BLOQUE PROTOCOLOS

TEMAS 110 y 114

TEMA 110

El modelo de referencia de interconexión de sistemas abiertos (OSI) de iso: Arquitectura, capas, interfaces, protocolos, direccionamiento y encaminamiento

TEMA 114

Redes IP: Arquitectura de redes, encaminamiento y calidad de servi-cio. Transición y convivencia IPV4 - IPV6. Funcionalidades específicas de IPV6

Bloque PROTOCOLOS

1. INTRODUCCIÓN

Este bloque está dedicado a los fundamentos más teóricos de las comunicaciones en redes de telecomunicaciones, comenzando por el modelo OSI, que no tiene implantanción real pero que sirve de referencia a los demás, y siguiendo por el modelo TCP/IP, que es el que predomina en las redes actuales (pero no el único). Se incluyen, además, contenidos de otros protocolos básicos de este modelo y un repaso del protocolo HTTP, protocolo fundamental de la WWW. Finalmente, se expone el protocolo IPv6: características básicas, diferencias con IPv4, adaptación e integración con IPv4, etc.

2. MODELOS DE REFERENCIA DE INTERCONEXIÓN DE SISTEMAS

- SNA (de IBM)
- OSI
- IPX/SPX (en redes Novell Netware)
- TCP/IP

Nota: SPX~TCP, IPX~IP

3. MODELO OSI (OPEN SYSTEMS INTERCONNECTION)

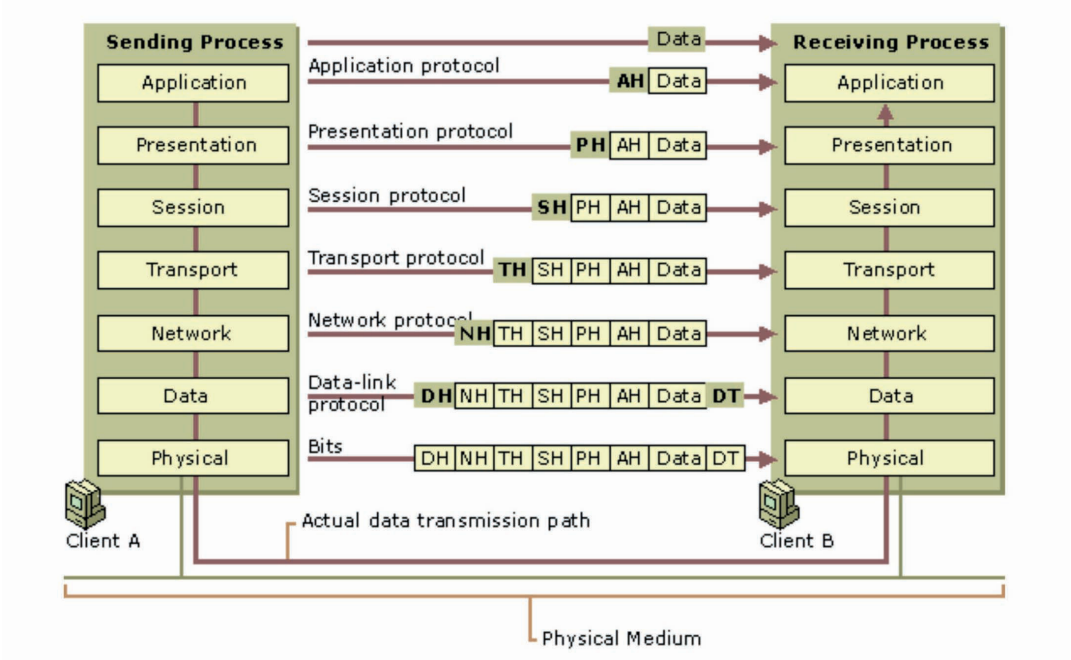
Modelo conceptual estandarizado por ISO (ISO/IEC 7498-1) y por ITU-T (estándar ITU-T X.200).

Conceptos básicos:

- **Protocolo**: conjunto de reglas perfectamente organizadas y convenidas de mutuo acuerdo entre los participantes en una comunicación.
- **Capas**: abstracción mediante la cual se reparten e independizan las diferentes funciones relativas a la comunicación realizadas por un sistema.
- **Servicios**: las capas prestan servicios a las de nivel superior para facilitar la comunicación
- **Primitivas** de servicio: funciones realizadas por los servicios en la interacción entre capas
- **Interfaz**: conjunto de reglas e información requerida para invocar un determinado servicio

3.1 CAPAS

El modelo OSI, en su recomendación X.200, presenta 7 capas o niveles.



