kerberos	Kerberos Agente de autenticación
143	imap	IMAP: Internet Message Access Protocol
389	ldap	LDAP Protocolo de acceso ligero a Bases de Datos
443	https	HTTPS: Hypertext Transfer Protocol over TLS/SSL
546	DHCPv6c	Protocolo de configuración dinámica de host DHCP para IPv6 (client)
547	DHCPv6s	Protocolo de configuración dinámica de host DHCP para IPv6 (server)
646	LDP	Label Distribution Protocol: routing protocol used in MPLS networks
989	ftps	FTP over TLS/SSL (data)
990	ftps	FTP over TLS/SSL (control)
993	imaps	IMAPS: Internet Message Access Protocol over TLS/SSL
995	pop3s	POP3S: Post Office Protocol 3 over TLS/SSL

Tabla 1: Puertos bien conocidos.

  - **bind**: conecta una dirección local a un socket.
  - **close**: cierra un socket.

- Primitivas para sockets TCP:

  - **listen**: anuncia la disposición de aceptar conexiones.
  - **accept**: bloquea al invocador hasta la llegada de un intento de conexión TCP.
  - **connect**: intenta establecer activamente una conexión TCP.
  - **send**: envía datos a través de la conexión TCP.
  - **receive**: recibe datos de la conexión TCP.

- Primitivas para sockets UDP:

  - **sendto**: envía datos a un socket UDP.
  - **rcvfrom**: recibe datos de un socket UDP.

4. ARP / RARP

4.1. ARP: Address Resolution Protocol

Protocolo de resolución de direcciones. Permite conocer la dirección MAC asociada a una dirección IP.

4.2. RARP: Reverse Address Resolution Protocol

Protocolo de resolución de direcciones inverso. Permite conocer la dirección IP asociada a una dirección MAC.

4.3. Mensajes ARP / RARP: Reverse Address Resolution Protocol

Según el valor contenido en el campo **Código de Operación** de una datagrama ARP / RARP:

- **ARP Request**: código de operación = 1.
- **ARP Reply**: código de operación = 2.
- **RARP Request**: código de operación = 3.
- **RARP Reply**: código de operación = 4.

5. IP Versión 4

5.1. Direccionamiento IPv4

- Las direcciones tienen 32 bits que se agrupan en 4 grupos de 8 bits. Cada grupo (1 byte) se codifica en decimal y se separa del siguiente por un ".".
- Las direcciones IP tienen dos partes: red (identifica la red y es común a todos los equipos que están en la misma red) y host (identifica un host concreto dentro de una red).
- **Máscara de red**: plantilla de 32 bits que indica qué parte de la dirección IP identifica a la red (1's en la plantilla) y qué parte identifica al host (0's en la plantilla).
- **Direcciones especiales**:
  - **Loopback**: 127.0.0.1 (no sale por la tarjeta de red).
  - **Broadcast**: parte de red igual al valor de red específico + parte de host todo a 1's.
  - **0.0.0.0**: la usa inicialmente un host cuando arranca.

5.2. Clases de Direcciones

Clase	Primer Byte	Máscara Red	Número Redes	Número Hosts
A	0xxxxxxx	255.0.0.0	126	$2^{24} - 2$
B	10xxxxxx	255.255.0.0	2^{14}	$2^{16} - 2$
C	110xxxxx	255.255.255.0	2^{21}	$2^{8} - 2$

5.3. Direcciones IP Privadas

Clase	Rango
A	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.255.255
C	192.168.0.0 - 192.168.255.255

5.4. VLSM: Variable Length Subnet Masking

Técnica por la cual se diseña un esquema de direccionamiento usando varias máscaras en función de la cantidad de hosts.

6. IP Versión 5

IPv5 es un protocolo experimental llamado ST (Internet Stream Protocol).

7. IP Versión 6

7.1. Direccionamiento IPv6

- Las direcciones tienen 128 bits que se agrupan en 8 grupos de 16 bits, expresados en hexadecimal y separados por ":".
- Hay tres tipos de direcciones:
  - **Unicast**: identifica unívocamente una interfaz. Un paquete dirigido a una dirección unicast se envía a la interfaz asociada a esa dirección.
  - **Multicast**: identifica un grupo de interfaces IPv6. Un paquete dirigido a una dirección multicast es procesado por todos los miembros del grupo.
  - **Anycast**: se asigna a múltiles interfaces. Un paquete dirigido a una dirección anycast es enviado a solo una de esas interfaces (p.e. la del router más próximo).

- Direcciones especiales:
  - **Loopback**: 0:0:0:0:0:0:0:1 ∼ ::1 ∼ ::1/128
  - **Multicast**: comienzan por FF00::/8
  - **Multicast todos los nodos de mi red**: sustituye a la dirección de broadcast o difusión de la red local. Tiene el valor FF01::1/128

7.2. Notación de Direcciones IPv6

Reglas a seguir en la notación de direcciones IPv6 (8 grupos de 16 bits):

- Se pueden eliminar los ceros por la izquierda en cada bloque. Ejemplo:
  FE80:0000:0000:0000:0202:8329:0000:0000 ≡ FE80:0:0:0:202:8329:0:0
- Se pueden eliminar bloques consecutivos de ceros utilizando el carácter ":", pero este carácter **sólo puede aparece una vez** en la dirección. Ejemplo:
  FE80:0:0:0:202:8329:0:0 ≡ FE80::202:8329:0:0
- Cuando el último bloque es todo ceros, se puede quitar. Ejemplo:
  FE80:0:0:0:202:8329:0:0 ≡ FE80::202:8329:0:

7.2.1. Formato Cabecera IPv6

Algunos campos de la cabecera de Ipv4 han sido eliminados o convertidos en opcionales para reducir el coste de proceso normal de los paquetes y limitar el coste en ancho de banda de la cabecera Ipv6.

