El Modelo TCP/IP

Bloque II. Tema 4

Gestión de Sistemas e Informática

Curso 2017 - 18

Juan José Aguado Gil

17 Enero 2018

1. Niveles Modelo OSI

Nivel 7	Aplicación
Nivel 6	Presentación
Nivel 5	Sesión
Nivel 4	Transporte
Nivel 3	Red
Nivel 2	Enlace
Nivel 1	Físico

1.1. Protocolos

Conjunto de normas y convenciones que permiten la comunicación entre dos capas de igual nivel jerárquico de entidades diferentes (no tienen porque ser máquinas diferentes).

Cada capa del modelo OSI proporcina servicios a su capa inmediatamente superior. La iteración entre capaa adyacentes (N y N+1) se realiza mediante cuatro primitivas: REQUEST, INDICATION, RESPONSE y CONFIRM.

La información básica que manejan los protocolos se conoce como **PDU** (Protocol Data Unit). 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. Niveles Arquitectura TCP/IP

Nivel	Nombre	Protocolos
5	Aplicación	Telnet, FTP, SMTP, HTTP, DNS, SNMP, SSL, ...
4	Transporte	TCP, UDP
3	Red	IP, ICMP, ARP, RARP, X25, MPLS, ...
2	Enlace	LAPB, HDLC, ATM, Frame Relay, ...
1	Físico	CSMA/CD, Ethernet, PLC, ...

3. Puertos

Números de puerto bien conocidos usados por los protocolos TCP y UDP.

Puerto	Nombre	Descripción
20	ftp-data	FTP File Transfer Protocol - Datos
21	ftp-cmd	FTP File Transfer Protocol - Control
80	http	HTTP HyperText Transfer Protoco
88	kerberos	Kerberos Agente de autenticación
389	ldap	LDAP Protocolo de acceso ligero a Bases de Datos
547	DHCPv6	Protocolo de configuración dinámica de host DHCP para IPv6

4. Protocolos de Nivel 3

4.1. IP Versión 4

4.1.1. 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 ".".

- 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.

4.1.2. Formato Paquete IP

- **Cabecera** (20 Bytes + Opciones):
  - **Versión** (4 bits): puede contener un 4 (IPv4) o un 6 (IPv6).
  - ...
  - **Longitud Total** (2 Bytes): longitud total en octetos del datagrama, incluyendo cabecera y datos. La longitud teórica máxima es de **64 KBytes**.
  - ...
  - **TTL (Time To Live)** (1 Byte): indica el número máximo de encaminadores que un paquete puede atravesar.
  - **Protocolo** (1 Byte): indica la entidad de la capa de transporte a la que debe entregarse el datagrama en destino.
  - **Checksum** (2 Byte): suma de comprobación de la cabecera.
  - **Dirección Origen** (4 Bytes).
  - **Dirección Destino** (4 Bytes).
  - **Opciones** (de 0 o 40 Bytes).
- **Cuerpo**: se corresponde con el segmento TCP/UDP de la capa de transporte.

4.2. IP Versión 6

Desarrollado en la **RFC 2460** (especificaciones del protocolo) y en la **RFC 2373** (direccionamiento).

4.2.1. Ventajas respecto a IPv4

- Soluciona las limitaciones de direccionamiento.
- Mejora los mecanismos multicast.
- Introduce las direcciones anycast.
- Desaparecen las direcciones broadcast.

4.2.2. Direccionamiento IPv6

- Identificadores de 128 bits (16 bytes) para interfaces. (**interfaz**: conexión al medio de transmisión). El formato es de 8 bloques de 16 bits expresados en hexadecimal y separados por ":".
- Las direcciones IP se asignan a interfaces (como en IPv4), no a nodos (como en OSI).
- 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 $\Rightarrow$ ::1
  - **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

4.2.3. Formato Cabecera IPv6

- **Versión**: para IPv6 su valor es siempre 6.
- **Prioridad**.
- **Etiqueta de Flujo**.
- **Longitud de Carga Útil**.
- **Next Header**: indica cuál de las seis cabeceras de extensión sigue a ésta. Si ésta es la última, esta 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.
- **Límite de Saltos**: equivalente al TTL de IPv4
- **Dirección Origen** (16 Bytes).
- **Dirección Destino** (16 Bytes).