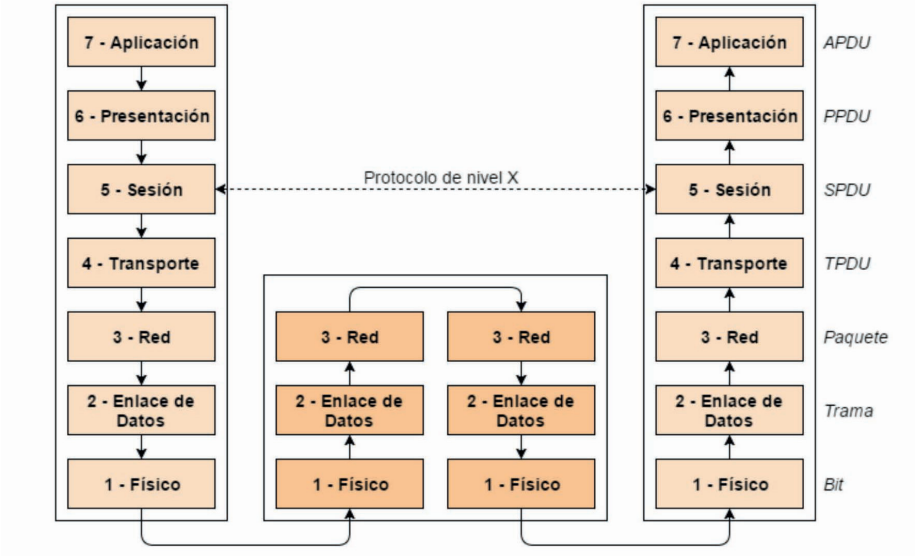
1. **Físico**: características físicas de la transmisión y los interfaces. Señal eléctrica, codificación y modulación, cables, conectores, etc.
2. **Enlace de Datos**: comunicación fiable entre dos nodos conectados a la misma capa física. Se encarga de dos tareas diferentes, por lo que típicamente tiene 2 subniveles:
   A. Construir tramas a partir de bits → LLC (Logical Link Control)
   B. Compartir el acceso al medio → MAC (Media Access Control)
3. **Red**: gestión y envío de paquetes a lo largo de una red estructurada formada por múltiples nodos. Proporciona direccionamiento, encaminamiento (routing) y control de tráfico. Ejemplo: IP
4. **Transporte**: transmisión fiable extremo a extremo, incluyendo segmentación, confirmación y multiplexación. OSI define 5 tipos de protocolos de transporte (TP0...TP4), siendo 4 el más completo, soportando detección y corrección de errores y control de flujo, por ejemplo. Es el tipo más cercano a TCP, si bien presenta algunas diferencias, como que un tipo TP4 puede ser sin conexión.
5. **Sesión**: gestión de sesiones de comunicación. Proporciona, entre otras funciones, control del diálogo (full-duplex o half-duplex), recuperación en caso de errores, etc.
6. **Presentación**: conversión de códigos entre nodos, cifrado, compresión de datos, etc.
7. **Aplicación**: interfaz directo con los procesos de usuario

3.2 COMUNICACIÓN, SERVICIOS E INTERFACES

Cada capa se comunica:

- **de forma lógica:** con la misma capa del otro extremo de la comunicación. El conjunto de datos intercambiados + la cabecera del protocolo de esta capa se denomina PDU (Protocol Data Unit).
- **de forma "real":** con la capa inferior mediante los servicios que ésta expone. Para ello emplea el interfaz que le presenta la capa inferior. La información recibida por esta interfaz se denomina IDU (Interface Data Unit) y se compone de la SDU (Service Data Unit) + la ICI (Interface Control Information).