- **Versión**: para IPv6 su valor es siempre 6.
- **Clase de Tráfico / Prioridad**: clases o prioridades de paquetes.
- **Etiqueta de Flujo**: permite diferenciar aquellos paquetes que requieren un tratamiento especial.
- **Longitud de Carga Útil**; longitud del paquete después de la cabecera.
- **Next Header** (1 Byte): indica cuál de las seis cabeceras de extensión sigue a ésta. Si ésta es la última, este campo indica el protocolo de transporte. Posibles cabeceras de extensión:
  - **Value 0**: Opciones de salto por salto.
  - **Value 43**: Enrutamiento.
  - **Value 44**: Fragmentación.
  - **Value 51**: Verificación de autenticidad.
  - **Value 50**: Carga útil cifrada de seguridad.

- **Value 60**: Opciones de destino.

Posibles valores para protocolos de transporte:

- **Value 6**: Protocolo de transporte TCP.
- **Value 17**: Protocolo de transporte UDP.

- **Límite de Saltos**: equivalente al TTL de IPv4
- **Dirección Origen** (16 Bytes).
- **Dirección Destino** (16 Bytes).

7.2.2. Diferencias IPv4 e IPv6

- La implementación del multicast es obligatoria en IPv6 y opcional en IPv4.
- El MTU mínimo de IPv6 es de 1280 bytes frente a los 576 bytes de IPv4.
- El encabezamiento de IPv6 sin opciones es MAYOR que el encabezado de IPv4 sin opciones.
- El soporte para IPsec es obligatorio en IPv6 y opcional en IPv4.

7.2.3. Link-Local Address

Una **dirección de enlace-local** es una dirección IP creada únicamente para comunicaciones dentro de una subred local. Los routers no enrutan paquetes con direcciones de enlace local.

Las direcciones de enlace local se asignan usando los procedimientos de **stateless address autoconfiguration** para IPv4 e IPv6. En IPv4, las direcciones de enlace local pueden usarse cuando no hay disponible un mecanismo externo de configuración de direcciones, tal como DHCP, u otro mecanismo principal de configuración ha fallado. En IPv6, las direcciones de enlace local son necesarias para el funcionamiento interno de varios componentes del protocolo.

Las direcciones de enlace local para IPv4 están definidas en el bloque 169.254.0.0/16. En IPv6, están reservadas con el prefijo fe80::/64.

8. ICMP: Internet Control Message Protocol

Detecta y notifica las condiciones de error de la red. Utiliza la orden **traceroute** para obtener la ruta que se sigue desde nuestro equipo hasta otro en Internet. Está definido en las RFC 792 y 2463.

ICMP envía mensajes en forma de datagramas que permiten al conjunto del protocolo TCP/IP realizar entre otras las siguientes funciones:

1. Control de flujo.

2. Detección de destinos inalcanzables.

3. Pruebas de conectividad.

9. DHCP: Dynamic Host Configuration Protocol

Protocolo que permite asignar direcciones IP dinámicas a los equipos que lo soliciten de una red. Los paquetes DHCP se encapsulan sobre el protocololo UDP.

Los protocolos DHCP y DHCPv6 (DHCP for IPv6) están definidos en los documentos RFC 2131 y RFC 3315, respectivamente.

10. TCP: Transmision Control Protocol

Es un protocolo de la capa de transporte orientado a conexión.

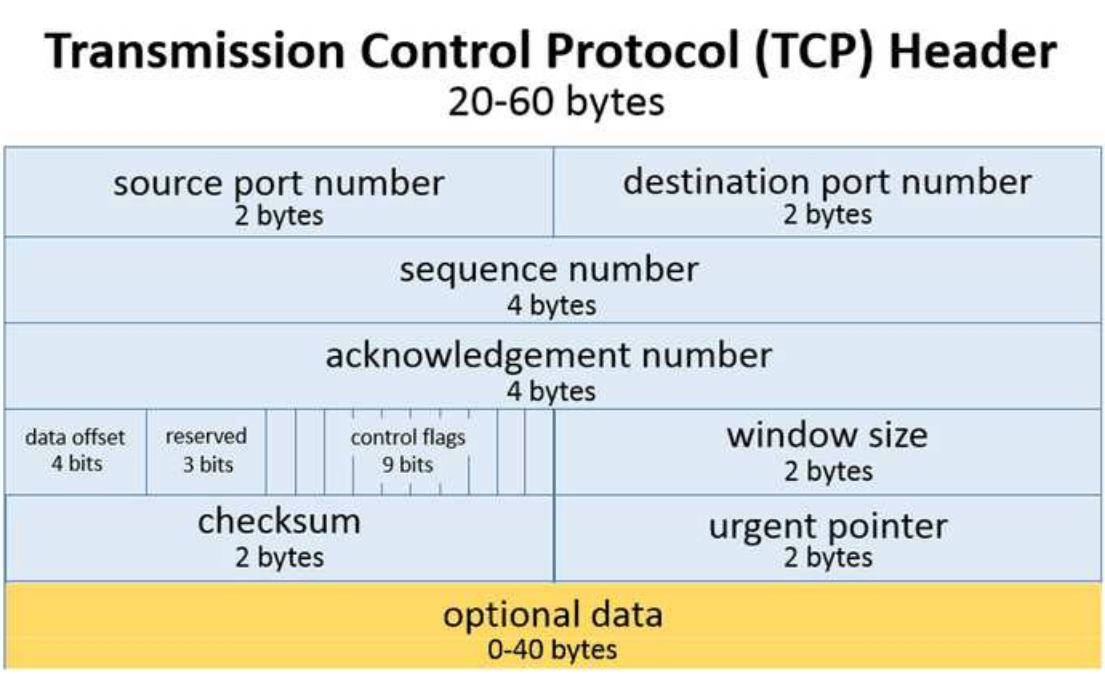

Figura 1: TCP Header.