4.3. ICMP: Internet Control Message Protocol

Detecta y notifica las condiciones de error de la red.

4.3.1. Tipos de mensajes ICMP

- **Echo Request**: mensaje de control que se envía a un host con la expectativa de recibir de él un Echo Reply (Respuesta Eco). Esto es conocido como **ping**.
- **Echo Reply**: mensaje generado como respuesta a un mensaje Echo Request (Petición de Eco).
- **Timestamp**: used for time synchronization. The originating timestamp is set to the time (in milliseconds since midnight) the sender last touched the packet.
- **Timestamp Reply**: replies to a Timestamp message.
- **Address Mask Request**: sent by a host to a router in order to obtain an appropriate subnet mask.
- **Address Mask Reply**: used to reply to an address mask request message with an appropriate subnet mask.
- **Source Quench**: requests that the sender decrease the rate of messages sent to a router or host. This message may be generated if a router or host does not have sufficient buffer space to process the request, or may occur if the router or host buffer is approaching its limit.
- **Redirect**: requests data packets be sent on an alternative route. ICMP Redirect is a mechanism for routers to convey routing information to hosts. The message informs a host to update its routing information (to send packets on an alternative route).

- **Time Exceeded**: generated by a gateway to inform the source of a discarded datagram due to the time to live field reaching zero. A time exceeded message may also be sent by a host if it fails to reassemble a fragmented datagram within its time limit.
- **Destination unreachable**: generated by the host or its inbound gateway to inform the client that the destination is unreachable for some reason.

4.4. LISP: Locator/Identifier Separation Protocol

It is a "map-and-encapsulate" protocol which is developed by the Internet Engineering Task Force LISP Working Group. The basic idea behind the separation is that the Internet architecture combines two functions, routing locators (where a client is attached to the network) and identifiers (who the client is) in one number space: the IP address. LISP supports the separation of the IPv4 and IPv6 address space following a network-based map-and-encapsulate scheme (RFC 1955). In LISP, both identifiers and locators can be IP addresses or arbitrary elements like a set of GPS coordinates or a MAC address.

4.5. ARP: Address Resolution Protocol

El Protocolo de Resolución de Direcciones es un protocolo de comunicaciones responsable de encontrar la dirección de hardware (Ethernet MAC) que corresponde a una determinada dirección IP. Para ello se envía un paquete (ARP request) a la dirección de difusión de la red (broadcast, MAC = FF:FF:FF:FF:FF:FF) que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (ARP reply) con la dirección Ethernet que le corresponde. Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo y la carga.

NOTA: las direcciones MAC son únicas a nivel mundial. Tienen un tamaño de 6 bytes (48 bits, de los cuales los 24 primeros los asigna el IEEE al fabricante y los otros 24 los utiliza el fabricante para identificar el dispositivo concreto).

4.5.1. Comando arp -a

Muestra la tabla ARP con la relación entre direcciones IP y MAC.

4.6. RARP: Reverse Address Resolution Protocol

Protocolo de Resolución de Direcciones Inverso. Se encarga de resolver las direcciones MAC a direcciones IP (versión 4). Utilizado por máquinas que desconocen al arrancar su dirección IP.

El problema de RARP es que usa una dirección de difusión limitada, con todos los bits a 1, que no es reenviada por los enrutadores.

RARP was superseded by the Bootstrap Protocol (BOOTP). This introduced the concept of a relay agent, which allowed the forwarding of BOOTP packets across networks, allowing one central BOOTP server to serve hosts on many IP subnets.

4.7. BOOTP: Bootstrap Protocol

It is a computer networking protocol used in Internet Protocol networks to automatically assign an IP address to network devices from a configuration server. The BOOTP was originally defined in RFC 951 in September 1985.

When a computer that is connected to a network is powered up and boots its operating system, the system software broadcasts BOOTP messages onto the network to request an IP address assignment. A BOOTP configuration server assigns an IP address based on the request from a pool of addresses configured by an administrator.

While some parts of BOOTP have been effectively superseded by the Dynamic Host Configuration Protocol (DHCP), which adds the feature of leases, parts of BOOTP are used to provide service to the DHCP protocol. DHCP servers also provide the legacy BOOTP functionality.

4.8. DHCP: Dynamic Host Configuration Protocol

Protocolo que permite asignar direcciones IP dinámicas a los equipos que lo soliciten de una red.