Así pues:



PDU (n) = datos + cabecera del protocolo de nivel n intercambiados con la capa n del extremo de la comunicación

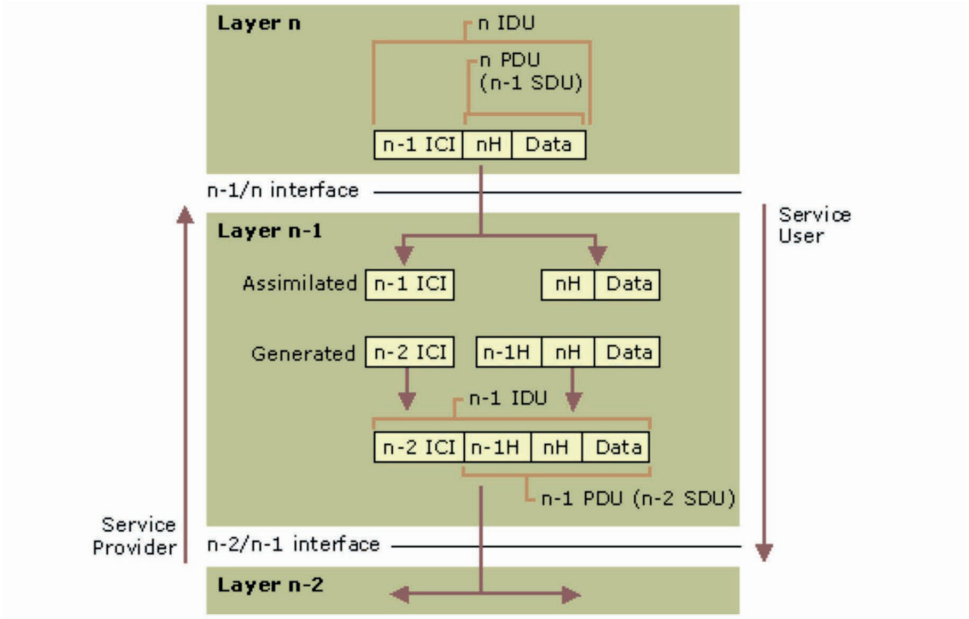
SDU (n) = datos + cabecera del nivel n+1 que recibe el servicio del nivel n para su procesamiento. Lógicamente: **SDU (n-1) = PDU (n)**

ICI (n) = información adicional al SDU (n) que la capa n+1 añade al invocar el servicio

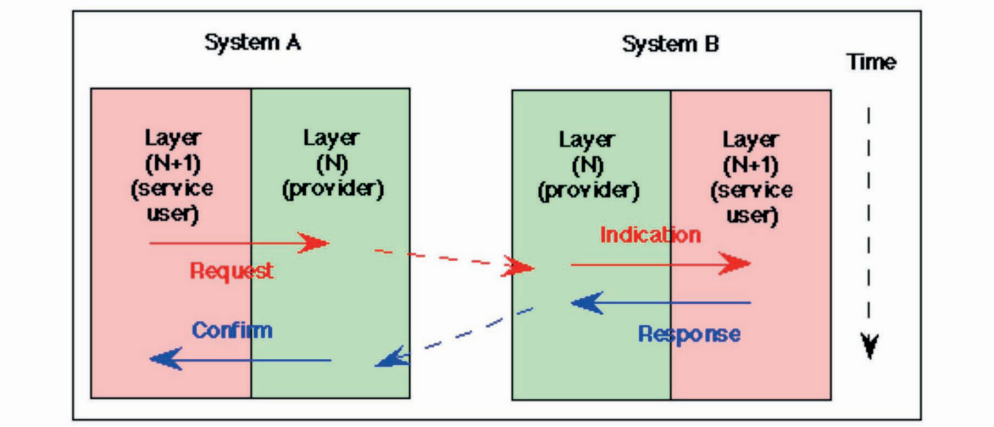
IDU (n) = ICI (n-1) + SDU (n-1)

Los servicios presentan las siguientes primitivas (las dos últimas únicamente en los servicios con confirmación, los no confirmados solo las dos primeras):