11. TFTP: Trivial File Transfer Protocol

Es un protocolo de transferencia muy simple, semejante a una versión básica de FTP. A menudo, TFTP se utiliza para transferir pequeños archivos entre ordenadores en una red, como cuando un terminal X Window o cualquier otro cliente ligero arranca desde un servidor de red. Algunos detalles de TFTP son:

- Utiliza UDP (en el puerto 69) como protocolo de transporte (a diferencia de FTP que utiliza los puertos 20 y 21 TCP).
- No puede listar el contenido de los directorios.
- No existen mecanismos de autenticación o cifrado.
- Se utiliza para leer o escribir archivos de un servidor remoto.
- Soporta tres modos diferentes de transferencia, *netascii*, *octet* y *mail*, de los que los dos primeros corresponden a los modos *ascii* e *imagen* (binario) del protocolo FTP.

Tipos de mensajes TFTP:

- **RRQ (Read ReQuest)**: opcode = 1.
- **WRQ (Write ReQuest)**: opcode = 2.
- **DATA**: opcode = 3.
- **ACK**: opcode = 4.
- **ERROR**: opcode = 5.

12. FTPS: FTP Secure

FTPS (also known as FTPES, FTP-SSL, S-FTP and FTP Secure) is an extension to the commonly used File Transfer Protocol (FTP) that adds support for the **Transport Layer Security (TLS)** and the **Secure Sockets Layer (SSL)** cryptographic protocols.

FTPS should not be confused with the SSH File Transfer Protocol (SFTP), a secure file transfer subsystem for the Secure Shell (SSH) protocol it is not compatible with. It is also different from FTP over SSH, the practice of tunneling FTP through an SSH connection.

12.1. Methods of Invoking Security

Two separate methods were developed to invoke client security for use with FTP clients:

- **Implicit**: requires that a Transport Layer Security is established from the beginning of the connection, which in turn breaks the compatibility with non-FTPS-aware clients and servers. In order to maintain compatibility with existing non-FTPS-aware clients, implicit FTPS was expected to listen on the IANA well known port 990/TCP for the FTPS control channel, and port 989/TCP for the FTPS data channel. This allowed administrators to retain legacy-compatible services on the original 21/TCP FTP control channel.
- **Explicit**: uses standard FTP protocol commands and replies in order to upgrade a plain text connection to an encrypted one, allowing a single control port to be used for serving both FTPS-aware and non-FTPS-aware clients. This is very similar to the way HTTPS and STARTTLS implement Transport Layer Security for HTTP and SMTP protocol, respectively. In explicit mode an FTPS client must "explicitly request" security from an FTPS server and then step up to a mutually agreed encryption method. If a client does not request security, the FTPS server can either allow the client to continue in insecure mode or refuse the connection.

13. TCP Wrapper

TCP Wrapper is a host-based networking ACL system, used to filter network access to Internet Protocol servers on (Unix-like) operating systems such as Linux or BSD. It allows host or subnetwork IP addresses, names and/or ident query replies, to be used as tokens on which to filter for access control purposes.

In Red Hat distributions, to determine if a client is allowed to connect to a service, TCP Wrappers reference the following two files, which are commonly referred to as hosts access files: */etc/hosts.allow* and */etc/hosts.deny*.

When a TCP-wrapped service receives a client request, it performs the following steps:

- It references */etc/hosts.allow*: the TCP-wrapped service sequentially parses the */etc/hosts.allow* file and applies the first rule specified for that service.
- If it finds a matching rule, it allows the connection.
- If not, it moves on to the next step.
- It references */etc/hosts.deny*: the TCP-wrapped service sequentially parses the */etc/hosts.deny* file.
- If it finds a matching rule, it denies the connection.
- If not, it grants access to the service.

14. DNS: Domain Name System

El Sistema de Nombres de Dominio es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombre de dominio asignado a cada uno de los participantes. Su función más importante es traducir nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

14.1. Tipos de Tegistros DNS

- **A**: registro de dirección IPv4. Enlaza un dominio con la dirección IPv4 física.
- **AAAA**: registro de dirección IPv6. Traduce nombres de dominio a direcciones IPv6.
- **CNAME**: registro que enlaza un nombre de alias con un nombre de dominio canónico.
- **MX**: intercambio de correo (mail exchange). Asocia un nombre de dominio a una lista de servidores de correo.
- **PTR**: indicador (pointer) o registro inverso. Inverso del registro A, traduce IPs en nombres de dominio.
- **SOA**: autoridad de la zona (start of authority). Proporciona información sobre el servidor DNS primario de la zona.

14.2. Formato de Mensajes DNS

DNS utiliza el mismo formato de mensaje para:

- Todo tipo de consultas de clientes y respuestas de servidores.
- Mensajes de error.
- Transferencia de información de registro de recursos entre servidores.

El formato de los mensajes DNS es el siguiente:

- **Cabecera**.
- **Pregunta**: la pregunta para el servidor de nombres.
- **Respuesta**: registros de recursos que responden la pregunta.
- **Autoridad**: registros de recursos que apuntan a una autoridad.
- **Adicional**: registros de recursos que poseen información adicional. servidores.

14.3. BIND: Berkeley Internet Name Domain

BIND es el servidor de DNS más comúnmente usado en Internet, especialmente en sistemas Unix, en los cuales es un estándar de facto. Es patrocinado por la Internet Systems Consortium. BIND fue creado originalmente por cuatro estudiantes de grado en la University of California, Berkeley y liberado por primera vez en el 4.3BSD. Paul Vixie comenzó a mantenerlo en 1988 mientras trabajaba para la DEC.

Una nueva versión de BIND (BIND 9) fue escrita desde cero en parte para superar las dificultades arquitectónicas presentes anteriormente para auditar el código en las primeras versiones de BIND, y también para incorporar DNSSEC (DNS Security Extensions). BIND 9 incluye entre otras características importantes: TSIG, notificación DNS, nsupdate, IPv6, rndc flush, vistas, procesamiento en paralelo, y una arquitectura mejorada en cuanto a portabilidad. Es comúnmente usado en sistemas GNU/Linux.