DHCP is based on BOOTP but can dynamically allocate IP addresses from a pool and reclaim them when they are no longer in use. It can also be used to deliver a wide range of extra configuration parameters to IP clients, including platform-specific parameters.

5. Protocolos de Encaminamiento

5.1. RIP: Routing Information Protocol

Es uno de los protocolos de encaminamiento más antiguos. Utiliza un algoritmo de vector distancia denominado Bellman-Fod distribuido que le permite calcular la métrica o ruta más corta posible hasta el destino a partir del número de saltos o equipos intermedios que los paquetes IP deben atravesar.

5.2. OSPF: Open Shortest Path First

Se estandarizó en los años 90s desbancando al protocolo de vector distancia RIP, que sólo funcionaba bien en sistemas pequeños. OSPF funciona mapeando el conjunto de redes, enrutadores y líneas en un **grafo dirigido**, en el que a cada arco se le asigna un coste, y calculando

la trayectoria más corta desde cada dispositivo de enrutamiento a todos los demás en base a los pesos de los arcos.

Al contrario que RIP, EIGRP o BGP, no usa TCP ni UDP, sino que se encapsula directamente sobre el protocolo IP (poniendo "89" en el campo protocolo).

5.3. EIGRP

Protocolo de encaminamiento vector distancia avanzado, propiedad de Cisco System.

5.4. EGP (Exterior Gateway Protocol)

XXXXXXXXXXX

5.5. BGP (Border Gateway Protocol)

Sustituyó a EGP. Diseñado para permitir muchos tipos de políticas de enrutamiento. Las políticas típicas comprenden consideraciones políticas, de seguridad o económicas. Se configuran manualmente en cada enrutador BGP y no son parte del protocolo mismo. Un ejemplo de restricción de enrutamiento es que el tráfico que comience o termine en una organización no debe transitar por redes de la competencia.

Tipos de mensajes BGP: Open, Update, Notification y Keepalive.

6. Protocolos de Nivel 4

6.1. TCP: Transmision Control Protocol

Se diseñó específicamente para enviar una secuencia de bits fiable a través de una interred no fiable. Orientado a conexión.

6.1.1. Formato Segmento TCP

- **Cabecera** (20 Bytes + Opciones):
  - **Puerto Origen** (2 Bytes)
  - **Puerto Destino** (2 Bytes)
  - **Sequence number** (4 Bytes)
  - **Acknowledgment number** (4 Bytes): especifica el siguiente paquete esperado.
  - **Data Offset** (4 bits): indica dónde empiezan los datos (en palabras de 32 bits). Este campo es necesario porque el campo *Opciones* es de longitud variable.
  - **Reserved data** (3 bits): para uso futuro. Debe estar a 0.

- **Flags** (9 bits): campos de control (NS, CWR, ECE, URG, ACK, PSH, RST, SYN, FIN).
- **Tamaño de la Ventana** (2 Bytes): número de paquetes que pueden enviarse desde el último ACK recibido.
- **Suma de Comprobación** (2 Bytes).
- **Urgent Pointer** (2 Bytes).
- **Opciones** (0 o más palabras de 32 bits)

▪ **Datos**: puede haber segmentos sin datos (usados para acuses de recibo y mensajes de control).