- Request
- Indication



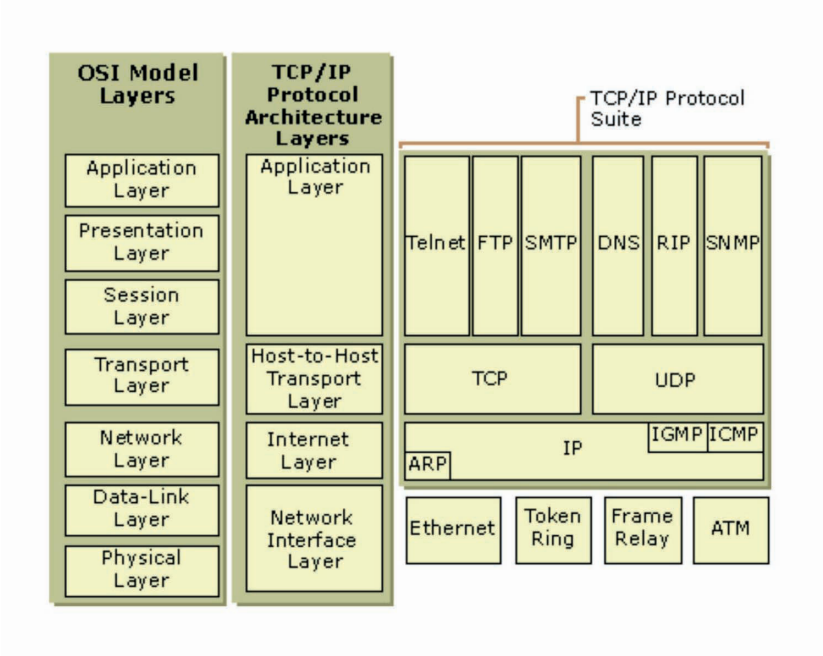
- Response



- Confirm

3.3 PARALELISMO ENTRE EL MODELO OSI Y TCP/IP (DARPA)

Existe un paralelismo bastante directo entre el modelo OSI y el modelo TCP/IP (o DARPA). La capa del modelo DARPA "Network Interface" muchas veces se denomina como "capa de acceso a la red", mientras que la capa "Internet" a veces se denomina como "Network".



4. IPV4

Internet Protocol (IP) nació como un proyecto para comunicar una serie de máquinas dentro de la red ARPANET, del departamento de defensa ARPA (posteriormente llamado DARPA). Su función principal es enviar los datagramas o segmentos (sus SDU, o PDU de nivel de transporte) hasta el otro extremo de la comunicación. La versiones actuales son la 4 y la 6, siendo las 0...3 versiones experimentales durante los años 1977 al 1979. La versión 4 es descrita en la RFC 791 por el IETF.

Principales características:

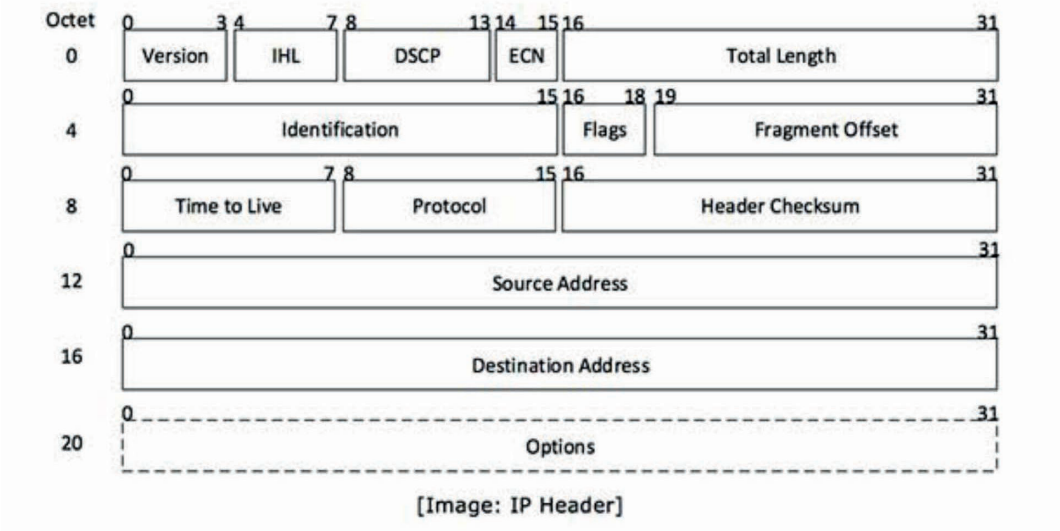
- Proporciona direccionamiento inter-red, permitiendo comunicar diferentes redes entre sí
- No orientado a conexión => cada paquete sigue su propio camino, la red es "sin estado"
- Fragmenta y reensambla. **Puede fragmentar en cualesquiera puntos del camino entre los dos extremos. Reensambla en el destino**

IPv6 fragmenta solo en origen

- No fiable: best effort => no garantiza:
- Que no se desordenen los paquetes
- Que no se pierdan
- Que no haya duplicidades

