

# Redes y Comunicaciones

<b>INSTITUCIONALES .....</b>	1
<b>¿Cómo está organizado este texto? .....</b>	5
<b>Introducción .....</b>	6
<b>Esquema .....</b>	9
<b>Situación profesional 1: ¿Cuál es la red que necesitamos? .....</b>	10
<b>SP1 / H1: Usos de las redes de datos .....</b>	11
<b>SP1 / Autoevaluación 1 .....</b>	16
<b>SP1 / H2: La filosofía Cliente - Servidor y los Sistemas Operativos Actuales .....</b>	19
<b>SP1 / Autoevaluación 2 .....</b>	22
<b>SP1 / H3: Clasificaciones de redes de datos .....</b>	26
<b>SP1 / Autoevaluación 3 .....</b>	31
<b>SP1 / Ejercicio resuelto .....</b>	35
<b>SP1 / Ejercicio por resolver .....</b>	36
<b>SP1 / Evaluación de paso .....</b>	37
<b>Situación profesional 2: ¿Cómo cuantificar la información que necesitamos? Modelos de Información .....</b>	41
<b>SP2 / H1: Concepto de símbolos, datos e información .....</b>	42
<b>REFERENCIAS 1 .....</b>	48
<b>SP2 / Autoevaluación 1 .....</b>	50
<b>SP2 / H2: Cantidad de información .....</b>	54
<b>REFERENCIAS 2 .....</b>	68
<b>SP2 / Autoevaluación 2 .....</b>	69
<b>SP2 / H3: Entropía, capacidad de los sistemas y Ley de Shannon .....</b>	73
<b>REFERENCIAS 3 .....</b>	83
<b>SP2 / Autoevaluación 3 .....</b>	85
<b>SP2 / Ejercicio resuelto .....</b>	88
<b>SP2 / Ejercicio por resolver .....</b>	89
<b>SP2 / Evaluación de paso .....</b>	90
<b>Situación profesional 3: ¿Qué modelo de referencia utilizaremos? Modelos multicapa: elm modelo del referencia OSI .....</b>	94
<b>SP3 / H1: Principio de funcionamiento de los modelos multicapa .....</b>	95

SP3 / Autoevaluación 1 .....	107
<i>SP3 / H2: Las Capas de Acceso al Medio: Física y Enlace de Datos</i> .....	111
SP3 / Autoevaluación 2 .....	116
<i>SP3 / H3: Las Capas Medianas: Red y Transporte</i> .....	120
SP3 / Autoevaluación 3 .....	127
<i>SP3 / H4: Las Capas Superiores: Sesión, Presentación y Aplicación</i> .....	131
SP3 / Autoevaluación 4 .....	137
<i>SP3 / Ejercicio resuelto</i> .....	141
<i>SP3 / Ejercicio por resolver</i> .....	142
<i>SP3 / Evaluación de paso</i> .....	143
<b>Situación Profesional 4: ¿Qué características tendrá nuestra red? Las redes de área local (LAN)</b>	
.....	147
<i>SP4 / H1: Introducción a las Redes de Área Local (LAN)</i> .....	148
REFERENCIAS 4 .....	151
SP4 / Autoevaluación 1 .....	152
<i>SP4 / H2: Los Métodos de Acceso al Medio en las redes LAN</i> .....	155
REFERENCIAS 5 .....	159
SP4 / Autoevaluación 2 .....	160
<i>SP4 / H3: La red Ethernet</i> .....	164
REFERENCIAS 6 .....	167
SP4 / Autoevaluación 3 .....	168
<i>SP4 / H4: El Control de Acceso al medio utilizado por Ethernet (CSMA/CD)</i> .....	172
SP4 / Autoevaluación 4 .....	179
<i>SP4 / H5: Definiciones de tramas. Los estándares IEEE 802.x</i> .....	183
SP4 / Autoevaluación 5 .....	186
<i>SP4 / Ejercicio resuelto</i> .....	190
<i>SP4 / Ejercicio por resolver</i> .....	191
<i>SP4 / Evaluación de paso</i> .....	192
<b>Situación profesional 5: Qué topologías, dispositivos y cables utilizar? La capa Física de las redes</b> .....	196
<i>SP5 / H1: Topologías básicas de redes LAN</i> .....	197
REFERENCIAS 7 .....	204

SP5 / Autoevaluación 1 .....	205
SP5 / H2: Nivel físico Ethernet .....	208
SP5 / Autoevaluación 2 .....	225
SP5 / H3: Estándares para el cableado .....	228
REFERENCIAS 8 .....	238
SP5 / Autoevaluación 3 .....	239
SP5 / H4: Estándares inalámbricos y distintos tipos de dispositivos de conexión .....	242
REFERENCIAS 9 .....	246
SP5 / Autoevaluación 4 .....	251
SP5 / H5: El Sistema de Cableado - Estándares y Diseño .....	255
SP5 / Autoevaluación 5 .....	267
SP5 / Ejercicio resuelto .....	270
SP5 / Ejercicio por resolver .....	271
SP5 / Evaluación de paso .....	272
<b>Situación profesional 6: Qué modelo de aplicación práctica utilizaremos? El Modelo TCP/IP ...</b>	
276	
SP6 / H1: El modelo arquitectónico de Internet .....	277
SP6 / Autoevaluación 1 .....	282
SP6 / H2: Arquitectura TCP/IP: capas de Acceso ala Red e Interred .....	286
SP6 / Autoevaluación 2 .....	296
SP6 / H3: Capas de transporte y aplicación .....	299
SP6 / Autoevaluación 3 .....	307
SP6 / H4: Máxima Unidad de Transferencia (MTU) .....	310
SP6 / Autoevaluación 4 .....	316
SP6 / H5: Diferentes tipos de interconexión .....	319
REFERENCIAS 10 .....	324
SP6 / Autoevaluación 5 .....	325
SP6 / Ejercicio resuelto .....	329
SP6 / Ejercicio por resolver .....	337
SP6 / Evaluación de paso .....	338
<b>Situación profesional 7: Cómo diseñar nuestra red LAN? Diseño de la red .....</b>	342
SP7 / H1: Objetivos de diseño .....	343
SP7 / Autoevaluación 1 .....	345

<i>SP7 / H2: Descripción de la solicitud de red</i>	349
SP7 / Autoevaluación 2	353
<i>SP7 / H3: Metodología para el diseño de redes</i>	357
REFERENCIAS 11	362
SP7 / Autoevaluación 3	363
<i>SP7 / H4: Consideraciones antes de comenzar con el diseño</i>	367
SP7 / Autoevaluación 4	369
<i>SP7 / Ejercicio resuelto</i>	373
REFERENCIAS 12	386
<i>SP7 / Ejercicio por resolver</i>	387
<i>SP7 / Evaluación de paso</i>	388
<b>Situación profesional 8: ¿Cómo será el direccionamiento de nuestra red? La capa de red. El protocolo Internet (IP)</b>	392
<i>SP8 / H1: La entrega de datos</i>	393
REFERENCIAS 13	400
SP8 / Autoevaluación 1	401
<i>SP8 / H2: Direcciones IP</i>	405
REFERENCIAS 14	423
SP8 / Autoevaluación 2	425
<i>SP8 / H3: Introducción al Ruteo IP</i>	429
REFERENCIAS 15	436
SP8 / Autoevaluación 3	437
<i>SP8 / Ejercicio resuelto</i>	441
<i>SP8 / Ejercicio por resolver</i>	443
<i>SP8 / Evaluación de paso</i>	445
<b>Situación profesional 9: Necesitaremos Subredes u Súper-redes? Extensiones de Dirección de subred</b>	449
<i>SP9 / H1: Problema del agotamiento de las direcciones IP por clases</i>	450
REFERENCIAS 16	456
SP9 / Autoevaluación 1	457
<i>SP9 / H2: Extensiones de Dirección de Subred</i>	461
SP9 / Autoevaluación 2	473

<i>SP9 / H3: VLSM: Máscaras de Subred de Longitud Variable</i> .....	477
<i>SP9 / Autoevaluación 3</i> .....	485
<i>SP9 / H4: Direccionamiento de Superred (CDIR)</i> .....	489
<i>REFERENCIAS 17</i> .....	494
<i>SP9 / Autoevaluación 4</i> .....	495
<i>SP9 / H5: DNS (Domain Name System)</i> .....	498
<i>REFERENCIAS 18</i> .....	505
<i>SP9 / Autoevaluación 5</i> .....	506
<i>SP9 / Ejercicio resuelto</i> .....	509
<i>SP9 / Ejercicio por resolver</i> .....	518
<i>SP9 / Evaluación de paso</i> .....	519
<b>Situación profesional 10: Necesitaremos confiabilidad y/o velocidad? La capa de Transporte.</b>	
<b>Los protocolos TCP y UDP</b> .....	523
<i>SP10 / H1: La Capa de Transporte en TCP/IP</i> .....	524
<i>REFERENCIAS 19</i> .....	527
<i>SP10 / Autoevaluación 1</i> .....	528
<i>SP10 / H2: Protocolo de Datagramas de Usuario - UDP</i> .....	532
<i>SP10 / Autoevaluación 2</i> .....	537
<i>SP10 / H3: Protocolo de Control de Transmisión - TCP</i> .....	541
<i>SP10 / Autoevaluación 3</i> .....	547
<i>SP10 / H4: Mecanismos de establecimiento y fin de conexión</i> .....	551
<i>SP10 / Autoevaluación 4</i> .....	554
<i>SP10 / H5: Mecanismos para control de flujo</i> .....	557
<i>REFERENCIAS 20</i> .....	563
<i>SP10 / Autoevaluación 5</i> .....	564
<i>SP10 / H6: El modelo cliente-servidor</i> .....	568
<i>SP10 / Autoevaluación 6</i> .....	575
<i>SP10 / H7: Protocolos, Puertos (Ports) y Conectores (Sockets)</i> .....	579
<i>SP10 / Autoevaluación 7</i> .....	586
<i>SP10 / Ejercicio resuelto</i> .....	590
<i>SP10 / Ejercicio por resolver</i> .....	593
<i>SP10 / Evaluación de paso</i> .....	594
<b>Situación profesional 11: Dispositivos de networking</b> .....	598

<i>SP11 / H1: Dispositivos de Conectividad: Capas 1 y 2: Repetidor, Hub, NIC, Bridge y Switch</i>	599
REFERENCIAS 21	617
<i>SP11 / Autoevaluación 1</i>	618
<i>SP11 / H2: Dispositivos de conectividad: Capas 3 a 7: Router, Firewall e IDS</i>	622
<i>SP11 / Autoevaluación 2</i>	628
<i>SP11 / H3: VLAN (Virtual LAN)</i>	632
<i>SP11 / Autoevaluación 3</i>	635
<i>SP11 / Ejercicio resuelto</i>	638
<i>SP11 / Ejercicio por resolver</i>	639
<i>SP11 / Evaluación de paso</i>	640
<b>Cierre</b>	644
<b>Bibliografía</b>	646

## AGRADECIMIENTOS

Agradecemos a todos aquellos que han aportado su investigación, su experiencia y su tiempo para la elaboración de este TID.

Especialmente a Norberto CURA por haber ofrecido el texto que se utilizó como base para hacer este. Agradecemos, finalmente, a Fernando FRIAS, Director de la Carrera de Análisis de Sistema del Colegio Universitario IES.

---

## AUTORES



Antonio Víctor Pérez Espaón

- Ingeniero de Sistemas, egresado del Instituto Universitario Aeronáutico.
  - Analista de Sistemas, egresado del Instituto Universitario Aeronáutico.
  - Licenciado en Sistemas Aéreos y Aeroespaciales, egresado del Instituto Universitario Aeronáutico.
  - Técnico Superior en Administración, egresado del Instituto Universitario Aeronáutico.
  - Jefe de los Departamentos de Coordinación, Informática y Control de Gestión de la Escuela de Suboficiales de la Fuerza Aérea.
  - Docente del *Colegio Universitario IES* y docente universitario desde 1999 a la fecha.
  - Coautor del texto de estudio Hardware, para educación semi-presencial.
  - Cursa actualmente MBA en Dirección de Sistemas de Información en la Universidad del Salvador.
- 

## EQUIPO DE PRODUCCIÓN

### Producción y dirección general

- Director general: Alberto Rabbat
- Directora Académica: María Fernanda Sin
- Vicedirectora Académica: María Teresa de las Casas

## Planificación y coordinación general

- Coordinador de estudios a distancia: Érica Bongiovanni

## Producción Multimedial

- Sebastian Benito
- Nicolás Irusta
- Sabrina Monteverde
- Facundo Moreno
- Diego Oliva

## Producción Académica

- Ana Paula Gamba
- Ana Giró
- Telmo Torres

## Coordinación de sistemas

- Marcela Giraudo
- Marco Moretti

## Diseño y Desarrollo

- M. Rosario Figueroa
- G. Alejandro Zabala

---

## USO DE MARCAS

### Cláusulas de uso de marcas y derechos de autor de terceros.

#### A. Uso atípico de marca ajena: Exclusión de los usos no comerciales del Derecho

Marcario.PERSPECTIVAS S.A. en su carácter de titular de los derechos intelectuales sobre la presente obra declara por esta vía que el uso que realiza de marcas comerciales de terceros lo es sólo a los fines informativos y didácticos, para mejor comprensión de los lectores y alumnos del contenido de la obra, siendo el mismo de carácter atípico (uso atípico de marca ajena) y lícito. Este uso, a tenor de la jurisprudencia vigente queda fuera del ius prohibendi, que detenta el titular de cada marca registrada, atento no ser el mismo de carácter comercial en relación al producto que distinguen las referidas marcas, y por ende de índole marcario.-

#### B. Uso de derechos de autor en videos, diskettes, imágenes y audio: Libre utilización -Uso privado- de obras protegidas. PERSPECTIVAS S.A. en su carácter de titular de los derechos intelectuales sobre la presente obra declara por esta vía que el uso que realiza de determinadas grabaciones (audio y video), e imágenes (fotografías) de terceros, lo es a los fines informativos y didácticos, para mejor

comprensión de los alumnos del contenido de la obra, siendo el mismo de carácter privado y no comercial, y desde ya respetando el derecho de cita, esto es declarando en toda ocasión la cita o fuente (obra y autor) de la cual se toman los fragmentos de obras de terceros para incorporarlos a la presente (Convenio de Berna, Acta de París, 1971 – Art. 10, § 2 y § 3).-

C. Modificación de obras literarias por el titular de los derechos patrimoniales: PERSPECTIVAS S.A. en su carácter de titular de los derechos intelectuales (patrimoniales) sobre la presente obra, Relaciones Sindicales, aclara que ha autorizado a su modificación a Víctor PÉREZ ESPAÑÓN respecto de la obra original, publicada por Editorial IES Siglo 21, en julio de 2010 bajo N° de ISBN 978-987-1161-52-2, constituyéndose en autor moral Norberto CURA de la obra referida y modificada. Se declara a todo efecto, que los derechos intelectuales se ceden y mantienen a favor de su titular PERSPECTIVAS S.A.

---

## COPYRIGHT

Pérez Espaón, Víctor.

**Redes y comunicaciones** / Víctor Pérez Espaón. ; coordinado por María Teresa de las Casas; dirigido por José Alberto Rabbat. - 1a ed. - Córdoba : IES Siglo 21, 2012.

E-Book.

ISBN 978-987-600-261-5

1. Informática. 2. Redes. 3. Comunicaciones. I. Casas, María Teresa de las, coord. II. José Alberto Rabbat, dir.

CDD 005.3

1er Edición

© 2012 - Editorial IES Siglo 21

Buenos Aires 563

TE: 54-351-4211717

5000 - Córdoba

Queda hecho el depósito que establece la Ley 11723

Libro de edición argentina

No se permite la reproducción parcial o total, el almacenamiento, el alquiler, la transmisión o la transformación de este libro, en cualquier forma o por cualquier medio, sea electrónico o mecánico, mediante fotocopias, digitalización u otros métodos, sin el permiso previo y escrito del editor. Su infracción está penada por las leyes 11723 y 25446.