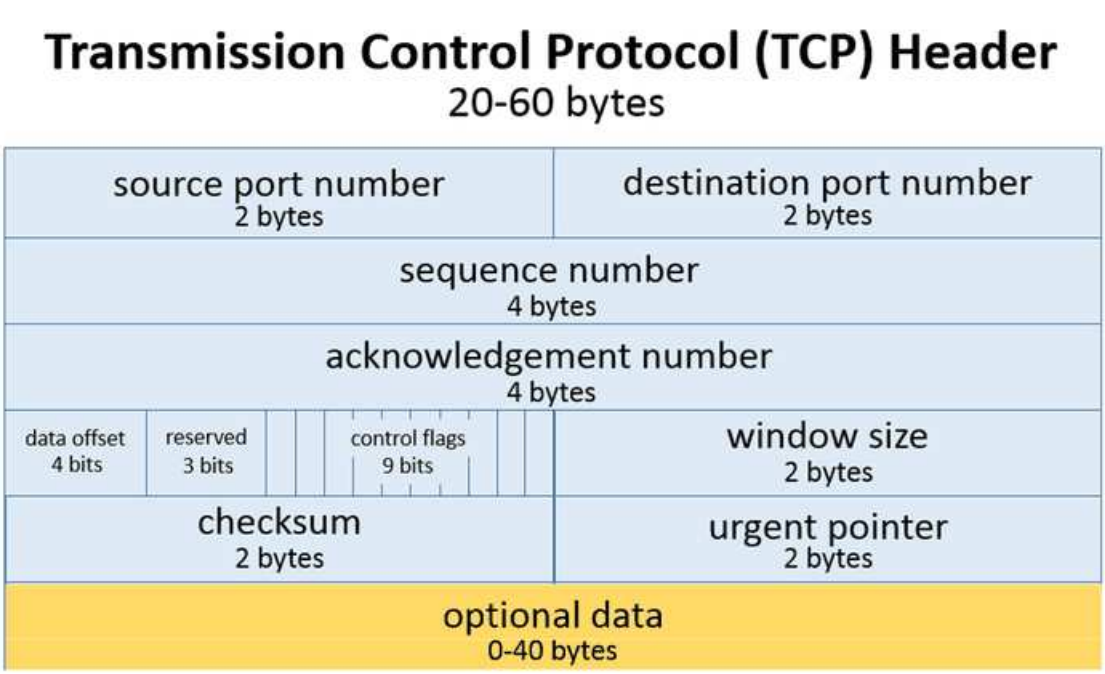

Figura 1: TCP Header.

6.2. UDP: User Data Protocol

Ofrece a las aplicaciones un mecanismo para enviar datagramas IP en bruto, encapsulados sin tener que establecer una conexión. Es una alternativa a TCP y se usa cuando una entrega rápida es más importante que una entrega garantizada. No orientado a conexión.

6.2.1. Formato Datagrama UDP

- **Cabecera** (8 Bytes):
  - **Puerto Origen** (2 Bytes)
  - **Puerto Destino** (2 Bytes)
  - **Longitud UDP** (2 Bytes): longitud incluyendo la cabecera y los datos.
  - **Suma de Comprobación** (2 Bytes): la suma es opcional.
- **Datos**

7. Protocolos de Nivel 7

7.1. FTP: File Transfer Protocol

Permite la transferencia de ficheros de texto o binarios desde un ordenador a otro sobre una conexión TCP.

El servicio se implementa a partir de dos conexiones TCP. Se establece una primera conexión (puerto 21) para el intercambio de mensajes de control (nombre de usuario, contraseña, nombres de ficheros, acciones a realizar, etc.). La segunda conexión (puerto 20 en modo activo) se establece para la transferencia de los datos.

7.1.1. Comandos FTP

Comando	Descripción
ascii	to set the mode of file transfer to ASCII
binary	to set the mode of file transfer to binary
bye	to exit the FTP environment (same as quit)
cd	to change directory on the remote machine
get	to copy one file from the remote machine to the local machine
lcd	to change directory on your local machine
ls	to list the names of the files in the current remote directory
mkdir	to make a new directory within the current remote directory
mget	to copy multiple files from the remote machine to the local machine
mput	to copy multiple files from the local machine to the remote machine
put	to copy one file from the local machine to the remote machine
pwd	to find out the pathname of the current directory on the remote machine
quit	to exit the FTP environment (same as bye)
rmdir	to to remove (delete) a directory in the current remote directory

7.1.2. Modos de Conexión

7.1.2.1. Activo

Among the two modes, Active mode is the older one. It was the mode introduced in the early days of computing when mainframes were more common and attacks to information security were not as prevalent.

Here's a simplified explanation on how an active mode connection is carried out, summarized in two steps. Some relevant steps (e.g. ACK replies) have been omitted to simplify things.

- A user connects from a random port on a file transfer client to port 21 on the server. It sends the PORT command, specifying what client-side port the server should connect to. This port will be used later on for the data channel and is different from the port used in this step for the command channel.
- The server connects from port 20 to the client port designated for the data channel. Once connection is established, file transfers are then made through these client and server ports.