15. RTP: Real-time Transport Protocol

El protocolo de transporte en tiempo real es un protocolo de nivel de aplicación utilizado para la transmisión de información en tiempo real, como por ejemplo audio y vídeo en una videoconferencia. Está desarrollado por el grupo de trabajo de transporte de audio y vídeo del IETF, publicado por primera vez como estándar en 1996 como la RFC 1889, y actualizado posteriormente en 2003 en la RFC 3550, que constituye el estándar de Internet STD 64.

Inicialmente se publicó como protocolo multidifusión, aunque se ha usado en varias aplicaciones unidifusión. Se usa frecuentemente en sistemas de retransmisión, junto a RTSP, videoconferencia y sistemas pulsa y habla (en conjunción con H.323 o SIP). Representa también la base de la industria de VoIP.

16. POP3: Post Office Protocol

Protocolo usado en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto, denominado Servidor POP. Es un protocolo de nivel de aplicación en el Modelo OSI.

17. IMAP: Internet Message Access Protocol

Es un protocolo de aplicación que permite el acceso a mensajes almacenados en un servidor de Internet. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet. IMAP tiene varias ventajas sobre POP (otro protocolo empleado para obtener correos desde un servidor). Por ejemplo, es posible especificar en IMAP carpetas del lado del servidor. Por otro lado, es más complejo que POP ya que permite visualizar los mensajes de manera remota y no descargando los mensajes como lo hace POP.

18. OCSP: Online Certificate Status Protocol

Es un protocolo que permite determinar el estado de vigencia de un certificado digital X.509 usando otros medios que no sean el uso de CRL (Listas de Revocación de Certificados).

19. HDLC (High Level Data Link Control)

HDLC (High-Level Data Link Control, control de enlace de datos de alto nivel) es un protocolo de comunicaciones de propósito general punto a punto, que opera a nivel de enlace de datos. Se basa en ISO 3309 e ISO 4335. Surge como una evolución del anterior SDLC. Proporciona recuperación de errores en caso de pérdida de paquetes de datos, fallos de secuencia y otros, por lo que ofrece una comunicación confiable entre el transmisor y el receptor. De este protocolo derivan otros como LAPB, LAPF, LLC y PPP.

19.1. Link Configurations

Link configurations can be categorized as being either:

1. **Unbalanced**, which consists of one primary terminal, and one or more secondary terminals.
2. **Balanced**, which consists of two peer terminals.

The three link configurations are:

1. **NRM (Normal Response Mode)**: is an unbalanced configuration in which only the primary terminal may initiate data transfer. The secondary terminal transmits data only in response to commands from the primary terminal. The primary terminal polls the secondary terminal(s) to determine whether they have data to transmit, and then selects one to transmit.
2. **ARM (Asynchronous Response Mode)**: is an unbalanced configuration in which secondary terminals may transmit without permission from the primary terminal. However, the primary terminal still retains responsibility for line initialization, error recovery, and logical disconnect.
3. **ABM (Asynchronous Balanced Mode)**: is a balanced configuration in which either station initialize, supervise, recover from errors, and send frames at any time. There is no master/slave relationship. The DTE (Data Terminal Equipment) and DCE (Data circuit-terminating equipment) are treated as equals.

20. Preguntas de Exámenes

1. (GSI.PI.2016.B4.21). **La dirección de broadcast de la red a la que pertenece el host con dirección IP 83.27.139.46/27 es:**

   a) 83.27.139.255
   b) 83.27.139.291
   c) 83.27.139.63
   d) 83.27.139.127

2. (GSI.PI.2016.B4.22, GSI.LI.2016.B4.21). **Una dirección IP en el protocolo IPv6 está formada por:**

   a) 32 bits
   b) 64 bits
   c) 128 bits
   d) 256 bits

3. (GSI.PI.2016.B4.24). **el campo "código de operación" de un datagrama ARP / RARP con el valor 4 se utiliza para una trama de:**

   a) solicitud RARP.
   b) respuesta RARP.
   c) solicitud ARP.
   d) respuesta ARP.

4. (GSI.PI.2016.B4.25). **¿Cuál es el nombre de la PDU de capa 2 del modelo OSI?:**

   a) MAC
   b) Trama
   c) Segmento
   d) Paquete

5. (GSI.PI.2016.B4.26). **¿Qué dos campos emplea IPv6 para proporcionar calidad de servicio?:**

   a) Tipo de Servicio y Clase de Tráfico.
   b) Límite de Saltos y Etiqueta de Tráfico.
   c) Clase de Tráfico y Etiqueta de Flujo.
   d) Tipo de Servicio y Prioridad.

6. (GSI.PI.2016.B4.27). **El protocolo IPv5:**

a) Es un protocolo de trancisión entre IPv4 e IPv6 con direcciones de 64 bits.

b) Es un protocolo experimental llamado ST (Internet Stream Protocol).

c) Es un protocolo de traducción/mapeo de direcciones IPv4 en IPv6, y viceversa.

d) No existe.

7. (GSI.PI.2016.B4.28). **¿Qué Puerto utiliza LDP (Label Distribution Protocol)?:**

   a) TCP 746

   b) TCP 646

   c) TCP 656

   d) TCP 756

8. (GSI.PI.2016.B4.44). **TFTP (Trivial File Transfer Protocol), según lo definido en la RFC 1350, soporta 5 tipos de paquetes, señale el incorrecto:**

   a) Data (DATA).

   b) Acknowledgment (ACK).

   c) Read-write request (RWQ).

   d) Error (ERROR).