Se terminó de replicar durante el mes de diciembre de 2012 en el departamento de Logística en Editorial IES Siglo 21.

COLEGIO  
UNIVERSITARIO



# ¿Cómo está organizado este texto?

Usted está en presencia de este texto que los autores proponen para la comprensión studio de la asignatura. Ha sido preparado y diseñado para facilitarle el acceso al conocimiento, a partir de una secuencia cuyo punto de partida es la práctica profesional cotidiana y no la teoría alejada de la realidad.

Está organizado de la siguiente manera:

- **Introducción.** Indica qué papel desempeña la asignatura dentro de la carrera y los conceptos básicos que usted conocerá.
- **Esquema.** Muestra los enlaces que unen los conceptos centrales de la asignatura entre sí.
- **Situación profesional.** Lo ubica frente a un problema de la práctica profesional cotidiana que puede ser resuelto, ya que existe al menos una solución para ello, a través de conocimientos específicos que en cada caso se aportan.
- **Herramientas.** Son los conocimientos necesarios para resolver la Situación profesional planteada.
- **Autoevaluación.** Para que usted compruebe si ha comprendido correctamente lo que se explicó en una herramienta, los autores proponen la resolución de actividades y le ofrecen las respuestas.
- **Ejercicio resuelto.** Bajo este título encontrará una manera de resolver los problemas de práctica profesional planteados, con la selección de las herramientas pertinentes.
- **Ejercicio por resolver.** Ahora le toca a usted. Es el momento de aplicar las herramientas a una Situación profesional nueva o similar a la ya expuesta. Todas las dudas que le aparezcan podrán ser planteadas a su docente.
- **Evaluación de paso.** Para que usted compruebe si ha comprendido correctamente lo que se explicó en las distintas herramientas que hasta el momento se han presentado, los autores proponen la resolución de actividades y le ofrecen las respuestas.
- **Bibliografía.** Se indican los textos, revistas y links de consulta a los que podrá recurrir para complementar o ampliar algunos temas.

# Introducción

Aunque no lo hayamos pensado, las redes han existido desde tiempos muy lejanos: algunos ejemplos son los caminos, el ferrocarril, las autopistas, el telégrafo, la red telefónica y actualmente, en la era de la información, las redes de computadoras.

A qué se debe la importancia de las redes? A que estas sirven para comunicarnos y la comunicación permite que mejoremos sustancialmente muchos aspectos de nuestra civilización.

Si el hombre no contara con la inteligencia necesaria para lograr la comunicación entre las personas, la raza humana no sería muy diferente del resto de las especies que habitan el planeta.

A nivel de organizaciones, ya sea comerciales o sin fines de lucro, la comunicación permite disponer de información actualizada, lo que aumenta la probabilidad de tomar decisiones correctas para alcanzar los objetivos y reducir la incertidumbre o la posibilidad de cometer un error.

La información es poder, y hoy más que nunca antes en la historia, la información es un elemento decisivo para el éxito o el fracaso de las organizaciones.

En la actualidad en todos los sectores de una organización están presentes las comunicaciones tanto de voz como de datos y multimedia a través de las redes de telecomunicaciones permitiendo obtener, procesar y presentar información a los distintos niveles de una empresa para tomar decisiones.

Aunque, hasta ahora, utilizamos cada servicio de comunicación con su red específica (la comunicación de voz con su red y la de datos por otra red) hoy en día, con la digitalización de todas las señales, las tecnologías de las redes y de las comunicaciones se encuentran en un crecimiento convergente sobre la base de utilizar un protocolo común: IP.

Entonces, es hora de que comencemos a pensar que es posible prestar cualquier tipo de servicio sobre la misma infraestructura de red, utilizando los usuarios terminales específicos para acceder a cada uno de ellos, o bien uno con capacidad multimedia.

De esta forma, veremos cómo la información viaja por las redes en forma digital y su tratamiento se puede realizar de la misma manera, con independencia de su origen, ya sea sonidos, texto, imágenes o videoconferencias.

Además, en las comunicaciones, los desarrollos alcanzados permiten utilizar la tecnologías 3,5G y 4G cada vez con menos costo (con la cual se pueden establecer vínculos a Internet aplicando nativamente el protocolo TCP/IP a velocidades de 100 Mbps y 1 Gbps) accediendo a un sinnúmero de servicios desde nuestro celular, que hasta hace muy poco tiempo eran "impensados".

También, la incorporación de otros conceptos como por ejemplo "Cloud Computing" nos obliga a pensar cada vez más en la capacidad de procesamiento que adquiere "la nube", y esto nos puede optimizar la forma de concebir las redes organizacionales.

En este TID se exponen los conceptos fundamentales para entender cómo son y cómo funcionan las distintas redes de datos que se emplean para la interconexión de computadoras y otros dispositivos, los servicios que se pueden utilizar a través de las redes y las técnicas que se utilizan para transmitir y acceder a la información, con un lenguaje ameno que no supone conocimientos previos de redes. El mismo fue especialmente escrito para ser utilizado como texto de estudio en la Asignatura Redes y Comunicación.

El diseño y elaboración ha sido implementado para que pueda adaptarse a cualquiera de las modalidades implementadas por el IES (*presencial, semipresencial y distancia*); pero, además, puede ser de utilidad para todo aquél que quiera introducirse en los conocimientos (a veces injustificadamente difíciles e incomprensibles) del

mundo de las redes y las comunicaciones.

La obra se estructura en once Situaciones profesionales que explican con claridad y detalle los conceptos que servirán de guía para la comprensión acabada del funcionamiento de los sistemas de comunicaciones actuales, concibiendo a este TID de gran utilidad como texto de estudio pero también de consulta para todos aquellos estudiantes, docentes, usuarios y profesionales que quieran abocarse al estudio de esta cada vez más importante materia y adquirir o reforzar conocimientos de aplicación práctica en todas las organizaciones actuales.

Diez de estas Situaciones profesionales nos llevarán a completar la idea del contenido y funcionamiento de los sistemas de comunicación, mientras que una de ella nos permitirá entender qué es la información; cómo podemos establecer una relación matemática con ella de manera de poder medirla y cuantificarla.

Se ha preguntado alguna vez, mientras navega por Internet, o cuando intercambia archivos o email, o cuando comparte recursos con sus amigos o compañeros: ¿Cómo es el mecanismo para que lo que yo poseo en mi computadora pase hacia la de mi compañero?, ¿Por qué, a veces, el intercambio se produce rápidamente y otras, tarda un tiempo más largo?, ¿Cómo es que puedo ver imágenes, videos, o también puedo hablar y dialogar ("chatear") con otras personas que están a miles de kilómetros, como si estuviéramos sentados a la misma mesa de café?, ¿Cómo es posible que distintas máquinas, con distintos sistemas operativos, intercambien información sin necesidad de adaptar las condiciones de diálogo?. Éstas y tantas otras se responden con: "Los sistemas de comunicación y las redes de información".

A veces, podemos sentir que es excesivamente complicado comprender el mundo de las telecomunicaciones y que sólo es materia para unos pocos especialistas que -por lo general- hablan en "otro idioma". No es para asustarse ni desanimarse, es natural que exista una "jerga" específica, con palabras que a veces no figuran en ningún diccionario, pero eso es normal en toda actividad humana, o ¿Acaso los médicos no tienen su propio idioma, o un plomero o un carpintero?.

Sin duda tendrá que vérselas con muchos términos y con una cantidad prácticamente ilimitada de siglas: FTP, UDP, HTTP, SNMP, PPP; TCP, IP, WWW, OSI, LAN, MAN, WAN, ATM, ISDN, MTU, NetID, HostID, LLC, MAC, RIP, OSPF, FDDI, IPX, SPX, ARP, RARP, RFC, IEEE, ACK... son sólo algunas. Con la cantidad tan grande de términos nuevos, es lógico que se sienta como que le están hablando en "otro idioma".

A todos quienes estamos en el tema nos resultó más o menos difícil acostumbrarnos a esto, pero en esta obra los explicaremos desde un lenguaje sencillo y verá cómo después de un tiempo en su uso, usted también se adaptará y utilizará esos términos nuevos.

Un consejo: no permita que el árbol le impida ver el bosque. Lo más importante (como siempre) son los conceptos; las siglas también son importantes, pero en un segundo término. Trate primero de entender los conceptos y a las siglas las aprenderá "casi sin querer" al releer y buscar sus referencias.

En realidad no hay ningún concepto inaccesible, críptico o profundamente difícil en esta materia, así que es muy probable que el mayor escollo sea superar cierta incomodidad en la lectura por la cantidad enorme de nuevos términos.

Los términos importantes, los conceptos principales y algunos enunciados significativos se encuentran resaltados en negrita, y también cuando la situación lo requiere, encontrará la respectiva ayuda que lo asistirá en la comprensión del texto.

Todas las situaciones profesionales incluyen preguntas y actividades sobre los conceptos más importantes y, por ello, recomendamos especialmente contestar esas preguntas y realizar las actividades propuestas, ya que le ayudaran a fijar los conocimientos y a poner de manifiesto todas las dudas que ciertamente le surgirán.

Espero, ciertamente, que el presente TID le ayude a prepararse para su actividad profesional y que a través de

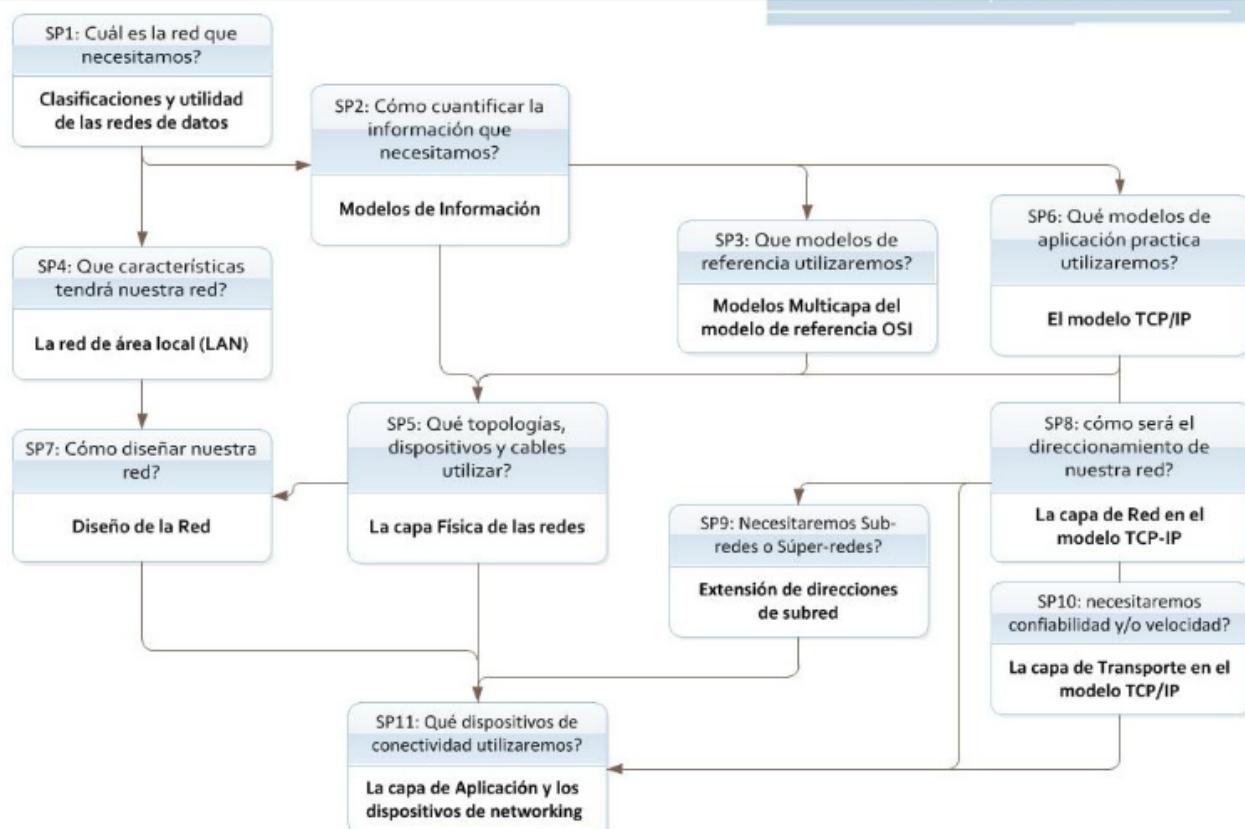
él encuentre las respuestas para comprender este maravilloso mundo de las redes.

*El autor*

# Esquema

## Esquema

Redes y Comunicación



# **Situación profesional 1: ¿Cuál es la red que necesitamos?**

## **Clasificaciones y utilidad de las redes de datos**

La empresa donde usted ha comenzado a trabajar como pasante, es una empresa que recién se inicia. Allí los empleados utilizan cada uno su computadora, cada uno en forma aislada.

Se prevé un crecimiento importante de la actividad de la empresa, incluso con apertura de varias sucursales.

Le solicitan a usted que analice la posibilidad de instalar una red que facilite el trabajo de la empresa.

Su primera pregunta, entonces es: ¿Necesitamos realmente una red? Si la respuesta es afirmativa, surgirá la segunda pregunta: ¿Cuál es la red que necesitamos?

A fin de poder contar con el conocimiento necesario para realizar una adecuada decisión, deberá tener en cuenta cuáles son los criterios de clasificación de las redes y cuál será la utilidad que le brinde cada una de ellas.

# SP1 / H1: Usos de las redes de datos

De acuerdo a lo planteado en esta situación profesional, para saber si necesitamos una red, comenzaremos analizando en nuestro entorno, algunos ejemplos de redes que conviven con nosotros. Desde tiempos muy lejanos el ser humano está inmerso en las redes. Ejemplos de ellas pueden ser los caminos, el ferrocarril, las autopistas, el telégrafo, el tendido telefónico y actualmente, en la era de las informaciones, las redes de computadoras, internet y últimamente hasta en las "redes sociales". El ser humano necesita estar comunicado, por eso, a través de la historia, ha buscado permanentemente el mejoramiento del intercambio de información utilizando las redes, hasta alcanzar lo que conocemos hoy por redes de computadoras, plataforma de innumerables aplicaciones empresariales y sociales.

Veamos algunos conceptos: al puesto de trabajo con una computadora que no forma parte de ninguna red lo llamamos *Stand Alone* (puesto aislado). En este entorno, una persona trabaja en su PC y tiene en su disco rígido tanto los programas que desea utilizar como los archivos sobre los que trabaja.

Sus capacidades de impresión y de escaneo, por ejemplo, estarán limitadas al hecho de poseer estos equipos conectados a su computadora o no.



"Entorno Stand Alone" | Elaboración DEPROE, IES siglo 21

Una de las ideas primigenias que impulsaron fuertemente la tecnología de redes está directamente vinculada a los costos: la idea es la de **compartir hardware**.

Por ejemplo el caso de las impresoras: si usted posee una, habrá notado que en general la mayor parte del tiempo la misma está sin uso (si quiere hacer la prueba, controle en un día cuánto tiempo está encendida su computadora y cuánto tiempo utiliza la impresora). Este hecho lleva a un análisis muy simple: supongamos una oficina en la cual trabajan 5 personas, seguramente cada una de ellas tendrá necesidad de imprimir los documentos que elabora; pero, ¿significa esto que cada una de ellas debe tener una impresora conectada a su computadora? ¿Será ésta una decisión rentable? Sabiendo que el tiempo de uso del dispositivo de impresión es en realidad una fracción del tiempo total que la persona trabaja, ¿no sería más racional, por ejemplo, proveer a

los 5 integrantes de la oficina de una sola impresora o quizá de dos, de tal forma que la pudieran compartir?

Es cierto que es posible dotar a la oficina de una impresora conectada a sólo una de las computadoras (en un entorno stand alone) y hacer que cada vez que uno de los integrantes necesitara imprimir, almacenara los archivos en un disquete y solicitara al "dueño" de la impresora que le hiciera las impresiones. Reconozcamos que esta situación es por lo menos incómoda.