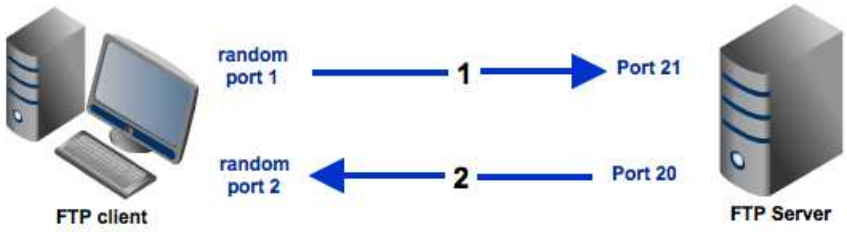

Figura 2: FTP Active Mode.

7.1.2.2. Pasivo

In passive mode, the client still initiates a command channel connection to the server. However, instead of sending the PORT command, it sends the PASV command, which is basically a request for a server port to connect to for data transmission. When the FTP server replies, it indicates what port number it has opened for the ensuing data transfer.

Here's how passive mode works in a nutshell:

- The client connects from a random port to port 21 on the server and issues the PASV command. The server replies, indicating which (random) port it has opened for data transfer.

- The client connects from another random port to the random port specified in the server's response. Once connection is established, data transfers are made through these client and server ports.

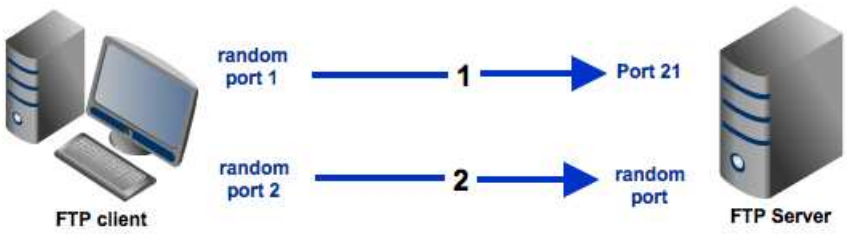

Figura 3: FTP Pasive Mode.

7.1.3. Anonymous FTP

A host that provides an FTP service may provide anonymous FTP access. Users typically log into the service with an "anonymous" (lower-case and case-sensitive in some FTP servers) account when prompted for user name. Although users are commonly asked to send their email address instead of a password, no verification is actually performed on the supplied data.

8. Comandos IP

- NETSTAT: es una herramienta de línea de comandos que muestra un listado de las conexiones activas de un ordenador, tanto entrantes como salientes. Permite mostrar las estadísticas de protocolos y las conexiones TCP/IP actuales .
- IPCONFIG: Muestra o actualiza la configuración de red TCP/IP.
- NBTSTAT: Muestra estadísticas del protocolo y conexiones TCP/IP actuales utilizando NBT. NBStat es una herramienta que resulta de utilidad para solucionar problemas con la resolución de nombres llevada a cabo por NetBIOS.
- TRACERT: muestra todas las direcciones IP intermedias por las que pasa un paquete entre el equipo ORIGEN y la dirección IP especificada.

9. Preguntas de Exámenes

1. (GSI.PI.2016.39). **¿Cuál de los siguientes es un protocolo de encaminamiento vector distancia avanzado, propiedad de Cisco System?:**

   a) EIGRP
   b) RIP
   c) OSPF
   d) BGP2

2. (GSI.PI.2016.40). **¿Qué protocolo no orientado a conexión se utiliza de forma extensa en el nivel de transporte del modelo TCP/IP?:**

   a) IP
   b) TCP
   c) UDP
   d) RPC

3. (GSI.PI.2015.34). **Los protocolos ARP y RARP se encargan de enlazar:**

   a) La sesión del usuario con la capa de transporte TCP.
   b) El nivel físico con la capa de sesión del protocolo TCP/IP.
   c) El protocolo de transporte utilizado con el nivel de red utilizado.
   d) Los sistemas de direccionamiento IP y el de la red física utilizada.

4. (GSI.PI.2015.35). **La dirección de loopback para IPv6 es:**

   a) ::127
   b) ::
   c) ff00::
   d) ::1

5. (GSI.PI.2015.36). **Según el modelo TCP/IP, el protocolo UDP pertenece a la capa de:**

   a) Aplicación.
   b) Transporte.
   c) Internet.
   d) Acceso al medio.

6. (GSI.PI.2015.37). **Entre los tipos de direccionamiento IPv6 están los siguientes:**

a) Unicast, Multicast, Anycast, Broadcast.

b) Unicast, Anycast, Broadcast.

c) Unicast, Multicast, Broadcast.

d) Unicast, Multicast, Anycast.