9. (GSI.PI.2015.B4.26). **Queremos segmentar la red a la que pertenece la dirección 192.168.18.2/24 creando al menos 5 subredes que puedan albergar unos 20-25 hosts cada una. ¿Cuál sería la máscara de subred necesaria?:**

   a) 255.255.255.192

   b) 255.255.255.224

   c) 255.255.255.240

   d) 255.255.255.248

10. (GSI.PI.2015.B4.29). **El campo de la cabecera TCP (RFC 793) que indica el tamaño de ventana (Window) tiene una longitud de:**

    a) 8 bits.

    b) 16 bits.

    c) 24 bits.

    d) 32 bits.

11. (GSI.PI.2015.B4.31). **El puerto utilizado por BOOTP y DHCP para escuchar y recibir mensajes de solicitud de los clientes es el:**

    a) Puerto UDP 65.

b) Puerto UDP 67.

c) Puerto UDP 76.

d) Puerto UDP 56.

12. (GSI.PI.2015.B4.Reserva.02). **En el contexto del Domain Name System (DNS), ¿Qué es el CNAME?:**

    a) Es un registro que enlaza un nombre de alias con un nombre de dominio canónico.

    b) Es un registro que proporciona información de texto a fuentes externas a tu dominio.

    c) Es un registro que dirige el correo electrónico de un dominio a los servidores que alojan las cuentas de usuario del dominio.

    d) Es un registro que enlaza un dominio con la dirección IP física.

13. (GSI.PI.2014.B4.19). **La especificación del protocolo RTP (Real-Time Transport Protocol) corresponde a:**

    a) ITU-T

    b) IETF

    c) W3C

    d) IEEE

14. (GSI.PI.2014.B4.20, GSI.LI.2014.B4.20). **El puerto del protocolo FTP sobre TLS/SSL (FTPS) es:**

    a) 2121

    b) 2020

    c) 980

    d) 990

15. (GSI.PI.2014.B4.21). **¿Qué números de puerto TCP tienen asignados por IANA los protocolos IMAP e IMAPS (IMAP4 sobre TLS/SSL)?:**

    a) IMAP 143 e IMAPS 993.

    b) IMAPS 143 e IMAP 993.

    c) IMAP 193 e IMAPS 443.

    d) IMAPS 193 e IMAP 443.

16. (GSI.PI.2014.B4.22). **Señale cuáles son las direcciones IP de red y de broadcast para la siguiente subred 132.27.43.25/27:**

    a) red: 132.27.43.31/27 y broadcast: 132.27.43.0

    b) red: 132.27.43.20/27 y broadcast: 132.27.43.1

c) red: 132.27.43.0/27 y broadcast: 132.27.43.1

d) red: 132.27.43.0/27 y broadcast: 132.27.43.31

17. (GSI.PI.2014.B4.23, GSI.LI.2014.B4.25). **Según RFC 2460, señale de las siguientes cabeceras IPv6 cuál es una cabecera de extensión:**

    a) Cabecera Siguiente.

    b) Fragmento.

    c) Límite de Saltos.

    d) Longitud de la Carga Útil.

18. (GSI.PI.2014.B4.24). **Señale los tipos de tráfico IPv6 que hay:**

    a) Unicast, Multicast y Broadcast.

    b) Somecast, Multicast y Broadcast.

    c) Unicast, Multicast y Anycast.

    d) Unicast, Megacast y Anycast.

19. (GSI.PI.2014.B4.25, GSI.LI.2014.B4.26). **¿Cuál es el tipo de la dirección IPv6 ::1/128?:**

    a) Loopback.

    b) Indefinida (Unspecified).

    c) Multicast.

    d) No es válida.

20. (GSI.PI.2014.B4.31). **¿Cuál es la dirección de broadcast de la subred 172.17.11.32/27?:**

    a) 172.17.11.255

    b) 172.17.11.63

    c) 172.17.11.47

    d) 172.17.255.255

21. (GSI.PI.2013.B4.27, GSI.LI.2013.B4.22). **Indicar cuál de las siguientes direcciones IP puede ser asignada a un host en la siguiente subred 135.26.41.80/28:**

    a) 135.26.41.94

    b) 135.26.41.95

    c) 135.26.41.96

    d) 135.26.41.97

22. (GSI.PI.2013.B4.28). **Si tenemos la siguiente dirección de broadcast 95.26.35.159, indicar a qué subred pertenece:**

a) 95.26.35.144/30

b) 95.26.35.144/29

c) 95.26.35.128/27

d) 95.26.35.128/25

23. (GSI.PI.2013.B4.29). **De las siguientes cabeceras IPv6 (RFC 2460), ¿cuál de las siguientes cabeceras NO es de extensión?:**

a) Fragmentacion.

b) Opciones de salto a salto.

c) Autenticación.

d) Límite de saltos.

24. (GSI.PI.2013.B4.30). **El puerto 69 es utilizado por:**

a) TFTP (Trivial File Transfer Protocol).

b) Finger.

c) IMAP (Internet Message Access Protocol).

d) SFTP (Secure File Transfer Protocol).

25. (GSI.PI.2013.B4.32, GSI.LI.2015.B4.23). **¿Qué protocolo utiliza la orden "traceroute" para obtener la ruta que se sigue desde nuestro equipo hasta otro en Internet?:**

a) Ping

b) ICMP

c) PPP

d) RSVP

26. (GSI.PI.2013.B4.33). **Con respecto al protocolo DNS. ¿Cuál de las siguientes opciones NO es una parte de un mensaje DNS?:**

a) Cabecera.

b) Checksum.

c) Registros de recursos de Respuesta.

d) Registros de recursos de Autoridad.

27. (GSI.PI.2013.B4.34). **Un equipo con la dirección IP 128.0.235.56/27 ¿Qué máscara de red, dirección de red y dirección de broadcast tiene?:**

a) Máscara 255.255.255.224, red 128.0.235.32, broadcast 128.0.235.63

b) Máscara 255.255.255.0, red 128.0.235.0, broadcast 128.0.235.255

c) Máscara 255.255.255.192, red 128.0.235.0, broadcast 128.0.235.63

d) Máscara 255.255.255.128, red 128.0.235.0, broadcast 128.0.235.127

28. (GSI.PI.2013.B4.35, GSI.LI.2013.B4.27). **¿De qué tipo es la dirección de IPv6 ff00::/8?:**

a) No es válida.

b) Unicast.

c) Multicast.

d) Loopback.