Las redes brindan una solución a situaciones de este tipo; si las computadoras de la oficina estuvieran conectadas en red, entonces, cualquiera podría imprimir, dando la orden directamente desde su computadora.

Obviamente que la solución de proveer de unas cuantas impresoras a los integrantes de una oficina, será más económica que brindar una a cada integrante de la misma.

Observe que hemos utilizado un dibujo sin una forma determinada para representar a "la red" (parece algo así como una nube), con esto queremos significar que lo expresado es independiente de la topología de la misma y de su estructura de conexión (podrían ser distintos tipo de cables o enlaces infrarrojos, etc).

*Computadoras o Host, conectados en un entorno de red.*

*Los usuarios tienen la posibilidad de compartir los recursos.*

En este contexto, un host es, simplemente, una computadora conectada a la red.

Otros argumentos surgen con igual o mayor fuerza que el de los costos para apoyar la idea de interconectar las computadoras en redes: **compartir información** suele ser uno de ellos.

En los últimos tiempos, un paradigma redescubierto se ha instaurado con fuerza: **el trabajo en equipo**. Cada vez se impulsa con más fuerza dentro de las empresas y organizaciones de todo tipo la idea de que el trabajo en equipo potencia las habilidades y destrezas de los integrantes del mismo, de tal forma que es posible que un equipo obtenga mejores resultados que los que obtendrían los integrantes por separado. No es motivo de este libro analizar este punto de vista, pero sí lo es resaltar que la interconexión de un instrumento de trabajo, como es la computadora en un entorno de red, permite a los usuarios compartir información, por ejemplo compartiendo archivos, inclusive permitiendo que varias personas trabajen simultáneamente sobre el mismo documento. También permite que las personas intercambien mensajes, con los servicios de correo electrónico (e-mail), que establezcan citas para reunirse (scheduling) (programas que permiten generar una agenda en común entre todos los integrantes de una red, al poseer las agendas de cada integrante permite generar horarios para reuniones grupales fácilmente) sin que sea necesario establecer un contacto previo o personal.

Otro hecho que ha impulsado el establecimiento de redes es, sin duda, el advenimiento de **los sistemas de bases de datos**. Para formarse una idea, piense en un ejemplo muy sencillo: suponga simplemente que un importante cliente de una empresa cambia su número telefónico y piense los problemas que ese simple cambio podría traer a una empresa que no tenga un sistema centralizado de base de datos. El cliente cambió su número de teléfono y supongamos que llama a la empresa para avisar el cambio. Este dato es recibido por una telefonista del turno mañana que lo anota prolíjamente en un cuadernito, pero resulta ser que la gente del departamento contable necesita confirmar si dicho cliente recibió una factura... por supuesto que intentará comunicarse al antiguo número de teléfono. Por otro lado, el gerente de marketing está interesado en invitarlo a una presentación de un nuevo producto que harán próximamente, ¿a dónde llamará?: al número anterior y no podrán comunicarse.

Se podría pensar que la telefonista que recibió la información del cambio de número de teléfono debería haber avisado al resto de la empresa. ¿Se imagina el tiempo que perdería si debe avisar a todos y cada uno de los departamentos que ella crea que pueden necesitar esa información? Y esto, considerando que quien reciba la información dentro de cada departamento la distribuya correctamente entre todos los integrantes.

Pensemos en empresas que tienen sus negocios distribuidos en distintos lugares geográficos, ¿cuánto vale el hecho de que puedan compartir información?

Definiremos como **red**, básicamente a un **grupo de computadoras interconectadas entre si, que pueden compartir recursos de hardware e información**.

La interconexión entre ellas se puede realizar mediante cableado o en forma inalámbrica mediante ondas de radiofrecuencia.

El tipo de computadoras utilizadas en la red puede variar: por ejemplo actualmente todavía existen redes que utilizan grandes computadoras, mientras que otras utilizan las que conocemos normalmente en las oficinas de la empresa, comercio o incluso en nuestros hogares.

Nosotros centraremos el estudio a las redes que utilizan computadoras (cuyos sistemas operativos veremos más adelante en esta misma situación profesional) lo que ya de por si no es poca cosa, pero teniendo en cuenta que los conceptos son fácilmente trasladables a otro tipo de redes que actualmente están en muy importante crecimiento tales como son las redes de dispositivos móviles, ya que el hardware de estos cada vez se parece más al de las computadoras personales y los protocolos utilizados tienden a converger.

Entonces, las computadoras que integran una red comparten recursos de hardware e información con las demás, evitando de esta forma costos innecesarios en recursos de hardware que ya se disponen.

Una red permite compartir los siguientes **recursos**:

Recursos de *hardware*:

- Procesador y Memoria RAM (el ejecutar programas de otras computadoras).
- Unidades de almacenamiento (Discos duros, flexibles, ópticos y unidades de cinta).
- Dispositivos de impresión.
- Dispositivos de comunicación (Modem, Fax, Routers y actualmente también telefonía IP).

También se puede compartir la siguiente *información*:

- Carpetas (directorios)
- Archivos de textos, imágenes, sonido, video, etc. (Un usuario puede guardar sus archivos en otra computadora, hasta puede que ni siquiera cuente con disco propio). Acceso compartido a una agenda común (scheduling).
- Acceso a base de datos (a los cuales pueden acceder muchos usuarios al mismo tiempo).
- Ejecución de programas de aplicación en forma remota (incluyendo aquellos que toman el control de otra computadora manejando su mouse y el teclado).

Para finalizar, en una red también podemos intercambiar información mediante:

- Envío y recepción de mensajes de correo electrónico (e-mail)
- Establecimiento de conversaciones (chat)
- Implementar conferencias de voz entre varios usuarios al mismo tiempo
- Video conferencias

Vemos, entonces, que en la red se pueden prestar los siguientes **servicios**:



Interactiva "Servicios"

Servicio de acceso a carpetas y archivos: los usuarios de la red, mediante correspondientes permisos de acceso, podrán leer, escribir, modificar, copiar, borrar, crear, mover y ejecutar archivos en otra computadora de la red.

Servicio de acceso a bases de datos: los usuarios de la red, mediante los correspondientes permisos, podrán consultar o actualizar una base de datos en otra computadora de la red

Servicio de impresión: los usuarios de la red, también podrán mandar a imprimir sus archivos en una impresora que se encuentre compartida por otra computadora en la red o tambien en impresoras que se conectan a la red directamente.

Servicio de copias de respaldo: existen programas que automatizan la tarea de copiar los archivos que se consideren importantes. Estos archivos se pueden copiar en otra computadora de la red

Servicio de correo electrónico: los usuarios de la red, pueden enviar y recibir correos electrónico a otras computadoras, ya sea de la misma red empresarial o hacia y desde otras computadoras a kilómetros de distancia.

Servicio de chat: los ususarios de la red pueden enviar y recibir mensajes de texto y voz hacia otros ususarios en tiempo real, ya sea de la red empresarial u otras redes fuera de la organización

Servicio de video: los usuarios tambien tienen la posibilidad de utilizar microfono y camaras para una comunicación con otros ususarios de la red o redes fuera de la organización

Servicios de navegación: los usuarios pueden acceder, mediante un programa llamado "navegador" a sitios web, páginas web tanto de la empresa (intranet) como del exterior (internet)

Servicio de fax: los usuarios de la red pueden compartir el servicio enviar y recibir fax, mediante una computadora conectada a una linea telefónica

## Ventajas y desventajas del trabajo en red

Estamos en condiciones entonces, de analizar **que ventajas ofrece el trabajo en una red** (en un entorno de red), en comparación con el trabajo donde las computadores se encuentran trabajando individualmente (en un entorno stand alone).

Las más importantes son:

- Disminuye costos de hardware en general: al evitar tener que equipar todas las computadoras con todos los dispositivos complementarios, como por ejemplo impresoras, lectoras de CD, etc. Es posible que algunas computadoras críticas deban comprarse con mayores garantías de calidad lo que incrementará su costo, pero en general, la suma total de costos es menor.
- Favorece el intercambio de información: se mejora sustancialmente la velocidad y la seguridad evitando el intercambio de disquettes o pendrives que pueden deteriorarse o perderse.

- Facilita las copias de respaldo: mejora la velocidad y la seguridad al hacer copias de respaldo sobre medios de almacenamiento masivo evitándose tener copias fragmentadas.
- Favorece la mejor administración de espacios de almacenamiento: al utilizar la red, se administra mejor el espacio utilizando medios masivos de almacenamiento donde se puede concentrar la información y efectuar las copias de respaldo, evitando tener duplicaciones en cada uno de los usuarios que puedan generar inconsistencias (errores).
- Mejora las actualizaciones: se evitan las pérdidas de tiempo que significa tener que actualizar todos los sistemas en todas las computadoras. Teniendo los sistemas centralizados, en un solo momento determinado se actualizarán todos los sistemas.
- Facilita la intercomunicación: mediante programas de aplicación para redes (correo electrónico, chat, agendas compartidas, etc.) se evitan papeles que van y vienen, como así también el uso de disquettes o pendrives. También se puede realizar trabajo en grupo mediante herramientas que permiten que varias personas trabajen sobre el mismo texto, aunque se encuentren separados, pudiéndose visualizar los cambios efectuados por cualquiera de los usuarios (este TID fue escrito de esa manera).
- Favorece la seguridad: disminuye la posibilidad de cometer errores, accesos no permitidos y deterioro intencional de la información. Esto se logra mediante permisos a los usuarios para que accedan a los recursos de la red, cuestión que no se podría administrar en forma centralizada si no existiera una red.

¿Cuáles serían, entonces, las **desventajas del trabajo en red?**

Podríamos ver como desventajas las siguientes:

- El cambio de no tener red a tenerla, en una organización requiere una fuerte inversión de tiempo, dinero y capacitación.
- Para poner en marcha una red, se debe adquirir hardware y software de red y además hay que instalarlo y configurarlo.
- Algunos usuarios pueden, en el proceso de adaptación al cambio, oponer resistencia al cambio y perder temporalmente capacidad productiva.
- En algunos casos se requiere de forma permanente un administrador de la red.



¡Vamos a comprobar cuánto aprendiste!

**1. Indique la opción correcta**

Definimos como red, básicamente a un grupo de computadoras interconectadas entre sí, que pueden compartir recursos de hardware e información.

- Verdadero
- Falso

**2. Indique la opción correcta**

Computadoras conectadas en red NO pueden compartir el acceso a Bases de Datos.

- Verdadero
- Falso

**3. Indique la opción correcta**

Una de las ideas primigenias que impulsó la tecnología de redes estaba vinculada a costos, ¿A qué se hacía referencia en ese momento?

- Compartir hardware.
- Compartir software.
- Compartir conexión a internet.
- Compartir el trabajo.

**4. Indique la opción correcta**

Otros argumentos surgen con igual o mayor fuerza que el de los costos para apoyar la idea de interconectar las computadoras en redes, uno de ellos suele ser:

- Compartir hardware.
- Compartir información.
- Compartir impresoras.
- Compartir costos.

**5. Indique la opción correcta**

¿Cuáles de los siguientes son argumentos para la implementación de redes?

- Disminuir Costos.
- Compartir información.
- Trabajo en equipo.
- Todas las anteriores.

**6. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Recursos de Hardware  
Información  
Intercambio de información

Acceso a base de datos  
Dispositivos de Impresión  
Correo electrónico

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Definimos como red, básicamente a un grupo de computadoras interconectadas entre sí, que pueden compartir recursos de hardware e información.

- Verdadero
- Falso

## 2. Indique la opción correcta

Computadoras conectadas en red NO pueden compartir el acceso a Bases de Datos.

- Verdadero
- Falso

## 3. Indique la opción correcta

Una de las ideas primigenias que impulsó la tecnología de redes estaba vinculada a costos, ¿A qué se hacía referencia en ese momento?

- Compartir hardware.
- Compartir software.
- Compartir conexión a internet.
- Compartir el trabajo.

## 4. Indique la opción correcta

Otros argumentos surgen con igual o mayor fuerza que el de los costos para apoyar la idea de interconectar las computadoras en redes: uno de ellos suele ser:

- Compartir hardware.
- Compartir información.
- Compartir impresoras.
- Compartir costos.

## 5. Indique la opción correcta

¿Cuáles de los siguientes son argumentos para la implementación de redes?

- Disminuir Costos.
- Compartir información.
- Trabajo en equipo.
- Todas las anteriores.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Recursos de Hardware  
Información  
Intercambio de información

Dispositivos de Impresión  
Acceso a base de datos  
Correo electrónico

# SP1 / H2: La filosofía Cliente - Servidor y los sistemas operativos actuales

## La filosofía Cliente-Servidor

Las redes actuales funcionan bajo el concepto de Cliente-Servidor; en toda interacción en la red, una computadora actúa como cliente y otra como servidor.

Veamos de qué se trata.

Supongamos que está conectado en red y no posee una impresora conectada a su computadora, pero otra de las computadoras de la red sí posee una impresora. Si tiene permitido el acceso a la impresora, podrá utilizarla: en este caso estará solicitando un servicio, "el servicio de impresión", y la otra computadora se lo estará brindando. Como usted solicita algo, está jugando el rol de cliente. La otra computadora, la que le brinda el servicio estará jugando el rol de servidor, concretamente de servidor de impresión. La idea es muy sencilla: quien solicita un servicio es el cliente y quien lo brinda es el servidor.

En una red, habrá entonces computadoras que soliciten servicios, y computadoras que brinden servicios.

Si bien en algunos casos, algunas computadoras pueden jugar los dos roles, es altamente recomendable utilizar Sistemas Operativos que están configurados para alguno de ellos, pues estos sistemas operativos diseñados para optimizar sus recursos en la ejecución de alguno de estos roles.

## Sistemas Operativos actuales que permiten la comunicación en cada caso

**En una red de computadoras existen dos componentes básicos:**

**1. Cliente:** es una computadora que utiliza recursos (modem, impresora, unidades de disco, etc.) e información (carpetas, archivos, programas, etc.) de otras computadoras de la red.

Las computadoras que actúan como cliente, pueden utilizar sistemas operativos de uso corriente: Windows 8, Windows 7, Windows XP (Professional) o también sistemas operativos anteriores diseñados específicamente para ser clientes de un servidor, tales como por ejemplo Microsoft Windows 2000 (Professional) o Windows NT 4.0 (WorkStation).

**2. Servidor:** es una computadora que tiene como única función ofrecer recursos e información a las otras computadoras de la red. Por lo general se trata de una computadora con recursos mucho más potentes que las otras computadoras de su red.

Las computadoras que actúan como servidor, en general utilizan alguno de los siguientes Sistemas Operativos:

- Microsoft: Windows 2012 Server, Windows 2008 Server, Windows 2003 Server, Windows 2000 Server, Windows NT 4.0 Server
- Linux
- Novell: Novell Netware 5.0
- Unix

- Lantastic

Tanto los clientes como los servidores tienen la capacidad de procesar datos y almacenar información.

Los clientes pueden realizar sus tareas en forma independiente del servidor, o solicitarle a este servicio cuando lo necesiten.

Por lo general, es recomendable equipar los servidores con capacidades más grandes que las computadoras convencionales, como por ejemplo más cantidad de procesadores y más memoria RAM. También mayor capacidad de almacenamiento.

## Tipos de servidores

Podemos clasificar los servidores en tres tipos:

### 1. Servidor centralizado

Es aquel servidor que tiene que realizar todas las tareas, pues **es el único servidor de la red**. Este tipo de servidores es útil solo en pequeñas empresas, cuya red se limita a pocas computadoras que exigen poco al servidor. En estas redes el servidor suele actuar como servidor de usuarios, servidor de acceso a internet y alguna otra función como servidor de impresión y/o copias de respaldo.

### 2. Servidor Dedicado

Son aquellos que **se especializan en dar algún servicio específico** dentro de la red. Es decir actúan realizando una sola función. En estos recae sólo una parte del trabajo en toda la red.