7. (GSI.PI.2015.38). **El protocolo de mensajes de control de Internet (ICMP) detecta y registra las condiciones de error de la red, pero NO registra:**

   a) Paquetes soltados: Paquetes que llegan demasiado rápido para poder procesarse.

   b) Fallo de conectividad: No se puede alcanzar un sistema de destino.

   c) Redirección: Redirige un sistema de envío para utilizar otro enrutador.

   d) Validación: Transmisión completa en orden de bytes.

8. (GSI.PI.2015.39). **¿Qué dirección de las indicadas es válida para un host en la subred 192.168.31.48/28?:**

   a) 192.168.31.48

   b) 192.168.31.64

   c) 192.168.31.49

   d) 192.168.31.63

9. (GSI.PI.2015.40). **La dirección IP 192.178.16.66 con la máscara de subred 255.255.255.192 se interpreta como:**

   a) Host 4 de la subred 192.178.16.66

   b) Host 2 de la subred 192.178.16.64

   c) Host 2 de la subred 192.178.16.66

   d) Host 1 de la subred 192.178.16.64

10. (GSI.PI.2015.Reserva.03). **Cuáles son las siglas (en inglés) del protocolo de separación localizador/identificador propuesto por CISCO como mecanismo de trancisión IPv4-IPv6:**

    a) RISP

    b) CISP

    c) LISP

    d) NISP

11. (GSI.PI.2014.36). **Dentro del protocolo TCP/IP, el comando arp -a:**

    a) Muestra la tabla RARP con la relación entre direcciones MAC e IP.

b) Muestra la tabla ARP con la relación entre direcciones IP y MAC.

c) Muestra la tabla ARP con la relación entre direcciones IP y puertos UDP.

d) Muestra la tabla de direcciones IP con la relación entre direcciones IP y puertos TCP.

12. (GSI.PI.2014.37). **La unidad de datos intercambiada en la capa de transporte, según el modelo OSI de ISO, es:**

a) TPDU.

b) Paquete.

c) Trama.

d) TCDU.

13. (GSI.PI.2014.38, GSI.LI.2014.40). **Señale qué número de puerto debería usarse si se quiere configurar un servicio para la autenticación de redes Kerberos:**

a) 88

b) 42

c) 74

d) 105

14. (GSI.PI.2014.39). **Indique el número de puerto que debería usarse si se quiere configurar un servicio para usar el protocolo de configuración dinámica de host DHCP para IPv6:**

a) 58

b) 169

c) 389

d) 547

15. (GSI.PI.2014.40, GSI.LI.2014.32). **¿Cuál es la dirección de red de una dirección IP: 192.168.30.200 cuya máscara es 255.255.255.128?:**

a) 192.168.30.0

b) 192.168.30.128

c) 192.168.30.255

d) 192.168.30.200

16. (GSI.PI.2013.38). **¿Cuál de las siguientes afirmaciones es correcta en relación al protocolo FTP?:**

a) En el modo activo el puerto de datos del cliente es el 20.

b) El comando "upload" permite subir un fichero al servidor.

c) Entre los tipos de acceso, está el acceso anónimo, que permite conectarse sin necesidad de usuario y contraseña.

d) El protocolo permite tres modos de conexión: activo, pasivo y bajo demanda.

17. (GSI.PI.2013.39, GSI.LI.2013.36). **Señale cuál de las siguientes opciones está basada en el protocolo ICMP:**

a) SMTP

b) SNMP

c) PING

d) DNS

18. (GSI.PI.2013.40). **Ethernet realiza la difusión recibiendo tramas con la siguiente dirección MAC de destino:**

a) 00:00:00:00:00:FF

b) FF:FF:FF:FF:FF:FF

c) FF:00:00:00:00:FF

d) 00:00:00:00:00:00

19. (GSI.PI.2011.09). **¿Cuál de los siguientes protocolos de encaminamiento se transmite directamente sobre el protocolo IP sin usar otro mecanismo de transporte?:**

a) EIGRP

b) OSPF

c) RIP

d) BGP

20. (GSI.PI.2011.28). **El protocolo de Internet versión 6 fue definido en el:**

a) RFC 2460

b) RFC 2430

c) RFC 730

d) RFC 720

21. (GSI.PI.2011.30, GSI.LI.2011.32). **El tamaño en bits del campo Puerto Destino de un paquete UDP es de:**

a) 15

b) 16

c) 14

d) 12

22. (GSI.PI.2011.34). **¿En el segmento TCP cuántos bits ocupa el campo "reserved"?:**

a) 6

b) 8

c) 4

d) 12

23. (GSI.PI.2011.38, GSI.LI.2011.39). **¿Qué indica el campo "Data Offset" en el segmento TCP?:**

a) Este campo no pertenece a TCP.

b) Indica dónde terminan los datos.

c) Indica dónde empiezan los datos.

d) Indica el número de campos de control.