Si hay error se descarta el paquete. No se obliga a notificar (ICMP). IPv6 ya no tiene checksum

- Que no se corrompan los datos (tiene CRC para detección de errores únicamente en la cabecera pero no corrige, se lo deja al nivel superior)



[Image: IP Header]

4.1 CABECERA IP

- Version: 4 ó 6
- IHL (IP Header Length): longitud de la cabecera en palabras de 32 bits (múltiplos de 4 bytes).
  - Valor máximo = 1111 = 15 => 60 bytes
  - Valor mínimo = 0101 = 5 => 20 bytes (es el más usual)
- DSCP (Differentiated Services Code Point): se emplea para DiffServ. Hay recomendaciones pero el uso es arbitrario en cada red
- ECN (Explicit Congestion Notification): es opcional y se emplea si ambos extremos están de acuerdo. En lugar de descartar paquetes en caso de congestión se marca con un flag y, cuando llega a destino, éste informa al origen de que reduzca la tasa de envío.
- Total length: tamaño del paquete entero en bytes, incluyendo la cabecera. Si este paquete proviene de uno mayor fragmentado, este campo indica el tamaño de este fragmento en particular, no del total.
- Valor máximo = 1111 1111 1111 1111 = 65535 bytes. Todos los hosts deben ser capaces de reensamblar como mínimo 576 bytes => no se puede fragmentar un paquete menor o igual a 576 bytes.

- Identification: para identificar el grupo de fragmentos de un datagrama (conjunto de paquetes). Igual para todos los fragmentes del paquete original.
- Flags:
  - primer bit debe ser cero
  - segundo bit: DF (Don›t Fragment): si hay que fragmentar y está a 1 se tira el paquete
  - tercer bit: MF (More Fragments): cuando se fragmenta se pone a 1 salvo el último paquete
- Fragment Offset: offset respecto al paquete original antes de fragmentarlo. Se mide en palabras de 64 bits (bloques de 8 bytes).
- TTL (Time To Live): originalmente eran segundos. Ahora son número de saltos máximos. Se mide en bits. Cuando llega a cero se descarta el paquete y se notifica mediante ICMP Time Exceded
- Protocol: identifica al protocolo usado en la parte de datos. IANA mantiene la numeración
- Checksum: CRC de 16 bits para la cabecera. Se recalcula en cada salto debido a que el TTL disminuye
- Source Address: 32 bits para la dirección origen, representadas como 4 octetos
- Destination Address: 32 bits para la dirección destino, representadas como 4 octetos
- Options: prácticamente no usado. Pueden ocupar hasta 40 bytes en múltiplos de palabras de 32 bits.

Algunos identificadores de protocolos significativos son los siguientes:

ICMP	1
IGMP	2
TCP	6
UDP	17
RDP	27
ENCAP	41
GRE	47
EIGRP	88
OSPF	89

Class	Leading bits	Size of *network number* bit field	Size of *rest* bit field	Number of networks	Addresses per network	Start address	End address
Class A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127.255.255.255
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255
Class D (multicast)	1110	not defined	not defined	not defined	not defined	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	240.0.0.0	255.255.255.255

4.2 DIRECCIONAMIENTO CLASSFULL

Las direcciones 127.*.*.* son parte de la clase A, si bien están reservadas para loopback.

La clase D está reservada para multicast y no puede ser empleada para otra cosa.

La clase E está reservada y no puede se empleada en Internet.

```
Class A
  0.  0.  0.  0 = 00000000.00000000.00000000.00000000
127.255.255.255 = 01111111.11111111.11111111.11111111
                  0nnnnnnn.HHHHHHHH.HHHHHHHH.HHHHHHHH

Class B
128.  0.  0.  0 = 10000000.00000000.00000000.00000000
191.255.255.255 = 10111111.11111111.11111111.11111111
                  10nnnnnn.nnnnnnnn.HHHHHHHH.HHHHHHHH

Class C
192.  0.  0.  0 = 11000000.00000000.00000000.00000000
223.255.255.255 = 11011111.11111111.11111111.11111111
                  110nnnnn.nnnnnnnn.nnnnnnnn.HHHHHHHH
```

4.3 DIRECCIONAMIENTO Y ENRUTAMIENTO CLASSLESS (CIDR)

CIDR (Classless Inter-Domain Routing). Mucho más potente que el anterior, se basa en el uso de máscaras de red de longitud variable (VLSM, Variable-length Subnet Masking).