Algunos ejemplos son:

**Servidor de usuarios:** es aquel que se encarga de administrar los permisos de los usuarios de la red, lo valida a su ingreso a la red, establece las políticas de acceso por grupos de usuarios y por usuarios individuales y controla el acceso que estos tienen a los diferentes recursos de la red.

**Servidor de archivos:** es aquel servidor que se encarga de atender los pedidos de los clientes en cuanto al acceso a los medios de almacenamiento masivo. Las operaciones con los archivos incluyen leer, escribir, copiar, modificar, crear, mover, ejecutar. Estas operaciones están íntimamente relacionadas con los permisos que posee cada usuario. Pueden establecerse cuotas de almacenamiento por usuario.

**Servidor de impresión:** administra las solicitudes de impresión de los usuarios. Para esto, almacena los archivos a imprimir en una cola de espera y les da las órdenes a la impresora para que los vaya imprimiendo según el orden solicitado.

**Servidor de comunicaciones:** (*gateway, proxy, etc.*) recibe los pedidos de transmisión de una red, por ejemplo para ser procesados en otra red, que puede ser otra red de la misma empresa o también internet. La función de estos servidores es officiar de traductores entre redes distintas.

**Servidor de back up de usuarios:** es un tipo especial de servidor que, producida una falla en otro servidor crítico como el servidor de usuarios, puede tomar el lugar de este automáticamente pues mantiene actualizada una copia de seguridad de los permisos de usuario.

**Servidor de back up de archivos:** es un tipo de servidor de archivos, pero que se utiliza para almacenar copias de respaldo de los archivos más importantes. Admite el almacenamiento de las copias de

seguridad según las políticas de seguridad establecidas y suele tener hardware especial para el almacenamiento duplicado y para efectuar copias de seguridad en medios seguros.

### 3. Servidor no dedicado

Son aquellos servidores que, además de **brindar servicios**, son también utilizados como clientes, es decir que **algún usuario también se siente frente a ellos a ejecutar otras tareas además de su tarea específica**.



¿Te animás a medir cuánto aprendiste?

**1. Indique la opción correcta**

En una red, las computadoras solo pueden desempeñar un solo rol, es decir ser Cliente o ser Servidor.

- Verdadero
- Falso

**2. Indique la opción correcta**

En una red, hay computadoras que solicitan servicios, y computadoras que brindan servicios.

- La que solicita servicios es llamada Servidor.
- La que solicita servicios es llamada Cliente.
- La que solicita servicios es llamada Cliente-Servidor.
- La que solicita servicios es llamada Host.

**3. Indique la opción correcta**

En una red de computadoras existe, como componentes básicos:

- El Cliente: es una computadora que brinda recursos a otras.
- El Cliente: es una computadora que brinda servicios a otras.
- El Cliente: es una computadora que utiliza recursos de otras.
- El Cliente: es una computadora actúa en forma independiente de las otras.

**4. Indique la opción correcta**

Otro componente básico es:

- Servidor: es una computadora que tiene como función ofrecer recursos a las otras computadoras de la red.
- Servidor: es una computadora que tiene como función utilizar recursos e información de las otras computadoras de la red.
- Servidor: es una computadora que tiene como función solicitar servicios a las otras computadoras de la red.
- Servidor: es una computadora que tiene como función actuar en forma independiente de las otras

computadoras de la red.

**5. Indique la opción correcta**

Los tipos de servidores son:

- Usuarios, Archivos, Impresión, Comunicaciones y de Back Up.
- Centralizado, Dedicado y No Dedicado.
- Windows, Linux y Novell.
- Del tipo Cliente-Servidor o Peer to Peer.

**6. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Sistema Operativo a utilizar como Servidor	Es el único servidor de la red
Servidor dedicado	Brinda algún servicio específico
Sistema Operativo a utilizar como Cliente	Windows 2008
Servidor centralizado	Windows 8

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

En una red, las computadoras solo pueden desempeñar un solo rol, es decir ser Cliente o ser Servidor.

Verdadero

Falso

## 2. Indique la opción correcta

En una red, hay computadoras que solicitan servicios, y computadoras que brindan servicios.

La que solicita servicios es llamada Servidor.

La que solicita servicios es llamada Cliente.

La que solicita servicios es llamada Cliente-Servidor.

La que solicita servicios es llamada Host.

## 3. Indique la opción correcta

En una red de computadoras existe, como componentes básicos:

El Cliente: es una computadora que brinda recursos a otras.

El Cliente: es una computadora que brinda servicios a otras.

El Cliente: es una computadora que utiliza recursos de otras.

El Cliente: es una computadora actúa en forma independiente de las otras.

## 4. Indique la opción correcta

Otro componente básico es:

Servidor: es una computadora que tiene como función ofrecer recursos a las otras computadoras de la red.

Servidor: es una computadora que tiene como función utilizar recursos e información de las otras computadoras de la red.

Servidor: es una computadora que tiene como función solicitar servicios a las otras computadoras de la red.

Servidor: es una computadora que tiene como función actuar en forma independiente de las otras computadoras de la red.

## 5. Indique la opción correcta

Los tipos de servidores son:

Usuarios, Archivos, Impresión, Comunicaciones y de Back Up.

Centralizado, Dedicado y No Dedicado.

Windows, Linux y Novell.

Del tipo Cliente-Servidor o Peer to Peer.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Sistema Operativo a utilizar  
como Servidor

Windows 2008

Servidor dedicado

Brinda algún servicio específico

Sistema Operativo a utilizar como Cliente

Windows 8

Servidor centralizado

Es el único servidor de la red

# SP1 / H3: Clasificaciones de redes de datos

## Tipos de redes. Clasificaciones

Se pueden establecer diversas clasificaciones para los tipos de redes. Por ejemplo, es posible clasificarlas:

- Segundo su tamaño y/o alcance (íntimamente relacionado con a quién pertenecen los recursos de interconexión)
- Segundo quién administra los recursos compartidos en la red.

### A. Clasificación según su tamaño y/o alcance

Una de las clasificaciones más utilizadas es la que se realiza *según el tamaño*. A veces puede resultar confuso distinguir una red de gran tamaño de una de pequeño tamaño, por lo que también se denomina esta clasificación *según el alcance*. Es de gran utilidad para ubicarse en qué contexto se establece una red.

Segundo su tamaño (extensión física) y/o alcance las redes pueden ser:

- **LAN (Local Area Network–Redes de Área Local).** Se denominan redes de Área Local a aquellas que se extienden en un espacio reducido, como puede ser un edificio o edificios contiguos. Habitualmente la organización que hace uso de la LAN es propietaria de todos los elementos de interconexión (como por ejemplo, los cables, las placas de red, etc.)
- **MAN (Metropolitan Area Network–Redes de Área Metropolitana).** Cuando las necesidades de interconexión se extienden más allá de los límites físicos de una estructura limitada, y hacen necesario interconectar usuarios ubicados, por ejemplo en distintos lugares de la una ciudad, se está en presencia de una MAN, o red de área metropolitana. En general, en estos casos, parte de los elementos de interconexión son alquilados o arrendados (por ejemplo, los cables que se "extienden" desde un edificio ubicado en el centro de la ciudad hasta otro ubicado en la periferia de la misma), a compañías que se encargan de brindar servicios de interconexión, como por ejemplo las compañías telefónicas. Por ejemplo, cuando contrata un servicio de acceso a Internet, Ud. se conecta vía telefónica con la red que posee el servidor de su proveedor, que generalmente está ubicada en su misma ciudad. En ese momento está formando una MAN con su proveedor de Internet (y con los demás usuarios de dicho proveedor). Observe que aunque es dueño de su módem, "alquila" la línea telefónica para conectarse con su proveedor de Internet a la compañía telefónica.
- **WAN (Wide Area Network- Redes de Área Ancha o Extensa).** Cuando los límites de la red exceden las distancias correspondientes a una ciudad, estamos hablando de una WAN. Por ejemplo, una empresa con sede en Buenos Aires, que posee una sede en Córdoba, utilizará una MAN para interconectar ambas sedes. De la misma forma que en las MAN, los dispositivos de interconexión entre ambas locaciones son habitualmente alquilados (por ejemplo, a las compañías telefónicas o a las que proveen servicios de conexión satelital). Observe que la cantidad de usuarios conectados a la red es independiente de su clasificación en LAN, MAN o WAN. Como podrá advertir, de estas definiciones, obtenemos algunas de las respuestas a la situación profesional planteada al comienzo. Al menos ahora podemos comprender que no es lo mismo la solución para la casa central o sucursales que para interconectar a ellas entre sí. Ya podemos decir, desde el punto de vista

geográfico, qué tipo de red necesitaremos en cada caso. Sin duda para la red de la casa central o sucursales, será una LAN, mientras que será necesaria una WAN para conectar las distintas LAN.

Estas tres anteriores son las más típicas, pero además existen otras que han surgido últimamente, a saber:

- **PAN** (*Personal Area Network - Red de Área Personal*). Aquellas que se extienden en el espacio donde se encuentran los dispositivos personales (teléfonos celulares, PDA (*Personal Digital Assistant*), dispositivos de audio, puntos de acceso a internet) (el medio de transmisión puede ser un cable pero suele habitualmente ser el Bluetooth)
- **WLAN** (*Wireless LAN - Red de Área Local Inalámbrica*). Son redes de área local, pero conectadas de forma inalámbrica. Son una alternativa muy utilizada a las redes de área local cableadas o como complemento de estas
- **VLAN** (*Virtual LAN- Red de Área Local Virtual*). Son redes que, aun teniendo diversa localización física dentro de una LAN, se comunican como si estuvieran dentro de una sola división lógica. Esto es posible dividiendo conmutadores en varios virtuales.
- **CAN** (*Campus Area Network - Red de Área Campus*) Aquellas que conectan redes de área local a través de un área geográfica limitada (campus universitario, base militar, hospital de varios edificios) mediante conexiones de alta velocidad pero con medios propios.

## B. Clasificación según quién administra los recursos compartidos de la red

Una de las clasificaciones más trascendentales es la que se realiza al determinar quién administra los recursos compartidos de la red. La gran importancia radica en las profundas consecuencias que esto tiene en el nivel de seguridad de la red.

En este caso suele utilizarse la siguiente clasificación:

1. Redes *peer to peer* (o redes entre pares).
2. Redes basadas en servidor.

### 1. Redes *peer to peer* (o redes entre pares)

Esta es una de las formas más sencillas de establecer una red LAN; en ella cada uno de los usuarios es administrador de los recursos que posee conectados a su propia computadora. En este tipo de redes no hay una jerarquía entre los distintos usuarios, sino que cada uno de ellos puede decidir qué recursos comparte con los demás usuarios de la red; en este sentido, se dice que todos los usuarios son pares.

Quizá el rasgo más distintivo es cualquiera de las computadoras conectadas puede jugar el rol tanto de cliente como de servidor: por ejemplo, la computadora que tiene conectada la impresora será el servidor de impresión para el resto de los usuarios, pero cuando este usuario desee acceder a los archivos guarda-dos en el disco rígido de otro, jugará el rol de cliente.

¿Quién administra los recursos en una red *peer to peer*? Los mismos usuarios.

En una red de este tipo, un usuario puede decidir compartir su impresora con los demás (o no), inclusive puede determinar qué carpetas o archivos puede compartir con el resto de los usuarios conectados a la red; si lo desea, puede compartir todo su disco rígido.

En algunos casos, el usuario que comparte sus recursos puede protegerlos con una contraseña, de tal forma que sólo los usuarios que la conozcan puedan acceder al recurso compartido.

Como puede imaginarse, siendo que cada uno de los usuarios es administrador de sus recursos, el nivel de seguridad en una red de este tipo es muy bajo.

Dado que cada usuario administra sus propios recursos, hay que tener en cuenta que alguien debe enseñarles cómo se hace. Si bien, en general es muy sencillo, muchas veces los usuarios menos experimentados en el uso de las computadoras presentan ciertos inconvenientes (lo cual significa asumir riesgos de seguridad).

Implementar redes *peer to peer* no insume grandes costos y, en general, suelen ser recomendadas para aquellos grupos de trabajo con una cantidad pequeña de usuarios (10 o 12), que se disponen en un ámbito físico limitado (esto no significa que no pueda implementar una red *peer to peer* con 30 o más usuarios, o que los mismos se encuentren ubicados en lugares distantes; sólo significa que no es recomendable, ya que probablemente las comunicaciones serán lentas). La verdad es que mejor que decir que son apropiadas para una cierta cantidad de usuarios, sería mejor decir que son apropiadas para redes con "bajo tráfico"; es decir que si va a implementar una red para 30 usuarios, la cual se usará solamente para que se establezca un servicio de mensajería que remitirá unos pocos emails por hora, entonces una red *peer to peer* será adecuada.

El bajo costo de este tipo de redes se debe fundamentalmente a que:

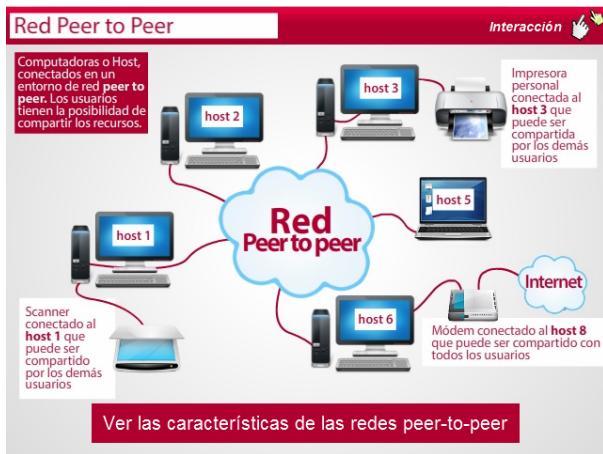
- *No es necesario disponer de una computadora "extra" que actúe de servidor.* Luego veremos las redes basadas en servidor, pero por ahora puede ir observando que el mejor funcionamiento de estas se obtiene cuando una computadora "no se usa" para las actividades cotidianas y se la designa como servidor; a este tipo de uso se lo denomina con servidor dedicado, en contraposición a la opción de servidor no dedicado.
- *El sistema operativo es económico.* Una red *peer to peer* puede instalarse simplemente con Windows 8, Windows 7, Windows XP o Windows 98, que son sistemas operativos populares y de bajo costo de Microsoft. Entre otras marcas, puede utilizarse Lantastic, que también es económico. Veremos luego que en las redes basadas en servidor es necesario adquirir un sistema operativo especial.
- *Las computadoras conectadas a la red *peer to peer* pueden ser las mismas que están siendo utilizadas en la actualidad sin grandes cambios.* Por ejemplo, si las computadoras que actualmente posee "corren" aceptablemente Windows XP, no necesita modificarlas para conectarlas en una red *peer to peer*, y "correrán" también, aceptablemente, en red. En este tipo de redes, cada computadora utiliza la mayor parte de sus recursos computacionales para el trabajo propio y dedica una fracción a la conexión grupal.

La siguiente figura muestra esquemáticamente lo que podría ser una red *peer to peer* típica. Observe que algunos *hosts*, poseen dispositivos externos conectados y otros, no. Si los usuarios poseedores de dichos dispositivos lo desean, pueden compartir dichos recursos con el resto de los usuarios de la red (o por quienes conozcan la password o contraseña). De esta forma, todos los usuarios conectados podrían imprimir en la impresora conectada al host 3, escanear fotografías en el scanner conectado al host 1 y navegar por Internet a través del módem conectado al host 6.

De la misma forma, los usuarios pueden compartir recursos "internos", como carpetas, archivos específicos o el disco rígido completo.

Además de compartir sus propios recursos, los usuarios pueden contar con un servicio de mensajería y enviarse e-mails, o utilizar un programa de scheduling para acordar la próxima reunión.

Resumiendo, las principales características de las redes *peer-to-peer* son:



Interactiva "Redes peer to peer (esquema y características)"

Elaboración DEPROE, IES siglo21

## 2. Redes basadas en Servidor

En las redes basadas en servidor cambia la filosofía con respecto a las redes peer to peer. En este caso, la prestación de servicios (de almacenamiento, de comunicaciones, de impresión, etc.) se centraliza en una o más computadoras denominadas servidores.