29. (GSI.PI.2013.B4.36). **Indique qué dirección IPv6 de las siguientes NO es correcta:**

a) ::1

b) 2022::0ab7::1528:67bb

c) ::

d) ::212.200.31.255

30. (GSI.PI.2013.B4.37). **En una empresa con 2.000 puestos de usuario final en su red local de comunicaciones existen 3 subredes con estos direccionamientos: red A: 10.X.X.X red B: 192.168.1.X y red C: 195.57.72.X. Teniendo en cuenta que en la ubicación de los equipos de usuarios y servidores se busca mantener la red operativa y a la vez con la máxima seguridad posible, ¿en qué subred ubicaría los servidores web públicos?:**

a) Red A.

b) Red B.

c) Red C.

d) Indistintamente en la red B o en la red C.

31. (GSI.PI.2013.B4.53). **El protocolo FTP sobre TLS/SSL (FTPS-data) usa el puerto:**

a) 989

b) 567

c) 742

d) 334

32. (GSI.PI.2011.B4.12, GSI.LI.2011.B4.10). **¿Cuál de las siguientes es una conocida aplicación de servidor de DNS?:**

a) BISS

b) DNSOPI

c) DHCP

d) BIND

33. (GSI.PI.2011.B4.15, GSI.LI.2011.B4.08). **¿Qué tipo de registros DNS recomienda utilizar la RFC 3363 en relación a IPv6?:**

a) ALIAS

b) AAAA

c) CNAME

d) HIPV6

34. (GSI.PI.2011.B4.16). **¿Cuántas direcciones IP podrán asignarse en la subred 136.145.9.32/28, sin considerar las direcciones de subred y de broadcast?:**

a) 256

b) 14

c) 16

d) Es una dirección no enrutable.

35. (GSI.PI.2011.B4.36). **¿Que es VLSM (Variable-length subnet masking)?:**

a) Técnica por la cual se diseña un esquema de direccionamiento usando varias máscaras en función de la cantidad de hosts.

b) Técnica que permite agrupar varias subredes bajo una misma dirección de subred.

c) Técnica que permite a un router usar protocolos que no consideran las clases como los límites naturales de las subredes.

d) Técnica que permite utilizar direcciones IPV6 en redes IPv4.

36. (GSI.PI.2011.B4.38). **Un valor 17 en el campo "Cabecera siguiente" para IPv6 identifica el protocolo de capa superior como:**

a) SSH

b) FTP

c) TCP

d) UDP

37. (GSI.PI.2010.B4.30). **¿Cuál de las siguientes afirmaciones es correcta, considerando diferencias entre IPv4 e IPv6?:**

a) Ipv6 duplica el tamaño de la dirección desde los 32 bits a los 64 bits.

b) Algunos campos de la cabecera de Ipv4 han sido eliminados o convertidos en opcionales para reducir el coste de proceso normal de los paquetes y limitar el coste en ancho de banda de la cabecera Ipv6.

c) IPV6 complica la cabecera, al añadir campos a los que ya tenía la cabecera Ipv4, para permitir mayor capacidad de configuración, lo que supone por contra, un mayor coste de proceso, que se compensará por la mayor potencia del hardware.

d) IPv6 triplica el tamaño de la dirección desde los 32 bits a los 96 bits.

38. (GSI.PI.2010.B4.31). **De las siguientes afirmaciones sobre el protocol ICMP, ¿cuál es cierta?:**

a) Está definido en las RFC 792 y 2463.

b) Se considera un protocolo de nivel de transporte, al ir sobre datagramas IP.

c) Permite conocer la dirección MAC asociada a una dirección IP.

d) La cabecera tiene una longitud de 4 bytes en ICMPv4 y de 8 en ICMPv6.

39. (GSI.PI.2010.B4.32). **¿Sobre qué protocolo se encapsulan los paquetes DHCP?:**

a) HTTP.

b) UDP.

c) TCP.

d) IP.

40. (GSI.PI.2008.B4.34). **Señale la afirmación correcta. TCP es:**

a) Un protocolo de la capa de transporte orientado a conexión.

b) Un protocolo de la capa de transporte no orientado a conexión.

c) Un protocolo de las capas de enlace y red que puede detectar y compensar paquetes perdidos o datos alterados.

d) Un protocolo de la capa de transporte orientado fundamentalmente a regular el flujo de transmisión para no saturar a los receptores más lentos.

41. (GSI.PI.2008.B4.35). **¿Cuáles son los principales protocolos que operan en la capa de transporte en el modelo TCP/IP?:**

a) IPX y FTP

b) UDP y TCP

c) IP y TCP

d) UDP y IP

42. (GSI.PI.2008.B4.36). **Señale cómo se denomina la unidad de datos usada en la capa de transporte:**

a) Paquete

b) Segmento

c) Trama

d) Ninguna de las anteriores

43. (GSI.PI.2008.B4.51). **Interprete el funcionamiento de aplicar la máscara de subred 255.255.240.0 a la dirección IP 132.90.132.5:**

a) Host 5 de la subred 132.90.132.0

b) Host 4.1 de la subred 132.90.128.4

c) Host 4 de la subred 132.90.128.5

d) Host 4.5 de la subred 132.90.128.0

44. (GSI.LI.2016.B4.22). **Señale la respuesta CORRECTA sobre el protocolo de transferencia segura de ficheros FTPS:**

a) Al igual que en FTP, se utilizan canales diferentes para comandos y datos.

b) Usa el puerto estándar 22 (SSH) para realizar la transferencia de archivos.

c) En el método de conexión explícito, el cliente debe conectarse directamente al puerto TCP 990.

d) Tanto el canal de comandos como el de datos deben cifrarse en cualquier caso.