24. (GSI.PI.2011.39, GSI.LI.2011.33). **La dirección IP 0.0.0.0:**

a) Se usa para difusión en una subred local.

b) Se usa para difundir un mensaje a todos los nodos de una red distante.

c) La usa inicialmente un host cuando arranca.

d) Se usa para pruebas de realimentación.

25. (GSI.PI.2010.37, GSI.LI.2010.34). **En IPv4, la cabecera IP tiene un campo denominado TTL (Time To Live) que indica el número máximo de encaminadores que un paquete puede atravesar. ¿Cuál es el rango de valores que puede tomar este campo?:**

a) 0-15.

b) 0-255.

c) 0-5.

d) 0-127.

26. (GSI.PI.2010.38). **Identificar la descripción del comando IP ERRÓNEO:**

a) NETSTAT: es una herramienta de línea de comandos que muestra un listado de las conexiones activas de un ordenador, tanto entrantes como salientes. Permite mostrar las estadísticas de protocolos y las conexiones TCP/IP actuales .

b) IPCONFIG: Muestra o actualiza la configuración de red TCP/IP.

c) NBTSTAT: Muestra estadísticas del protocolo y conexiones TCP/IP actuales utilizando NBT. NBStat es una herramienta que resulta de utilidad para solucionar problemas con la resolución de nombres llevada a cabo por NetBIOS.

d) TRACERT: muestra todas las direcciones IP intermedias por las que pasa un paquete entre el equipo remoto y la dirección IP especificada.

27. (GSI.PI.2010.39). **La máxima longitud de un datagrama IP es:**

a) 128 Kbytes.

b) 64 Kbytes.

c) 32 Kbytes.

d) No tiene longitud máxima.

28. (GSI.PI.2010.40). **¿Cuál es la versión extendida del protocolo BOOTP?:**

a) DHCP.

b) RARP.

c) RTSP.

d) DNS.

29. (GSI.PI.2008.38). **En el ámbito del modelo TCP/IP, señale cuál de las siguientes siglas identifica un algoritmo de encaminamiento:**

a) NTP (Network Time Protocol)

b) RIP (Routing Information Protocol)

c) RPC (Remote Procedure Call)

d) FTP (File Transfer Protocol)

30. (GSI.PI.2008.39). **Señale cuál es la afirmación FALSA:**

a) La arquitectura del TCP/IP consta de cinco niveles o capas en las que se agrupan los protocolos, y que se relacionan con los niveles OSI.

b) TELNET es un protocolo TCP/P.

c) El protocolo IP identifica a cada ordenador que se encuentre conectado a la red mediante su correspondiente dirección.

d) IP al igual que X.25 está orientado a conexión.

31. (GSI.PI.2008.40). **Se presentan a continuación tres niveles de la torre de protocolos TCP/IP y tres protocolos:**
1) Nivel 1 (Físico)
2) Nivel 2 (Enlace de datos)
3) Nivel 5 (Aplicación)

I) GPRS (General Packet Radio Service).
II) PLC (Power Line Communications).
III) TLS/SSL (Transport Layer Security/Secure Sockets Layer).
Señale cuál es el emparejamiento correcto de nivel/protocolo:

a) 1/I, 2/II, 3/III.

b) 1/II, 2/I, 3/III.

c) 1/III, 2/I, 3/II.

d) 1/II, 2/III, 3/I.

32. (GSI.LI.2016.35). **En IPv6, el campo Next Header define la siguiente cabecera en el datagrama, indique cuál debería ser su valor para el encabezado "opciones de destino":**

a) 0

b) 43

c) 44

d) 60

33. (GSI.LI.2016.36). **Señale la respuesta correcta, en relación a los tipos de mensajes usados en el protocolo BGP son:**

a) OPEN, KEEPALIVE, UPDATE y CLOSE.

b) OPEN, READ, WRITE, NOTIFICATION y KEEPALIVE.

c) OPEN, KEEPALIVE, NOTIFICATION y UPDATE.

d) OPEN, READ, WRITE, UPDATE y CLOSE.