Los servidores son computadoras, habitualmente dotadas de importantes recursos de hardware que corren sistemas operativos especiales (denominados "de red" o "de servidor"); lo cual les permite administrar meticulosamente el uso de los recursos con que cuenta la red.

A diferencia de los que ocurre con las redes entre pares, las redes basadas en servidor suelen requerir la asistencia de un administrador de red que conozca con precisión el uso de los recursos de hardware y software con que cuenta la red.

Si la red deberá contar con numerosos usuarios, o si el tráfico será grande, deberá pensar seriamente en una red basada en servidor. No debe confundirse con la terminología:

Cuando se dice "red basada en servidor" no significa que deba haber un único servidor; según sean las necesidades de la empresa, podrá contar con un único servidor o con varios servidores. Cada uno de ellos brindará a los usuarios distintos servicios; y la red podrá contar con un servidor de almacenamiento (que provea de espacio en disco); un servidor de mails (que gestionará todas las comunicaciones de correo), un servidor de Internet (que brindará acceso a los usuarios a la mencionada interred); un servidor de impresión (que gestiona las requisitorias de impresión en impresoras de distintas características); etc.

La gestión de la seguridad se centraliza en el grupo de administradores de la red, pudiendo estos definir qué usuario accede a qué recursos. Es posible limitar el acceso de ciertos usuarios sólo a determinados archivos, o a determinados dispositivos.

En la actualidad, todos los sistemas operativos de red, permiten definir grupos de usuarios con accesos a recursos distintos, la definición puede llegar al nivel de usuario. En este sentido, los administradores definirán un nombre para cada usuario y definirán los grupos a los cuales se asignarán los usuarios; definiendo en el proceso los permisos con que contará cada uno de los grupos.

Los administradores de red pueden monitorear toda la actividad de los usuarios, es decir, pueden saber que

hace cada usuario y revisar cada uno de los mensajes que circulan en la red.

Como puede observar, en este caso a diferencia de las redes peer to peer, la seguridad no es administrada por los usuarios, sino por el grupo de administradores de la red, lo cual proporciona un nivel de seguridad más alto.

A diferencia de las redes peer to peer, donde el resguardo de los datos ante posibles pérdidas depende del criterio de cada usuario, las redes basadas en servidor suelen proveer de herramientas que permiten realizar la gestión de la red.

Por otro lado, los sistemas operativos de red suelen ser más "sólidos o estables", provocando menos fallos que los utilizados en redes peer to peer; en esencia, debe pensarse que los servidores de red son sistemas que pueden no apagarse nunca.

En cuanto a los requerimientos de hardware, existe una gran diferencia entre las máquinas clientes y las máquinas que actúan como servidores. En cuanto a los clientes, éstos pueden ser las mismas computadoras que en una red peer to peer, pero en cuanto a los servidores; éstos tienen requisitos que pueden llegar a ser bastante superiores: por ejemplo Microsoft recomienda en cuanto a los requisitos de memoria RAM para un servidor Windows Server 2008 un mínimo de 2 GB de memoria RAM.

Es habitual encontrar servidores de red que utilizan muchos microprocesadores en su *motherboard* y que cuentan con, por ejemplo con 16 GB de memoria RAM. Los recursos mencionados anteriormente dependen de la cantidad de usuarios y de tráfico.

En resumen, las principales características de las redes basadas en servidor son:

### **Características redes basadas en servidor**

**El nivel de seguridad es alto.**

**La cantidad de usuarios sólo se encuentra limitada por la capacidad del hardware.**

**Pueden tener uno o varios servidores**

**Si bien las computadoras que actúan como servidores pueden utilizarse también como estaciones de trabajo, no son recomendables ya que disminuye notablemente el rendimiento de la red.** Es decir, que debe disponerse de máquinas "extra" que actúen como servidores.

**El hardware de los servidores debe ser de buena calidad y sus requerimientos suelen ser costosos.** Pueden necesitar grandes cantidades de memoria RAM, grandes cantidades de espacio de almacenamiento en discos rígidos, e inclusive varios microprocesadores por cada servidor.

**Los servidores pueden ser equipos muy caros.**

**La organización debe contar con, por lo menos, un administrador de red.**

**Los sistemas operativos de red son más caros que los necesarios para una red peer to peer.**

**Los sistemas operativos de red deben ser "sólidos y estables", y junto con el hardware deben estar diseñados para no apagarse nunca.**

"Redes basadas en servidor" | Elaboración DEPROE, IES siglo21



¿Estás listo para un desafío?

**1. Indique la opción correcta**

La cantidad de usuarios conectados depende de la clasificación LAN, MAN o WAN:

- Verdadero
- Falso

**2. Indique la opción correcta**

Una red peer to peer tiene una única computadora que se comporta como servidor.

- Verdadero
- Falso

**3. Indique la opción correcta**

Una red basada en servidor, es una red que tiene un solo servidor que brinda todos los servicios:

- Verdadero
- Falso

**4. Indique la opción correcta**

Las redes según el tamaño se clasifican en:

- Peer to peer - Cliente-Servidor.
- LAN - MAN - WAN.
- Alámbricas e inalámbricas.
- Punto a punto - Broadcast.

**5. Indique la opción correcta**

Los enlaces en una WAN generalmente son:

- Propios.
- Arrendados.
- Contratos de terceros.
- (b) y (c) son correctas.

**6. Indique la opción correcta**

Una red para 16 usuarios que trabajan en oficinas contiguas, dentro del mismo edificio, ¿cómo se clasifica según su tamaño?

- Red LAN.
- Red MAN.
- Red WAN.
- Red PAN.

**7. Indique la opción correcta**

¿Cómo es el nivel de seguridad en una red basada en servidor?

- Bajo.
- Medio.
- Alto.
- No importa el nivel de seguridad.

**8. Indique la opción correcta**

¿De qué características deben ser los sistemas Operativos para una red basada en servidor?

- Bajo costo.
- Uso popular.
- Solidez y estabilidad.
- Alta compatibilidad con juegos.

**9. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Administración de redes  
igualitarias  
Administración de redes LAN  
Administración de redes WAN  
Administracion de redes  
basadas en Servidor

Habitualmente propiedad  
de terceros  
Medios propios  
Los propios usuarios  
El Administrador de la red

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

La cantidad de usuarios conectados depende de la clasificación LAN, MAN o WAN:

- Verdadero
- Falso

## 2. Indique la opción correcta

Una red peer to peer tiene una única computadora que se comporta como servidor.

- Verdadero
- Falso

## 3. Indique la opción correcta

Una red basada en servidor, es una red que tiene un solo servidor que brinda todos los servicios:

- Verdadero
- Falso

## 4. Indique la opción correcta

Las redes según el tamaño se clasifican en:

- Peer to peer - Cliente-Servidor.
- LAN - MAN - WAN.
- Alámbricas e inalámbricas.
- Punto a punto - Broadcast.

## 5. Indique la opción correcta

Los enlaces en una WAN generalmente son:

- Propios.
- Arrendados.
- Contratos de terceros.
- (b) y (c) son correctas.

## 6. Indique la opción correcta

Una red para 16 usuarios que trabajan en oficinas contiguas, dentro del mismo edificio, ¿cómo se clasifica según su tamaño?

- Red LAN.
- Red MAN.
- Red WAN.
- Red PAN.

## 7. Indique la opción correcta

¿Cómo es el nivel de seguridad en una red basada en servidor?

- Bajo.
- Medio.
- Alto.

- No importa el nivel de seguridad.

**8. Indique la opción correcta**

¿De qué características deben ser los sistemas Operativos para una red basada en servidor?

- Bajo costo.
- Uso popular.
- Solidez y estabilidad.
- Alta compatibilidad con juegos.

**9. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Administración de redes  
igualitarias  
Administración de redes LAN  
Administración de redes WAN  
Administracion de redes  
basadas en Servidor

Los propios usuarios  
Medios propios  
Habitualmente propiedad  
de terceros  
El Administrador de la red

# SP1 / Ejercicio resuelto

## Planteo del ejercicio

En la empresa donde usted ha comenzado a trabajar, los empleados utilizan cada uno su computadora, cada uno en forma aislada.

Previendo un crecimiento importante de la actividad de la empresa, le solicitan a usted que analice la posibilidad de instalar una red.

Tendrá poner en práctica los conocimientos adquiridos en la SP1 y diseñar una red para la empresa con 16 puestos de trabajo. La red deberá brindar servicios de impresión a todos los usuarios y compartir una conexión de acceso a Internet. Las computadoras, actualmente instaladas, tienen Windows 7, ejecutándose satisfactoriamente y todas tienen ya cargados en sus discos rígidos los programas que deberán usar los empleados.

Deberá:

- Definir (de acuerdo al tamaño) que tipo de red instalar
- Definir el tipo de red según quien administre los recursos compartidos

## Respuesta

La red que usted instale será una red LAN ya que todos se encuentran en un mismo entorno físico.

La red será del tipo Cliente-Servidor por cuanto la cantidad de usuarios es importante y hay expectativas de crecimiento posterior.

Se sugiere instalar por lo menos dos impresoras para brindar los servicios de impresión requeridos.

Dado que todas las computadoras actualmente poseen Windows 7, solo se requerirá instalar una computadora que actúe al menos como Servidor de Usuarios, se aconseja Windows 2012 Server.

## SP1 / Ejercicio por resolver

Siguiendo con el ejemplo anterior, la empresa decide ampliar su espacio de trabajo y alquila el piso de abajo, donde funcionará el Departamento de Marketing y Ventas y se atenderá a los clientes. Para ello se prevé incrementar la capacidad con 10 puestos de trabajo adicionales.

Determine las características que debería tener, ahora, la red.

# SP1 / Evaluación de paso



¡Vamos a comprobar cuánto aprendiste!

**1. Indique la opción correcta**

Definiremos como red a un grupo de computadoras interconectadas entre sí, que pueden compartir recursos de hardware e información.

- Verdadero
- Falso

**2. Indique la opción correcta**

En una pequeña red, de hasta una docena de usuarios, si tratamos de armarla fácil y rápidamente, es más conveniente usar el modelo "peer to peer".

- Verdadero
- Falso

**3. Indique la opción correcta**

Una red permite compartir los siguientes recursos de hardware:

- Ejecución de programas de aplicación en forma remota.
- Envío y recepción de mensajes de correo electrónico (e-mail).
- Unidades de almacenamiento (Discos duros, flexibles, ópticos y unidades de cinta).
- Video conferencias.

**4. Indique la opción correcta**

Una red permite compartir la siguiente información:

- Procesador y Memoria RAM.
- Carpetas (directorios).
- Dispositivos de impresión.
- Dispositivos de comunicación.

**5. Indique la opción correcta**

El servidor que se encarga de administrar los permisos de los usuarios de la red, validar sus ingresos, establecer políticas de acceso por grupos de usuarios y por usuarios individuales y controlar el acceso

que estos tienen a los diferentes recursos de la red se llama:

- Servidor de archivos.
- Servidor de impresión.
- Servidor de comunicaciones.
- Servidor de usuarios.

**6. Indique la opción correcta**

El servidor que se especializa en dar algún servicio específico dentro de la red se llama:

- Servidor centralizado.
- Servidor dedicado.
- Servidor no dedicado.
- Cliente - Servidor.

**7. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Sistema Operativo normal (que actúa como cliente)	Atiende un servicio específico
Servidor Centralizado	Windows 2012 Server
Sistema Operativo que actúa como Servidor	Windows 8
Servidor Dedicado	Único servidor de la red

**8. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Ventaja del trabajo en red	Servicios de impresión
Servicio básico ofrecido por una red	Cliente - Servidor
Desventaja de las redes	Instalación y Configuración
Tipo de red	Disminución de costos de hardware

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Definiremos como red a un grupo de computadoras interconectadas entre sí, que pueden compartir recursos de hardware e información.

- Verdadero
- Falso

## 2. Indique la opción correcta

En una pequeña red, de hasta una docena de usuarios, si tratamos de armarla fácil y rápidamente, es más conveniente usar el modelo "peer to peer".

- Verdadero
- Falso

## 3. Indique la opción correcta

Una red permite compartir los siguientes recursos de hardware:

- Ejecución de programas de aplicación en forma remota.
- Envío y recepción de mensajes de correo electrónico (e-mail).
- Unidades de almacenamiento (Discos duros, flexibles, ópticos y unidades de cinta).
- Video conferencias.

## 4. Indique la opción correcta

Una red permite compartir la siguiente información:

- Procesador y Memoria RAM.
- Carpetas (directorios).
- Dispositivos de impresión.
- Dispositivos de comunicación.

## 5. Indique la opción correcta

El servidor que se encarga de administrar los permisos de los usuarios de la red, validar sus ingresos, establecer políticas de acceso por grupos de usuarios y por usuarios individuales y controlar el acceso que estos tienen a los diferentes recursos de la red se llama:

- Servidor de archivos.
- Servidor de impresión.
- Servidor de comunicaciones.
- Servidor de usuarios.

## 6. Indique la opción correcta

El servidor que se especializa en dar algún servicio específico dentro de la red se llama:

- Servidor centralizado.
- Servidor dedicado.
- Servidor no dedicado.
- Cliente - Servidor.

## 7. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Sistema Operativo normal (que actúa como cliente)	Windows 8
Servidor Centralizado	Único servidor de la red
Sistema Operativo que actúa como Servidor	Windows 2012 Server
Servidor Dedicado	Atiende un servicio específico

#### 8. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Ventaja del trabajo en red	Disminución de costos de hardware
Servicio básico ofrecido por una red	Servicios de impresión
Desventaja de las redes	Instalación y Configuración
Tipo de red	Cliente - Servidor

# Situación profesional 2: ¿Cómo cuantificar la información que necesitamos?

## Modelos de Información

En la misma empresa citada en la anterior situación profesional están satisfechos con labor de conexión en red y, ahora, le plantean el siguiente desafío: Desean poder mostrarle a los clientes las imágenes de los edificios que la empresa construye. Esta información se encuentra en el piso de arriba, donde trabajan los arquitectos en el diseño de las mismas.

La gerencia, confiando en usted, le pide que analice si es posible transmitir en tiempo real las imágenes producidas con una calidad de 5 megapíxeles con una profundidad de 256 colores sobre la red por usted instalada.

# SP2 / H1: Concepto de símbolos, datos e información

## Teoría de la información

Frente al desafío que le han planteado, usted se pregunta: ¿estoy en condiciones de cuantificar los datos de la empresa y por consiguiente la información asociada a ellos?, ¿podré dar respuesta al comportamiento de todo el sistema, su capacidad de almacenamiento, las necesidades de los canales de comunicación, las velocidades de procesamiento, etc.?

Para contestar estas preguntas, vamos a recurrir a la Teoría de la Información, la cual está relacionada con las leyes matemáticas que rigen la transmisión, el almacenamiento y el procesamiento de información, lo que nos permitirá ocuparnos de la medición, de la representación y de la capacidad de los sistemas de información.

*Más concretamente, la teoría de la información se ocupa de la medición de la información y de la representación de la misma (como, por ejemplo, su codificación) y de la capacidad de los sistemas para transmitir, almacenar y procesar información.*

La codificación puede referirse tanto a la transformación de voz o imagen en señales eléctricas o electromagnéticas, como al cifrado de mensajes para asegurar su privacidad.

La teoría de la información fue desarrollada inicialmente, en 1948, por el ingeniero electrónico estadounidense Claude E. Shannon \* 1.1, en su artículo, *A Mathematical Theory of Communication* (Teoría Matemática de la Comunicación). La necesidad de una base teórica para la tecnología de la comunicación surgió del aumento de la complejidad y de la masificación de las vías de comunicación, tales como el teléfono, las redes de teletipo y los sistemas de comunicación por radio. La teoría de la información también abarca todas las restantes formas de transmisión y almacenamiento de información, incluyendo la televisión y los impulsos eléctricos que se transmiten en las computadoras y en la grabación óptica de datos e imágenes.