45. (GSI.LI.2016.B4.23). **Las direcciones IPv6 que proporcionan direccionamiento IP automático a los nodos en caso de que no exista un servidor DHCP, se denominan:**

a) Link-Local.

b) Aggregatable-Local.

c) Anycast.

d) Site-Local.

46. (GSI.LI.2016.B4.28). **¿Qué puertos por defecto utiliza el protocolo LDP (Label Distribution Protocol) de MPLS (Multiprotocol Label Switching)?:**

a) El 646 en TCP y UDP.

b) El 646 en UDP y el 647 en TCP.

c) El 647 en UDP y el 646 en TCP.

d) El 647 en TCP y UDP.

47. (GSI.LI.2015.B4.18). **TCP Wrappers es un sistema que permite controlar el acceso a:**

a) los servidores de una máquina UNIX. En concreto, permite filtrar conexiones no deseadas y permitir conexiones legítimas. Las reglas que se configuran son muy sencillas haciendo uso de un par de ficheros.

b) los servidores de una máquina UNIX. En concreto, permite filtrar conexiones no deseadas y permitir conexiones legítimas a un nivel muy bajo de la capa OSI por lo que podemos prescindir del uso de cortafuegos.

c) cada servicio que está corriendo en una máquina UNIX. Para ello es necesario tener instalado el GUI o entorno gráfico que nos permite configurar cada una de las reglas.

d) cada servicio que está corriendo en una máquina UNIX de manera remota. Es utilizado por los auditores de seguridad cuando se pretende interceptar paquetes TCP en una red. Se acompaña del uso de algún lenguaje de alto nivel como JAVA para su configuración.

48. (GSI.LI.2015.B4.19). **¿Cuál de los siguientes NO es un tipo de registro DNS válido?:**

a) MX

b) SOA

c) PTR

d) AAA

49. (GSI.LI.2015.B4.20). **¿Cuál de las siguientes respuestas se corresponde con el número de puerto tcp "bien conocido" para poder usar servicio de correo saliente POP3 sobre SSL (pop3s)?:**

a) 295

b) 995

c) 445

d) 725

50. (GSI.LI.2015.B4.21). **La RFC 1918 regula los rangos de direcciones reservadas para redes privadas, según dicho RFC ¿cuál de los siguientes rangos sería INCORRECTO considerarlo como red privada:**

a) 10.0.0.0 a 10.255.255.255

b) 192.168.0.0 a 192.168.255.255

c) 169.16.0.0 a 169.31.255.255

d) 172.16.0.0 a 172.31.255.255

51. (GSI.LI.2015.B4.22). **¿Cuál de las siguientes NO sería una dirección válida en IPv6?:**

a) FFED::BA98:3210:4562

b) 3FFE:FFFF::8:800:20C4:0

c) 8000::56FA::FE12

d) 3FFE:FFFF:0:CD30::/64

52. (GSI.LI.2014.B4.19). **El protocolo DHCP (Dynamic Host Configuration Protocol) y DHCPv6 (DHCP for IPv6) están definidos en los documentos:**

a) RFC 792 y RFC 4361, respectivamente.

b) RFC 826 y RFC 3315, respectivamente.

c) RFC 1034 y RFC 4361, respectivamente.

d) RFC 2131 y RFC 3315, respectivamente.

53. (GSI.LI.2014.B4.21). **¿Cuál de los siguientes protocolos permite conocer en tiempo real si un certificado ha sido o no revocado?:**

a) OCSP

b) CRL

c) PKCS#10

d) HTTPS

54. (GSI.LI.2014.B4.22). **ICMP envía mensajes en forma de datagramas que permiten al conjunto del protocolo TCP/IP realizar entre otras las siguientes funciones, señale la FALSA:**

a) Control de flujo.

b) Detección de destinos inalcanzables.

c) Encriptación de paquetes.

d) Pruebas de conectividad.

55. (GSI.LI.2014.B4.23). **Señale cuál de las siguientes direcciones IP puede ser asignada a un host en la siguiente subred 132.26.41.90/26:**

a) 132.26.41.128

b) 132.26.41.127

c) 132.26.41.124

d) 132.26.41.55

56. (GSI.LI.2014.B4.24). **Indique a qué subred pertenece la siguiente dirección de broadcast 95.25.46.159:**

a) 95.25.30.128/27

b) 95.25.30.128/25

c) 95.25.46.128/27

d) 95.25.46.128/25

57. (GSI.LI.2014.B4.27). **Señale cuál de las siguientes afirmaciones es correcta en relación a la MTU (Maximum Transfer Unit) en redes IP, la MTU del camino es el valor de la:**

a) suma de todas las MTU entre el receptor y el emisor.

b) media aritmética de todas las MTU entre el receptor y el emisor.

c) MTU más baja de todos los enlaces a lo largo del camino entre nodos receptor y emisor.

d) MTU más alta de todos los enlaces a lo largo del camino entre nodos receptor y emisor.

58. (GSI.LI.2013.B4.21). **Indicar de las siguientes, cuál es una cabecera de extensión IPv6:**

a) Cabecera siguiente.

b) Enrutamiento.

c) Longitud de la carga útil.

d) Límite de saltos.

59. (GSI.LI.2013.B4.23). **En IPv6 (RFC 2460), ¿cuánto ocupa el campo "tipo de enrutamiento"?:**

a) 15 bits.

b) 8 bits.

c) 10 bits.

d) 3 bits.

60. (GSI.LI.2013.B4.26). **En las comunicaciones a través de sockets, ¿cuál de las siguientes NO se corresponde con una primitiva?:**

a) Bind

b) Listen

c) Reject

d) Socket

61. (GSI.LI.2013.B4.29). **En una empresa con 2.000 puestos de usuario en su red local de comunicaciones existen 3 subredes con estos direccionamientos: red A: 10.X.X.X, red B: 192.168.1.X y red C: 195.57.72.X.Teniendo en cuenta que en la ubicación de los equipos de usuarios y servidores se busca mantener la red operativa y a la vez con la máxima seguridad posible, ¿dónde se ubicarían los servidores de Base de Datos de los que se alimentan tanto los servidores web públicos como los de la intranet?:**

    a) Red A.

    b) Red B.

    c) Red C.

    d) Habría dos servidores de bases de datos, el público en la red C y el privado en la red B.