34. (GSI.LI.2016.37). **Indique cuál de las siguientes es un tipo de estación definida en el protocolo HDLC (High-Level Data Link Control):**

a) Combinada

b) Simple

c) Dúplex

d) Semidúplex

35. (GSI.LI.2016.Reserva.03). **El campo "Límite de Saltos" de la cabecera IPv6 disminuye en uno en cada salto (routers intermedios) del paquete, cuando este campo contiene el valor cero el paquete:**

a) Es destruido y se envía de regreso al nodo fuente un mensaje ICMPv6 tipo 3.

b) Sigue su camino pero se envía de regreso al nodo fuente un mensaje ICMPv6 tipo 1.

c) Sigue su camino y se envía de regreso al nodo fuente un mensaje ICMPv6 tipo 4.

d) Es destruido y se envía de regreso al nodo fuente un mensaje ICMPv6 tipo 2.

36. (GSI.LI.2015.33). **El campo "versión" de la cabecera del protocolo IPv4 puede contener:**

    a) Desde 0000 hasta 1111.

    b) 0100 ó 0110.

    c) 4 y 6 en complemento a1.

    d) Siempre 1111.

37. (GSI.LI.2015.34). **Según la especificación del protocolo de encaminamiento BGP-4:**

    a) En E-BGP, los prefijos que aprende un router de un vecino no pueden ser anunciados a otro vecino mediante I-BGP.

    b) Un prefijo aprendido de un vecino mediante I-BGP no puede reanunciarse a otro vecino por I-BGP.

    c) Es un protocolo que funciona sobre TCP por el puerto 169.

    d) En un protocolo que funciona sobre UDP por el puerto 169.

38. (GSI.LI.2014.38). **Una red TCP usa el protocolo de ventana deslizante como mecanismo de control de flujo. Supongamos que se establece el tamaño de la ventana en 4 y los paquetes se numeran del 1 en adelante. Con estas condiciones, el emisor podrá enviar al receptor el paquete número 5:**

    a) Únicamente cuando reciba el ACK del paquete 4.

    b) Cuando haya recibido al menos dos ACK.

    c) Cuando reciba cualquier ACK.

    d) Cuando se cumpla el timeout de envío del paquete 1.

39. (GSI.LI.2014.39). **¿Cuál de las siguientes respuestas NO se considera una de las cuatro primitivas de servicio que define el modelo OSI de ISO para la comunicación entre niveles?:**

    a) Request.

    b) Invoke.

    c) Response.

    d) Confirmation.

40. (GSI.LI.2011.38). **¿Cuál de los siguientes NO es un tipo de dirección en IPv6?:**

a) Broadcast.

b) Anycast.

c) Multicast.

d) Unicast.

41. (GSI.LI.2010.35). **¿Cuál de los siguientes NO es un campo de control en el segmento TCP?:**

a) URG.

b) PSH.

c) END.

d) ACK.

42. (GSI.LI.2008.21). **El encaminamiento mediante algoritmos que se ejecutan en los nodos de la red con los últimos datos que han recibido sobre su estado y convergen rápidamente optimizando sus nuevas rutas se denomina:**

a) Encaminamiento adaptativo distribuido.

b) Encaminamiento adaptativo centralizado.

c) Encaminamiento adaptativo aislado.

d) Encaminamiento determinístico estático.

43. (GSI.LI.2008.21). **XXX:**

a) .

b) .

c) .

d) .

10. Soluciones

1. A
2. C
3. D
4. D
5. B
6. D
7. D
8. C
9. B
10. C
11. B
12. A
13. A
14. D
15. B
16. C
17. C
18. B
19. B
20. A
21. B
22. C
23. C
24. C
25. B
26. D
27. B
28. A
29. B
30. Anulada
31. B
32. D
33. C
34. A
35. A
36. B
37. B
38. C
39. B
40. A
41. C
42. A

Referencias

[1] Active v.s. Passive FTP Simplified - Understanding FTP Ports - JScape
http://www.xxx.xx/xx/xxx/xxx/xxx