El término información se refiere a los mensajes transmitidos: voz o música transmitida por teléfono o radio, imágenes transmitidas por sistemas de televisión, información digital en sistemas y redes de computadoras, e incluso a los impulsos nerviosos en organismos vivientes. De forma más general, la teoría de la información ha sido aplicada en campos tan diversos como la cibernetica, la criptografía, la lingüística, la psicología y la estadística.

## Símbolos y datos

Denominamos **SÍMBOLO** a todo aquello que por convención nos remite a algo que no necesariamente necesita estar presente.

Este algo se encuentra en nuestro entendimiento a través del símbolo, de acuerdo con lo que el signo representa o significa.

De acuerdo con esto decimos que el símbolo nos trae a nuestra mente lo que está ausente.

Ese símbolo tiene sentido cuando lo interpretamos, cuando responde a lo que significa. O sea, cuando podemos establecer una relación entre el símbolo y lo que constituye su significado, de acuerdo con cierta convención.

No existe una relación intrínseca o natural entre el símbolo y su significado, entre el nombre y lo nombrado. La misma es arbitraria y convencional.

Así, cuando decimos "perro", no existe identidad o semejanza alguna entre el sonido de esa palabra y las características físicas de su significado.

El significado de un símbolo es establecido por el uso que le da la cultura que lo utiliza. Puede ocurrir que el mismo símbolo tenga distintos significados dentro de una misma cultura, dependiendo del contexto en que se inserta.

Por ejemplo, si a usted se le pregunta qué significa el gesto de levantar la mano abierta y moverla hacia un lado y otro, obviamente indicará que se trata de un saludo de despedida. Para nuestra cultura ese gesto es algo amable, que significa "adiós". Pero si hago lo mismo en Grecia, casi seguro que la voy a pasar mal, ya que ese gesto significa un insulto. Para los griegos tiene un significado totalmente distinto, aunque el gesto haya sido exactamente el mismo.

No solo son símbolos las letras y palabras, habladas o escritas. También lo son los gestos, los colores, el vestido, las costumbres, los sonidos no lingüísticos como el aplauso, etc.

Se dice que el hombre es un "animal simbólico" en el sentido de que no necesita considerar a entes y sucesos en sí mismos, sino que puede referirse mediante símbolos.

**Las propiedades o cualidades que determinan esos entes y sucesos, al ser representados simbólicamente constituyen lo que denominamos ATRIBUTOS** de los mismos. Pueden representarse en forma oral o escrita.

Así como la palabra "rayo" identifica ciertos sucesos, del mismo modo un nombre, un número de documento, es un atributo identificador de un ente o persona.

Si además indicamos su color de piel, ojos, cabello, su domicilio, fecha de nacimiento, etc., estamos agregando otros atributos que son descriptores, localizadores, relacionadores, etc.

Cuando especificamos cuantitativamente o cualitativamente un atributo, decimos que le asignamos un valor.

Ejemplo:

Identificadores	Descriptores	Localizadores	Relacionadores
Nombre	Color de ojos	Domicilio	Hijo de
Número de Documento	Color de cabello	Lugar de Nacimiento	Padre de
.	Estatura	Número de Teléfono	.
.	Edad	.	.
.	.	.	.

"Atributo. Asignación de un valor" | Elaboración DEPROE, IES siglo21

En general, los atributos son los "**DATOS**", que sirven de referencia con vistas a algún accionar concreto, presente o futuro.

O sea, el hombre opera con representaciones simbólicas que determinan hechos, entes, conceptos, órdenes, situaciones, etc, a partir de las cuales decide un curso de acción entre varios posibles.

Podemos decir entonces que **DATOS son representaciones simbólicas de propiedades o cualidades de entes y sucesos**, que pueden ser requeridos en un cierto momento como antecedentes, para decir la mejor manera de llevar a cabo una acción concreta.

**Los datos tienen la propiedad de que se pueden:**

- **Transmitir:** o sea llevarlos de un lugar a otro, o comunicárselos a alguien.

- **Almacenar:** para su posterior uso.
- **Transformar o procesar:** operando sobre ellos con ciertas reglas, para obtener nuevos datos.

## Información

Definimos como información a **todas aquellas representaciones simbólicas que por el significado que le asigna quien la reciba e interpreta, contribuyen a disminuir la incertidumbre de forma que pueda decidir un curso de acción entre varios posibles.**

De esta manera, se dispondrá en cada caso de un conjunto ordenado de datos relacionados, que permitirá tomar la decisión con el menor riesgo posible.

Pero no nos asustemos: la cosa no es difícil, siempre las definiciones, cuando son emitidas sin haber hecho una introducción previa, suelen ser complicadas de interpretar; por ello ahora vamos a trabajar sobre esta definición, y al final verá que no era para asustarse.

De acuerdo con la definición anterior, como se trata de representaciones simbólicas de acuerdo con ciertas acciones a realizar, puede ocurrir que aquello que es información para una persona no lo sea para otra.

Podemos suponer que ante un problema o situación por resolver, hemos elaborado o aprendido varias alternativas de acción, que responden a esquemas lógicos del tipo "sí"...(condición A)... entonces accionar A, "sí"...(condición B)... entonces accionar B,...

Cuando la información es suficiente como para tener la certeza de que se cumple una de las condiciones, decidimos realizar la acción correspondiente.

**La información no solo sirve para decidir cuál es el mejor accionar para lograr un objetivo. Tomada una decisión por un determinado curso de acción, para concretarlo se requiere saber qué acciones hacen falta realizar, y en qué secuencia.**

Se trata de información descriptiva, sin la cual no se puede efectuar la acción.

En el caso de las computadoras, la información descriptiva está involucrada en los programas, que indican la secuencia de operaciones a realizar para alcanzar el resultado deseado.

También existe la **información de control**, útil para verificar que un determinado accionar se ha efectuado correctamente. Así, una vez que hacemos una resta, podemos verificarla mediante una suma.

## Diferencias entre Datos e Información

De acuerdo con las definiciones dadas:

# Diferencias entre Datos e Información

## Datos

"Datos" son representaciones simbólicas de entes, hechos, atributos, etc,

## Información

"Información" alude a aquellos datos que por el significado que le atribuye quien necesita decidir una acción entre varias, permite tomar tal decisión con la menor incertidumbre posible.

"Diferencias entre Datos e Información" | Elaboración DEPROE, IES siglo21

Debemos distinguir entonces, entre una representación simbólica, y el significado que puede tener la misma para una persona, en función de una determinada acción que debe realizar.

Se dice que los símbolos portan información para quién pueda interpretarlos. Puede ocurrir que un mismo mensaje provea información distinta para dos o más decisiones diferentes de tomar. La diferencia así establecida entre datos e información, se manifiesta especialmente en el ámbito de la computación.

Una computadora recibe símbolos correspondientes a ciertos datos, opera con ellos y obtiene resultados que también son representaciones simbólicas, que en ningún momento tiene significado para la máquina. Sólo pueden tenerlo para el hombre, cuando los interpreta mediante su mente de manera que pueda tomar una decisión. Si bien muchas veces se confunden con un significado semejante las palabras "información" y "datos", diremos que: **toda información consta de datos, pero no todos los datos constituyen información.**

## Conceptos de Información

Si bien podríamos escoger una definición matemática precisa para el concepto de información, vamos a recurrir al sentido de la intuición para la definición de información.

Cuando escuchamos un boletín informativo, o cuando leemos el diario, es con el objeto de enterarnos de algo nuevo, algo que no estaba previsto, o por lo menos no estaba en nuestros planes.

Si consideramos un fenómeno cualquiera y si tal fenómeno es invariable, o sea totalmente determinado, no se puede aprender nada de él, no se puede decir nada nuevo, de manera que:

No hay información si no se trata de un elemento variable.

Con esto podemos definir a la información como:

*Sea un elemento variable, cuyos finitos cambios de estado sean impredecibles, se define como información, cuando es posible determinar el estado actual del fenómeno.*

Si bien esta definición suena un tanto académica, podemos resumir en que la información tiene que ver con los

"fenómenos variables" y con el "cambio impredecible".

De acuerdo con esto, podemos decir que las fuentes de información son:

- El cerebro del hombre, a través de las ideas.
- La modificación de los estados ambientales.
- Los censos poblacionales (número de habitantes de una población).
- Los medios que suplen las aptitudes mentales y nerviosas, como ser: radiotelefonía, TV, fotos, facsímil, etc.

Del concepto anterior de información, podemos deducir que cuanto más rápido sea el cambio impredecible, mayor es la cantidad de información. También surge de la definición que, al ser la información consecuencia de un fenómeno variable, puede de alguna manera ser representada y, lo más conveniente, es la representación numérica.

Cuando la información debe ser procesada o transmitida por medios electrónicos, las representaciones pueden ser otras, pero de todas maneras, siempre debe ser inteligible por el consumidor final.

## Información y certidumbre

Cuando definimos a la **información**, se explicó que ella **contribuye a disminuir la incertidumbre** que tenemos acerca de cuál es el mejor camino para resolver un problema. La incertidumbre se refiere a lo desconocido, a aquello que no se sabe si sucederá y a lo que es inesperado, imprevisible.

La información permite tener certeza de la existencia u ocurrencia de algún suceso o aspecto de la realidad, a la vez que disminuye el grado de incertidumbre que se tenía para tomar una decisión.

Es de hacer notar que, si una información se repite, no disminuye la incertidumbre que queda luego de haberla obtenido por primera vez. Lo esperado, aquello conocido de antemano, no representa información, ya que la probabilidad de ocurrencia es del 100%. Por ejemplo, la estimación que después del día viene la noche, no constituye información, ya que la probabilidad de que esto ocurra es del ciento por ciento, por cuanto no existe otra posibilidad.

Si por otra parte, si nos informamos que aconteció un evento significativo, del cual, por su baja probabilidad de ocurrencia, estábamos bastante seguros de que no iba a suceder, tendrá para nosotros un gran valor informativo en relación con esa decisión.

Por ejemplo, si alguien quiere hacer una inversión, sin duda va a comprar acciones de una empresa muy solvente, pero si a último momento escucha que se descubrió un fraude en relación con esa empresa, casi seguramente no tomará la determinación que tenía decidida con anterioridad.

Esta persona había hecho acopio de información sobre la mencionada empresa y por ello tenía decidido comprar esas acciones; pero bastó que llegue una noticia, que de acuerdo con los antecedentes era poco probable, para que la decisión cambiara radicalmente. Ahora la decisión obviamente no es la misma; esto nos lleva a poder determinar que ese hecho de baja probabilidad de ocurrencia nos ha provisto de mucha información, ya que nos ha hecho tomar otra decisión. No olvidar que la información nos sirve para disminuir la incertidumbre y así poder tomar decisiones.

Podemos afirmar, entonces, que **a menor probabilidad o certeza de ocurrencia, mayor será su significado informativo; y a mayor probabilidad o certeza de ocurrencia, menor será dicho significado**. O sea que hemos encontrado una relación entre Información y Probabilidad, lo cual es muy importante, ya que si se puede medir la Probabilidad, también lo podremos hacer con la Información.

La importancia de este concepto radica en que si podemos medir algo, lo podemos cuantificar; de esta forma

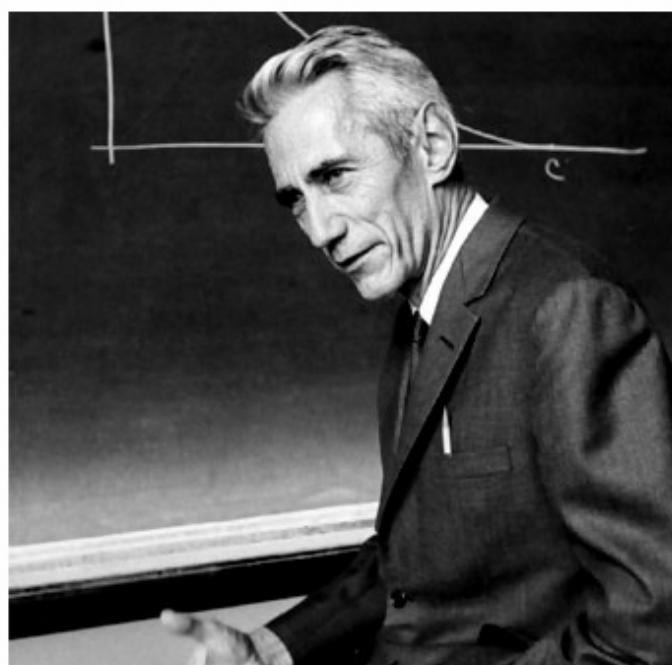
podemos saber qué recursos debemos contar para poder administrar esa Información.

### 1.1 : Claude E. Shannon

## Claude Shannon

(Claude Elwood Shannon; Gaylord, 1916 - Medford, 2001) Ingeniero estadounidense, padre de la moderna teoría de la información, una formulación matemática que analiza las unidades de información (bits) y su pérdida en los procesos de transmisión. Claude Shannon se graduó en ingeniería por la Universidad de Michigan en 1936 y, cuatro años más tarde, obtuvo un doctorado de matemáticas en el Massachusetts Institute of Technology.

Durante su estancia en dicha institución empezó a trabajar sobre el problema de la eficacia de los diferentes métodos existentes de transmisión de la información, tanto mediante el flujo a través de hilos o cables como el aéreo, por medio de corrientes eléctricas fluctuantes o bien moduladas por la radiación electromagnética. Shannon orientó sus esfuerzos hacia la comprensión fundamental del problema y en 1948 desarrolló un método para expresar la información de forma cuantitativa.



Claude Shannon





¿Te animás a medir cuánto aprendiste?

**1. Indique la opción correcta**

La teoría de la información se ocupa de la medición de la información y de la capacidad de los sistemas de transmisión:

- Verdadero
- Falso

**2. Indique la opción correcta**

La información ayuda a aumentar la incertidumbre.

- Verdadero
- Falso

**3. Indique la opción correcta**

¿A qué denominamos atributo?

- A la información.
- A la cantidad de información.
- A las propiedades de la información.
- Son propiedades o cualidades de los símbolos.

**4. Indique la opción correcta**

¿A qué denominamos símbolo?

- A los datos presentados.
- A todo aquello que por convención nos remite a algo que no necesariamente necesita estar presente.
- A la información procesada.
- A los datos y a la información.

**5. Indique la opción correcta**

¿A qué llamamos dato?

- A la información.

- A los símbolos.
- A los atributos de los entes.
- A la cantidad de información

**6. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Información	Aquello que nos remite a algo no necesariamente presente
Símbolo	Representación simbólica de entes y sucesos
Dato	Propiedad o cualidad de los entes al ser representados simbólicamente
Atributo	Representación simbólica que disminuye la incertidumbre

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

La teoría de la información se ocupa de la medición de la información y de la capacidad de los sistemas de transmisión:

- Verdadero
- Falso

## 2. Indique la opción correcta

La información ayuda a aumentar la incertidumbre.

- Verdadero
- Falso

## 3. Indique la opción correcta

¿A qué denominamos atributo?

- A la información.
- A la cantidad de información.
- A las propiedades de la información.
- Son propiedades o cualidades de los símbolos.

## 4. Indique la opción correcta

¿A qué denominamos símbolo?

- A los datos presentados.
- A todo aquello que por convención nos remite a algo que no necesariamente necesita estar presente.
- A la información procesada.
- A los datos y a la información.

## 5. Indique la opción correcta

¿A qué llamamos dato?

- A la información.
- A los símbolos.
- A los atributos de los entes.
- A la cantidad de información

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Información

Representación simbólica que disminuye la incertidumbre

Símbolo

Aquello que nos remite a algo no necesariamente presente

Dato

Representación simbólica de entes y sucesos

Atributo

Propiedad o calidad de los entes al ser representados simbólicamente



# SP2 / H2: Cantidad de información

## Medida de la Información

Un concepto fundamental en la teoría de la información es que la cantidad de información contenida en un mensaje es un valor matemático bien definido y medible. El término cantidad no se refiere a la cuantía de datos, sino a la probabilidad de que un mensaje, dentro de un conjunto de mensajes posibles, sea recibido.