62. (GSI.LI.2011.B4.13). **Indique la respuesta INCORRECTA, respecto al protocolo FTP (File Transfer Protocol) en modo pasivo:**

    a) Siempre se abren dos puertos, uno para comando y otro para datos en cada extremo.

    b) El servidor ftp establece la conexión de datos con el cliente.

    c) Se usa para soslayar problemas de comunicaciones, cuando las tramas entrantes pueden ser filtradas por un firewall.

    d) El puerto de control en el servidor normalmente es el puerto 21.

63. (GSI.LI.2011.B4.31). **ICMP es un protocolo de:**

    a) Intercambio de correos electrónicos.

    b) Oficina de correo para obtener los mensajes de correo electrónico de un servidor remoto.

    c) Control y notificación de errores.

    d) Red utilizado para el intercambio de mensajes de correo electrónico.

64. (GSI.LI.2010.B4.19). **Dada la red 193.168.14.192/27, podemos decir que:**

    a) La dirección de broadcast de dicha red es la 193.168.14.255.

    b) Admite hasta 30 hosts, sin contar la direcciones de identificación de red y de broadcast.

    c) La dirección 193.168.14.225 pertenece a dicha red.

    d) Es una red con direccionamiento privado.

65. (GSI.LI.2010.B4.21). **Entre las diferencias en los protocolos IPv4 e IPv6 NO se encuentra que:**

a) La implementación del multicast es obligatoria en IPv6 y opcional en IPv4.

b) El MTU mínimo de IPv6 es de 1280 bytes frente a los 576 bytes de IPv4.

c) El encabezamiento de IPv6 sin opciones es menor que el encabezado de IPv4 sin opciones.

d) El soporte para IPsec es obligatorio en IPv6 y opcional en IPv4.

66. (GSI.LI.2010.B4.22). **Un socket necesita, para estar correctamente definido, especificar el protocolo de nivel de:**

a) Enlace.

b) Red.

c) Transporte.

d) Aplicación.

67. (GSI.LI.2010.B4.23). **El protocolo FTP es un protocolo:**

a) Seguro.

b) Orientado a conexión.

c) De nivel de enlace.

d) Diseñado para gestionar señalización de red.

68. (GSI.LI.2010.B4.24). **¿Cuántas direcciones IP serán asignadas en la subred 134.141.0.0/24, sin considerar las direcciones de subred y de broadcast?:**

a) 256.

b) 254.

c) 30.

d) 64.

69. (GSI.LI.2010.B4.25). **Hablando del modelo OSI ¿Cuál de las siguientes parejas NO es correcta?:**

a) Nivel 4 - HDLC.

b) Nivel 1 - CSMA/CD.

c) Nivel 3 - X.25.

d) Nivel 2 - LAPB.

70. (GSI.LI.2010.B4.27). **Una dirección IP identifica:**

a) Una conexión.

b) Una interfaz de tarjeta de red.

c) Un ordenador.

d) Una aplicación interactiva.

71. (GSI.LI.2008.B4.25). **Indique cuál de los siguientes conceptos se corresponde con una primitiva de servicio entre niveles del modelo OSI:**

a) RECEIVE

b) INDICATION

c) SEND

d) ECHO

72. (GSI.LI.2008.B4.26). **Señale quién realiza, en una arquitectura de comunicaciones TCP/IP, la función de conversión del intercambio de datagramas en una conexión de datos entre aplicaciones:**

a) TCP.

b) XML.

c) IP.

d) X-25.

73. (GSI.LI.2008.B4.27). **Señale qué servicio NO es básico dentro de la arquitectura de comunicaciones TCP/IP:**

a) Transferencia de archivos.

b) Terminal virtual.

c) Correo.

d) Acceso a archivos.

74. (GSI.LI.2008.B4.29). **Señale la afirmación correcta. La cabecera de IPv6 es:**

a) Menor que la de IPv4.

b) Mayor que la de IPv4.

c) Igual que la de IPv4.

d) No hay cabecera propiamente dicha.

75. (GSI.LI.2008.B4.41). **Señale qué puerto estándar está asociado al protocolo HTTPS (HyperText Transfer Protocol):**

a) 161

b) 115

c) 443

d) 22

76. (GSI.LI.2013.B4.25). **Indicar cuál de los siguientes NO es un modo de transferencia de datos utilizado por el protocolo HDLC (High Level Data Link Control):**

   a) Modo de respuesta normal (NRM, Normal Response Mode).

   b) Modo balanceado asíncrono (ABM, Asynchronous Balanced Mode).

   c) Modo de respuesta asíncrono (ARM, Asynchronous Response Mode).

   d) Modo balanceado síncrono (SBM, Synchronous Balanced Mode).

21. Soluciones

1. C
2. C
3. B
4. B
5. C
6. B
7. B
8. C
9. B
10. B
11. B
12. A
13. B
14. D
15. A
16. D
17. B
18. C
19. A
20. B
21. A
22. C
23. D
24. A
25. B
26. B
27. A
28. C
29. B
30. C
31. A
32. D
33. B
34. B
35. A
36. D
37. B
38. A
39. B
40. A
41. B
42. B
43. D
44. A
45. A
46. A
47. A
48. D
49. B
50. C
51. C
52. D
53. A
54. C
55. C
56. C
57. C
58. B
59. B
60. C
61. B
62. B
63. C
64. B
65. C
66. C
67. B
68. B
69. A
70. B
71. B
72. Anulada
73. D
74. B
75. C
76. D