La máscara indica que los bits puestos a "1" son parte de la subred, no pudiendo formar parte de la parte de host de la dirección IP. Si cambia alguno de los bits identificados con "1" por la máscara el dispositivo forma parte de una subred diferente.

Ejercicio de notación CIDR: indicar todas las direcciones disponibles para hosts en la red 10.50.5.0/22.

Deducciones:

- **Al ser /22 la máscara es = 255.255.252.0 (1111 1111 . 1111 1111 . 1111 1100 . 0000 0000)**
  - **Esto quiere decir que el primer y el segundo octeto de la dirección están totalmente bloqueado para la subred**
  - **El tercer octeto tiene bloqueados los 6 primeros bits en la subred, pudiendo emplear 2 de ellos para la parte del host. Concretamente: 5 = 0000 0101 (parte de la subred en negrita).**
- **Dirección o identificación de red: deben ponerse a 0 TODOS los bits de la parte del host, luego la dirección es: 10.50.4.0 (nótese que el tercer octeto será 0000 0100)**
- **Dirección de broadcast de red: deben ponerse a 1 TODOS los bits de la parte del host, luego la dirección es: 10.50.7.255**

Resultado:

- **Dirección de red en notación CIDR: 10.50.4.0/22 (10.50.5.0/22 no es incorrecta pero llama a engaño, esta trampa está hecha para que no se te olvide).**
- **Primera dirección disponible para un host: 10.50.4.1**
- **Última dirección disponible para un host 10.50.7.254**
- **Dirección de broadcast de la red: 10.50.7.255**

Casos particulares del CIDR:

- 0.0.0.0/0 identificaría a todo Internet
- *.*.*.*/32 identificaría a un host concreto, no a una red
- *.*.*.*/31 no permite redes, solo enlaces punto a punto (dos direcciones disponibles)

Los siguientes rangos tienen usos reservados:

- 10.0.0.0/8: direccionamiento privado, especificado en la RFC 1918
- 127.0.0.0/8: loopback
- 169.254.0.0/16: por defecto cuando el host no consigue dirección (ej.: falla DHCP)
- 172.16.0.0/12: direccionamiento privado, especificado en la RFC 1918
- 192.168.0.0/16: direccionamiento privado, especificado en la RFC 1918
- 224.0.0.0/4: reservadas para multicast
- 255.255.255.255/32: broadcast

4.4 ASIGNACIÓN DE DIRECCIONES

La IANA (departamento de ICANN, empresa privada americana sin ánimo de lucro) se encarga de supervisar la asignación de IPs, números de AS, zonas root DNS, etc.

Delega en 5 registros internacionales la asignación de IPs:

- AFRINIC (África)
- ARIN (USA, Canadá, Antártida y algunas islas del Caribe)
- APNIC (Asia-Pacífico)
- LACNIC (Centro y Sudamérica)
- RIPENIC (Europa, Rusia, Oriente Medio y Asia Central)

4.5 CLASES DE SERVICIOS: INTSERV VS DIFFSERV

Para implementar calidad de servicio se han seguido dos aproximaciones: Integrated Services (IntServ) y Differentiated Services (DiffServ).

IntServ es un sistema de QoS con un control muy fino. Pretende que todos los routers del sistema implementen IntServ y que todas las aplicaciones que quieran usarlo realicen una reserva de recursos. Se se apoya en el protocolo RSVP para anunciar esa reserva y en Flow Specs para describir los flujos a priorizar y el tipo de reserva que necesitan.

DiffServ, por contra, ofrece un control más grueso y arbitrario, dejando los detalles a los administradores de a red. Emplea los 6 bits DSCP de la cabecera para crear una serie de clases de tráfico que condicionan el comportamiento de los routers salto a salto. El tráfico es marcado a la entrada y salida de la red. Si bien se deja libertad al operador para implementar DiffServ se suelen emplear las siguientes clases:

- Default PHB (Per-Hop Behaviour): es lo mismo que best effort
- EF PHB (Expedited Forwarding): para tráfico con bajas pérdidas y poca latencia
- AF PHB (Assured Forwarding): garantiza la entrega bajo ciertas condiciones
- Class Selector PHB: para compatibilidad hacia atrás en el uso del campo TOS (Type Of Service), que antiguamente agrupaba los campos DSCP y ECN

En la actualidad DiffServ se ha impuesto totalmente.