Si examinamos con detalle el contenido de información de un mensaje, podemos ahorrar esfuerzo en su transmisión desde un punto a otro, o bien podemos reducir la capacidad de almacenamiento para guardarlo, o bien reducir los tiempos de procesamiento.

Por ejemplo, supongamos que entre varios amigos ponemos una empresa que transmite telegramas de felicitación entre varias localidades, ante acontecimientos determinados, como por ejemplo nacimientos, cumpleaños, casamientos, etc.

Nuestra empresa deberá contar en cada localidad con una oficina y equipamiento de comunicaciones. Supongamos que ese equipamiento es una computadora en donde escribimos el texto del mensaje y los nombres y domicilios de destinatario y remitente, y que luego lo transmitimos hacia el destino indicado.

Si Juan le quiere enviar un mensaje de "feliz cumpleaños" a su amigo Pedro, debemos escribir el nombre de Pedro (destinatario), el mensaje (feliz cumpleaños) y Juan (el remitente). Si Alejandra quiere hacer lo mismo con su amiga Virginia, debemos hacer lo mismo.

Pero después de haber montado esta empresa, nos damos cuenta de que gastamos mucho en comunicaciones; debemos hacer algo para disminuir ese gasto. Entonces, a alguien se le ocurre que podríamos establecer un código que nos permitiría reducir el texto a unos pocos caracteres. Por ejemplo, podríamos establecer lo siguiente:

Texto del mensaje	Código
Feliz Cumpleaños	1
Saludos por nacimiento de hijos	2
Felicitaciones por casamiento	3
Felicitaciones por materias aprobadas	4
Etc. Etc.	.

"Códigos para textos de mensajes" | Elaboración DEPROE, IES siglo21

Ahora, el mensaje será Pedro (destinatario), el código 1 (el mensaje) y Juan (el remitente), con lo cual hemos reducido de 16 caracteres (el espacio entre Feliz y cumpleaños también se cuenta) a uno solo.

De aquí podemos deducir que si bien el texto se ha reducido no ha ocurrido lo mismo con la información, ya que el mensaje sigue manteniendo el mismo contenido a pesar de haberlo reducido a un solo carácter.

Esta conclusión es muy interesante, ya que podemos deducir que la cantidad de información no depende del tamaño del mensaje (tamaño del texto en nuestro ejemplo). El operador simplemente indicará el destino, el remitente y un número o código que identifique el texto estandarizado típico.

De aquí también podemos sacar tres conclusiones extras, que son el concepto de protocolo, el de sincronización y el de estandarización.

The slide has a red header bar with the text "Conclusiones extras". Below it are three numbered boxes:

- 1 codificación**  
El primero nos indica que para poder establecer la codificación acordada, previamente hubo que ponerse de acuerdo; si no no hubiera sido posible interpretar el texto.
- 2 sincronización**  
El segundo, o sea el de sincronización, nos indica que ambos corresponsales deben funcionar coordinadamente en cuanto al tiempo, porque si no el mensaje puede llegar fuera de tiempo y no tendría el mismo efecto.
- 3 estandarización**  
El segundo, o sea el de sincronización, nos indica que ambos corresponsales deben funcionar coordinadamente en cuanto al tiempo, porque si no el mensaje puede llegar fuera de tiempo y no tendría el mismo efecto.

Interactiva "Conclusiones extras"

El primero nos indica que para poder establecer la codificación acordada, previamente hubo que ponerse de acuerdo; si no no hubiera sido posible interpretar el texto.

El segundo, o sea el de sincronización, nos indica que ambos corresponsales deben funcionar coordinadamente en cuanto al tiempo, porque si no el mensaje puede llegar fuera de tiempo y no tendría el mismo efecto.

Y el tercero, o sea el de estandarización, se refiere al establecimiento de las convenciones regulares, de modo que todos puedan interpretar los símbolos de la misma manera. Se refiere a las reglas del juego.

Elaboración DEPROE, IES siglo21

En un sentido intuitivo podemos ver que algunos mensajes largos no contienen gran información. El concepto de contenido de información en un mensaje particular debemos formalizarlo, para luego encontrar que cuando menor es la información en un mensaje, más rápido podemos transmitirlo.

El concepto de información está ligado al de predictibilidad. Cuanto más probable es un mensaje, menor es la información transmitida. Por ejemplo, si en el lugar donde trabajo, cobramos el sueldo el último día hábil del mes, avisarle a un compañero de esa novedad, no le transmitirá gran información, ya que la probabilidad de que ello ocurra es del ciento por ciento. Pero si le decimos que va a cobrar un premio extra determinado, la cosa es distinta, ya que la probabilidad de que ello ocurra es mucho menor que en el caso anterior.

Por lo tanto, podemos decir que la medida de la información está relacionada con la incertidumbre. Hay que destacar que la cantidad de información depende más de la incertidumbre del mensaje que del contenido del mismo.

La medida de la información es una indicación de la libertad de elección que puede tener la fuente en seleccionar el mensaje. Si la fuente puede emitir libremente un mensaje, el receptor tiene alta incertidumbre respecto del mensaje que será seleccionado. Pero si no hay selección, no hay incertidumbre, por lo tanto no hay información. Es evidente entonces, que la medida de la información comprende probabilidades. Los mensajes de alta probabilidad indican poca incertidumbre, llevando por consiguiente poca información y viceversa.

## Cantidad de Información

En 1946, Claude Shannon desarrolló su "Teoría Matemática de las Comunicaciones", en donde se planteó el objetivo de hacer lo más eficiente posible la transmisión de información, lo que implica la transmisión de

mensajes lo más rápida posible y con la mínima cantidad de errores.

Hay un límite en la tasa de información que puede ser transmitida por un sistema. Este límite es la capacidad, la cual viene determinada por las limitaciones físicas fundamentales en la transmisión de información. Lo primero que Shannon se planteó fue que dado un conjunto de posibles mensajes que una fuente puede transmitir.

¿Cómo pueden ser representados estos mensajes de la mejor manera posible para llevar la información sobre un sistema con sus limitaciones inherentes?

Para tratar este problema, es necesario concentrarse en la "información", más que en las señales eléctricas de comunicación y, por esta razón, el trabajo de Shannon fue rebautizado como "Teoría de la Información".

Dado que la información no es material ni tangible, se requiere para transmitirla que sea señalizada o codificada en alguna forma que pueda llegar al receptor en forma adecuada.

En lo que se refiere a la cantidad de información, el valor más alto se le asigna al mensaje que menos probabilidades tiene de ser recibido. Si se sabe con certeza que un mensaje va a ser recibido, su cantidad de información es 0.

Para relacionar la cantidad de información ( $I$ ) con la probabilidad, Shannon presentó la siguiente fórmula:

The image shows an interactive formula for Shannon's formula. At the top, it says 'Formula de Shannon' and 'Interacción'. Below that, a box contains the text: 'log<sub>2</sub> es el logaritmo de 1/P en base 2[NJC1] 2 [NJC1]: 2 log<sub>2</sub> de un número dado 'X' es el exponente 'Y' al que tiene que ser elevado el número '2' para obtener dicho número 'X'. Por ejemplo, log<sub>2</sub> de 8 = 3, porque 2<sup>3</sup> = 8.' In the center, the formula  $I = \log_2 1/P$  is displayed. A pink box at the bottom right says 'P es la probabilidad del mensaje que se transmite'.

Interactiva "Fórmula de Shannon"

$$I = \log_2 (1/P)$$

Donde  $P$  es la probabilidad del mensaje que se transmite y  $\log 2$  es el logaritmo de  $1/P$  en base 2[NJC1].

2 [NJC1]:

$2 \log_2$  de un número dado 'X' es el exponente 'Y' al que tiene que ser elevado el número '2' para obtener dicho número 'X'. Por ejemplo,  $\log_2$  de base 2 de 8 = 3, porque  $2$  elevado a la 3 = 8.

Elaboración DEPROE, IES siglo21

La cantidad de información de un mensaje puede ser entendida como el número de símbolos posibles que representan el mensaje. El 0 y el 1 son los dígitos del **sistema binario [NJC2]** \* 2.1, y la elección entre estos dos símbolos corresponde a la llamada unidad de información binaria o bit.

Si se lanza una moneda tres veces seguidas, los ocho resultados (o mensajes) igualmente probables pueden ser representados como:

Lanzamiento	Representación
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

"Lanzamiento-representación en binario" | Elaboración DEPROE, IES siglo21

La probabilidad de cada mensaje es de un octavo.

## Componentes de un sistema de comunicación

Antes de entrar a la explicación de la expresión de Shannon para la Cantidad de Información, vamos a ver en qué se basó para la determinación de su Teoría; para ello vamos a analizar en qué consiste un Sistema de Comunicación.

El tipo de sistema de comunicación más estudiado consta de varios componentes. El primero es una fuente de información (por ejemplo, una persona hablando) que produce un mensaje o información que será transmitida. El segundo es un transmisor (como, por ejemplo, un teléfono y un amplificador, o un micrófono y un transmisor de radio) que convierte el mensaje en señales electrónicas o electromagnéticas.

Estas señales son transmitidas a través de un canal o medio, que es el tercer componente, como puede ser un cable o la atmósfera. Este canal es especialmente susceptible a interferencias procedentes de otras fuentes, que distorsionan y degradan la señal. (Algunos ejemplos de interferencias, conocidas como ruido, incluyen la estática en la recepción de radios y teléfonos, y la nieve en la recepción de imágenes televisivas). El cuarto componente es el receptor, como por ejemplo el de radio, que transforma de nuevo la señal recibida en el mensaje original. El último componente es el destinatario, como por ejemplo una persona escuchando el mensaje.

Dos de las principales preocupaciones en la teoría de la información son la reducción de errores por interferencias en los sistemas de comunicación, y el uso más eficiente de la capacidad total del canal.

Hay que recordar que Shannon desarrolló su teoría de acuerdo con el esquema descripto y que se muestra en la siguiente figura:



"Esquema de Shannon" | Elaboración DEPROE, IES siglo21

Si bien esta teoría fue desarrollada sobre la base de los problemas de los circuitos y redes telefónicas, no obstante, como veremos, puede extenderse a cualquiera de los otros conceptos explicados.

La teoría de la información trata con tres conceptos básicos:

- La medida de la información.
- La capacidad de un canal o sistema de transmisión para transferir información, la cual podemos generalizar como la capacidad de un sistema para administrar la información.
- La codificación como un medio de utilizar los sistemas a máxima capacidad.

Estos conceptos pueden ser enlazados por el teorema fundamental de la teoría de la información que dice:

*"Dada una fuente de información y un canal de comunicación, existe una técnica de codificación tal, que la información puede ser transmitida sobre el canal con una tasa menor que la capacidad del canal y con una frecuencia de errores arbitrariamente pequeña a pesar de la presencia de ruido".*

Lo sorprendente de esto es la posibilidad de transmisión casi libre de errores sobre un medio ruidoso, logrado por medio de la codificación. En esencia, la codificación es usada para adaptar la fuente al canal, para máxima transferencia de información.

Como consecuencia de todo lo anterior nos planteamos las siguientes preguntas:

- ¿Cómo se mide la información?
- ¿A qué nos referimos cuando decimos cantidad de información?
- ¿Cómo se mide la capacidad de un sistema o canal?
- ¿Cuáles son las características de eficiencia de un proceso de codificación?
- ¿Cómo se pueden minimizar los efectos indeseables de factores exógenos?

Como decíamos anteriormente, por su intangibilidad, la información debe ser representada de alguna manera. Así, cuando una persona habla, las vibraciones de sus cuerdas vocales actúan sobre las moléculas del aire formando un sistema de ondas (similar al que se produce cuando se arroja una piedra en un estanque de agua calma), propagando de esta manera el sonido, hasta que actúen sobre un oído receptor al mismo ritmo que fue emitido.

De la misma forma, a través de las ondas electromagnéticas, al variar sus propiedades eléctricas, se pueden enviar mensajes a través de medios físicos como alambres conductores, cables de fibra óptica, o el aire. La señal que viaja por estos medios es portadora de mensajes con datos hacia el receptor.

Con estos ejemplos, se pretende introducir en las ideas básicas de la "Teoría de la Información" y verificar la diferencia entre los conceptos de "información" y "cantidad de información".

Vamos a ver cómo influye la incertidumbre en la toma de decisiones en la medida que se recibe información.

Para ello vamos a suponer que tenemos un sistema compuesto por un emisor, con una pila eléctrica que puede

ser aplicada en el extremo de dos cables. En el otro extremo, tenemos un receptor que puede medir la tensión eléctrica, verificando si está colocada o no la pila. A fin de que ambos extremos funcionen sincrónicamente, se tiene un reloj que sirve para tomar los tiempos en que deberá realizarse la medición.

De esta manera, hemos implementado un sistema binario de transmisión de mensajes. Así, si hemos acordado que cuando se mide una tensión eléctrica equivale a un "1" y cuando nos encontramos con ausencia de tensión eléctrica, tenemos un "0", podemos transmitir mensajes codificados de esta manera.

A fin de simplificar, vamos a suponer que tenemos que transmitir ocho letras (de la A hasta la H). Por tratarse de un sistema binario, se necesitan 3 elementos binarios para codificar las ocho letras. Esto viene del hecho de que al ser binario, o sea cada elemento puede variar en dos estados posibles (0 y 1), con una sola variable se pueden codificar dos estados, con dos variables se pueden codificar cuatro estados, con tres variables se pueden codificar ocho estados y así sucesivamente. Generalizando, con "n" variables se pueden codificar " $2^n$ " estados.

Para ello, vamos a codificar las ocho letras como sigue:

Letra	Código Binario
A	000
B	001
C	010
D	011
E	100
F	101
G	110
H	111

"Letra-código binario" | Elaboración DEPROE, IES siglo21

Para enviar una letra deberá enviarse tres variables binarias, así, por ejemplo, si se quiere emitir la letra "A", deberá transmitirse el código "000", si se quiere enviar la "B", se hará a través del código "001", y así sucesivamente hasta la "H" que corresponde al código "111".

Si además, convenimos que se comenzará la transmisión desde el dígito más significativo (el de más a la izquierda), el receptor, a medida que van llegando, irá disminuyendo la incertidumbre por cuanto aumenta la probabilidad de arriba de una determinada letra.

Para ello veamos el siguiente ejemplo:

Antes de comenzar la transmisión, el receptor tiene una incertidumbre total de cual será el mensaje a recibir. Como la fuente tiene "8" elementos (letras A a la H) y como todas tienen la misma probabilidad de emitirse (sistema equiprobable), la incertidumbre tiene una probabilidad de:

$$p = 1/8 = 0,125 = 12,5\%$$

Supongamos, que la primera medición indica ausencia de tensión eléctrica, o sea que ha llegado un "0". Ahora sabemos que la letra A estará entre las cuatro primeras, ya que ellas son las que comienzan con "0".

A = 000

B = 001

C = 010

D = 011

Ahora la probabilidad de que llegue una letra determinada es de:

$$p = 1/4 = 0,25 = 25\%$$

Si en el segundo período medimos y nos encontramos que existe una tensión eléctrica, estaremos ante la presencia de un "1", con lo cual se reduce la incertidumbre por cuanto sólo hay dos posibilidades:

C = 010

D = 011

La probabilidad aumenta a:

$$p = 1/2 = 0,5 = 50\%$$

Al recibir el tercer símbolo, se alcanza la certidumbre total, ya que si suponemos que después de la tercera medición vemos que existe ausencia de tensión eléctrica, o sea llegó otro "0", estaremos ante la única alternativa posible:

C = 010

En este caso la probabilidad será:

$$p = 1/1 = 1 = 100\%$$

Como podemos apreciar, en el ejemplo anterior, la llegada de un símbolo duplica la probabilidad, disminuyendo en la misma proporción la incertidumbre de la llegada de un símbolo.

En otras palabras, podemos decir que la incertidumbre era:

- Antes de comenzar a transmitir era = 1 = 100%.
- Despues de la llegada del primer símbolo (0) = 0,75 = 75%.
- Despues de la llegada del segundo símbolo (1) = 0,5 = 50%.
- Despues de la llegada del tercer símbolo (0) = 0 = 0%.

O sea, con cada llegada de símbolo la incertidumbre se reduce, hasta llegar a la incertidumbre nula, cuando la probabilidad es del 100%.

Si en vez de tener que transmitir 8 letras, se necesita transmitir 16 letras, hacen falta 4 variables binarias, ya que:

$$2^n = 2^4 = 16$$

Para poder codificar todo el alfabeto (27 letras) se necesitarían 5 variables binarias, ya que:

$$2^n = 2^5 = 32$$

En este caso, nos sobrarían combinaciones.

Para codificar más símbolos, como ser las letras más los números (0 al 9) y algunos otros códigos de control se utilizan

"n = 7" o "n = 8"

Elementos, dependiendo del tipo de código.

Como podemos apreciar, ahora los mensajes contienen mayor "cantidad de información", ya que para cada letra debemos transmitir 7 u 8 elementos.

Generalizando, si tenemos una fuente con " $N = 2^n$ " mensajes posibles a transmitir, se requerirá combinar un número mínimo "n" de elementos binarios para codificar cada uno de los "N".

Antes de continuar con las definiciones, vamos a considerar una fuente de información que produce varios mensajes. Sea "A" uno de los mensajes y " $P_A$ " su probabilidad de que sea elegido para su transmisión. De acuerdo con lo expresado describimos a la Información asociada a "A" como una función de su probabilidad, o sea:

$$I_A = f(P_A)$$

Donde la función debe ser determinada. Para encontrar  $f(P_A)$ , es intuitivo suponer los siguientes requerimientos:

The slide has a red header bar with the title 'Funciones' and a blue 'Interacción' button with a hand icon. Below the header are three red boxes containing requirements:

- $f(P_A) > 0$  donde  $0 < P_A < 1$
- $\lim_{P_A \rightarrow 1} f(P_A) = 0$
- $f(P_A) > f(P_B)$  para  $P_A < P_B$

To the right of the boxes is a text box with the following note:

La primera nos indica que la función es positiva, ya que no existe información negativa, (puede ser nula, pero nunca negativa), para la probabilidad que siempre varía entre cero y uno.

Interactiva "Funciones"  
 $f(P_A) > 0$  donde  $0 < P_A < 1$

$$\lim_{P_A \rightarrow 1} f(P_A) = 0$$

$$f(P_A) > f(P_B) \text{ para } P_A < P_B$$

La primera nos indica que la función es positiva, ya que no existe información negativa, (puede ser nula, pero nunca negativa), para la probabilidad que siempre varía entre cero y uno.

La segunda nos dice que cuando la probabilidad se hace mayor (tiende a uno), la información se debe reducir, haciéndose nula cuando la probabilidad vale 1 (100%).

Y la tercera nos dice que para dos informaciones distintas, será mayor aquélla que tiene una probabilidad menor.

Elaboración propia DEPROE, IES siglo 21

Todo esto ya lo vimos anteriormente en forma intuitiva; ahora sólo hemos encontrado alguna relación matemática que nos permitirá concluir con la medición de la información.

De estas expresiones podemos deducir que entre Información y Probabilidad existe una relación muy estrecha, pero son inversamente proporcionales, o sea que cuando una crece la otra decrece.

Existen muchas funciones que satisfacen las tres anteriores, pero la decisión final se obtiene al considerar la transmisión de mensajes independientes.

Cuando el mensaje "A" es entregado al usuario, éste recibe " $I_A$ " unidades de información.

Cuando es entregado un segundo mensaje, la información total recibida debería ser la suma de las informaciones mutuas:

$$I_A + I_B$$

Esto es más fácil de ver si consideramos que "A" y "B" vienen de diferentes fuentes.

Pero supongamos que "A" y "B" provienen de la misma fuente: podemos hablar entonces del mensaje compuesto:  $C = AB$ .

Si "A" y "B" son estadísticamente independientes tenemos:

$$P_C = P_A \cdot P_B$$

Por lo tanto, la información será:

$$C = f(P_A \cdot P_B) \quad (1)$$

Pero la información recibida también es la suma de las informaciones parciales:

$$I_C = I_A + I_B = f(P_A) + f(P_B) \quad (2)$$

Y así, igualando la expresión (1) y la (2) tenemos:

$$f(P_A \cdot P_B) = f(P_A) + f(P_B)$$

Que es el requerimiento para  $f(P_C)$ .

Hay una sola ecuación que satisface las condiciones anteriores y es la función logarítmica

$$f(x) = \log_b(x)$$

Donde "b" es la base del logaritmo.

Así, la información es definida como:

$$I_A = \log_b(1/P_A)$$

Recordar que entre Información (I) y Probabilidad (P) existe una relación inversamente proporcional, siendo el logaritmo la función que provee la proporcionalidad.

Como la probabilidad sólo varía entre  $0 < P_A < 1$ , el logaritmo es positivo, como se desea.

De acuerdo con lo que ya vimos en el ejemplo anterior, la probabilidad de ocurrencia es:

$$P = 1 / N$$

Resulta que:  $N = 1 / P$

O sea que:  $I = \log_2(1/P) = \log_2(P^{-1}) = -\log_2(P)$

Expresión que relaciona la cantidad de información con la probabilidad de que ocurra un evento.

Para poder medir la "Cantidad de Información", es necesario definir la "UNIDAD" de medida. Como todas las unidades, debe utilizarse una convención para determinarla.

De acuerdo con la teoría de la información, puede definirse la cantidad de información de un mensaje "I", como: "El número mínimo "n" de elementos codificados en binario necesarios para identificar el mensaje entre un total de "N" mensajes posibles".

O sea:

$$I = n = \log_2 (N)$$

Resulta práctico relacionar la cantidad de información de un mensaje con el grado de probabilidad de ocurrencia del mensaje.

Ahora sólo nos resta por determinar la base de los logaritmos, ya que al especificar la base "b" del logaritmo, podemos determinar la unidad de información.

Lo más usual es tomar "b = 2" (base del sistema binario) denominándose la unidad así determinada como [bit], como ya habíamos establecido anteriormente.

Dado que el sistema binario es el más sencillo de los infinitos sistemas de numeración de notación posicional, y como las computadoras utilizan este sistema para el manejo de la Información, se define como:

*"Unidad de Cantidad de Información a la obtenida al especificar una de dos alternativas igualmente probables, llamándose [bit] a esa unidad".*

Entonces sí  $P_A = P_B = P = 1/2$ , la cantidad de información será:

$$I_A = I_B = I = \log_2 1/P = \log_2 2 = 1 \text{ [bit]}$$

Recordar que el logaritmo de la base es igual a 1.

La palabra **bit**, define la unidad de cantidad de información y se obtiene por contracción de las palabras inglesas "**binary digit**".

Estas alternativas se presentan, por ejemplo, al observar una moneda lanzada al aire, o la salida de una comunicación digital.

Ya hemos visto que la información está relacionada con la incertidumbre. Entonces, podríamos decir que información es lo que reduce la incertidumbre, por consiguiente, puede afirmarse intuitivamente que:

La cantidad de información es una función "f(P)" que decrece al aumentar la probabilidad "P" de un proceso. La información relativa a un suceso cierto es nula  $f(1) = 0$ ; y  $f(0) = \infty$ .

Si hubiéramos tomado como base "b = e = 2,71828", la base de los logaritmos naturales, tendríamos:

$$I_A = I_B = \ln (1/P_A) = \ln 2 = 1 \text{ [NAT]}$$

Si hubiéramos tomado como base "b = 10", la base de los logaritmos decimales tendríamos:

$$I_A = I_B = \log (1/P_A) = \log 10^2 = 1 \text{ [HARTLEY]}$$

Como es fácil demostrar:

1 HARTLEY = 3,32 bit.

1 NAT = 1,44 bit.

La demostración se deja para que la realice usted.

Sabemos que en el caso de dos posibilidades igualmente probables (caso de la moneda), la probabilidad es:

$$P = 1/2^n$$

Donde: 2 = cantidad de variables y n = Cantidad de elementos

Si generalizamos esta expresión tenemos:

$$P = 1/N^E$$

Donde: N = cantidad de variables y E = Cantidad de elementos

Entonces, por definición, cantidad de información es:

$$I = \log_2(N^E) \text{ [bit]}$$

En el caso de la moneda lanzada al aire es:

N = 2 (las dos alternativas, cara y cruz) y E = 1 (la moneda).

Aplicando la fórmula anterior:

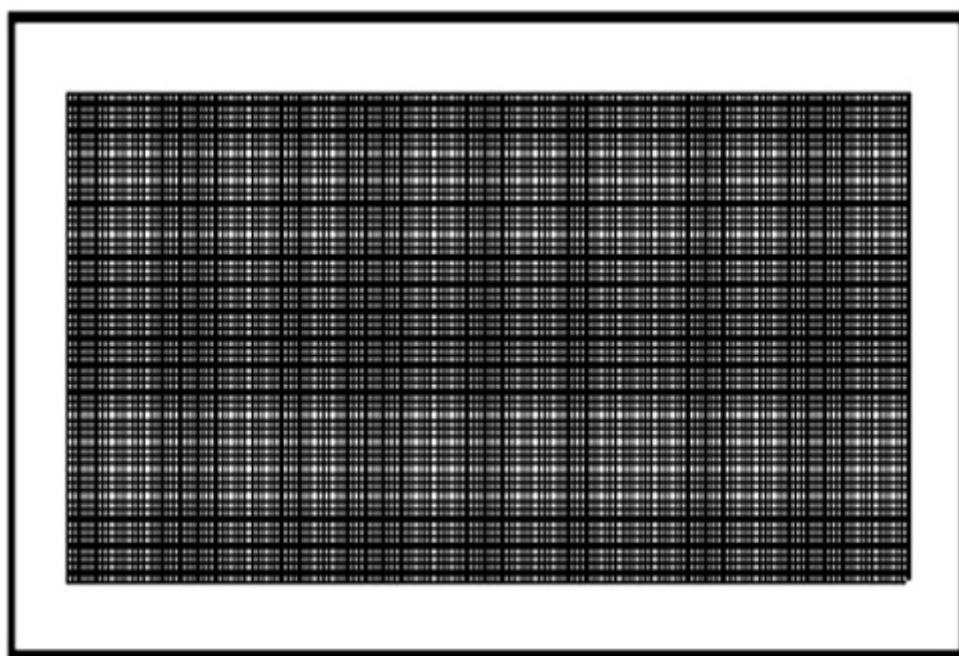
$$I = \log_2 N^E = \log_2 2^1 = 1 \text{ [bit]}$$

Ahora que ya conocemos la unidad de cantidad de información, vamos a ver dos ejemplos prácticos, que nos darán una idea de "Cantidad de Información".

### Ejemplo 1

#### Imagen de TV

A los fines del ejemplo y para facilitar su entendimiento, vamos a realizar algunas simplificaciones. Para ello consideraremos la pantalla compuesta por 500 líneas y 600 columnas, tal como se aprecia en la siguiente figura.



Esto nos da un total de:  $500 \times 600 = 300.000$  puntos.

Estos puntos serán los E elementos que variarán.

Supongamos que cada punto puede tomar 10 valores distintos (las variables N) entre el negro y el blanco, pasando por tonos de 8 grises intermedios.

De esta forma, vamos a tener  $N^E = 10.300.000$  imágenes distintas, que son las combinaciones de los 300.000 puntos variando entre los 10 valores. Si todas son igualmente probables, la cantidad de información será, aplicando la fórmula:

$$I = \log_2(N^E) = \log_2(10^{300.000}) = 300.000 \times \log_2(10) = 300.000 \times 3.32 @ 106 \text{ bits}$$

#### Ejemplo 2:

Vamos a suponer ahora, que tenemos un documento de 1.000 (E) palabras y supongamos que esas palabras fueron elegidas de un repertorio de 10.000 (N) palabras igualmente probables.

La cantidad de información será:

$$\begin{aligned} I &= \log_2(N^E) = \log_2(10.000^{1.000}) = 1.000 \times \log_2(10.000) = 1.000 \times \log_2(10^4) = \\ &= 4 \times 1.000 \times \log_2(10) = 4 \times 1.000 \times 3.32 = 1.328 \times 10^4 @ 10^4 \text{ bits} \end{aligned}$$

Como puede apreciarse, de la comparación de ambos ejemplos, una imagen (simplificada), tiene una cantidad de información de aproximadamente un millón de bit, mientras que un documento escrito está en el orden de los diez mil bit.

Esto nos da una idea de "cantidad de información" y conceptualmente que los métodos visuales, como los gráficos, implican una mayor cantidad de información. De allí los inconvenientes del procesamiento, transmisión y almacenamiento de imágenes.

Con esto podemos hemos demostrado matemáticamente aquel viejo refrán que expresaba que: "Una imagen dice más de mil palabras".

Así, los mensajes para transmitir una de las ocho letras, de nuestro primer ejemplo, contienen 3 bit de cantidad de información. En una computadora, los elementos en cuestión son pulsos eléctricos que pueden tomar dos estados posibles; de allí la definición de unidad de información utilizando los elementos binarios. Por otro lado, el código binario es el sistema numérico de menor base posible

De las definiciones anteriores resulta evidente la diferencia entre "información" y "cantidad de información".

Información se refiere al significado de un conjunto de símbolos, mientras que cantidad de información MIDE

el número de símbolos necesarios para codificar un mensaje, cuya probabilidad de ocurrencia es "P".

En el ejemplo, podemos decir que de las ocho opciones, cada bit recibido, permite decidir una de dos alternativas posibles, codificables mediante mensajes de un solo símbolo: 1 o 0.

El bit es la menor cantidad de información que se puede comunicar y corresponde a la determinación de un mensaje entre dos posibles, cuya probabilidad de ocurrencia es  $P = 1/2$ .

Cualquier forma de información puede simbolizarse mediante bit.

Como ya vimos, si quisiéramos codificar las letras del alfabeto, son necesarios 5 bits, tal como puede verse en la siguiente tabla:

Letra	Código Binario
A	00000
B	00001
C	00010
D	00011
E	00100
F	00101
G	00110
H	00111
I	01000
J	01001
K	01010
L	01011
M	01100
N	01101

Letra	Código Binario
N	01110
O	01111
P	10000
Q	10001
R	10010
S	10011
T	10100
U	10101
V	10110
W	10111
X	11000
Y	11001
Z	11010

"Ejemplo documento (letra-código binario)" | Elaboración DEPROE, IES siglo21

Esta condición supone que todas las letras tienen igual probabilidad de aparición ( $P = 1/27$ ), siendo:

$$I = \log^2(27) = 4,755 \text{ [bit]}$$

O sea que se puede verificar que se necesitan aproximadamente 4,755 bit, lo que redondeando da 5 bit; el redondeo significa que nos quedan combinaciones sin utilizar, ya que "25 = 32" y nosotros sólo utilizamos 27.

Esto último podría haberse estimado directamente sin utilizar los logaritmos, ya que:

$$2^4 = 16 < 27 < 2^5 = 32$$

De esta forma, cada palabra se codificaría con un número de bits igual al número de letras que la constituyen multiplicado por cinco.

Este número de bits podría reducirse, si tenemos presente que algunas letras se repiten con mayor frecuencia que otras, o sea que tienen mayor probabilidad que otras.

Dicho en otros términos, esto significa que nuestro vocabulario obtiene mensajes de una fuente que no es equiprobable (igual probabilidad).

Además, cuando escribimos o hablamos, no existe la misma probabilidad, no solo en la elección de las letras, sino también en las palabras.

Esto hace al problema mucho más complejo de lo que vimos hasta ahora y es motivo de estudios matemáticos de teoría de probabilidades mucho más avanzado.

Nosotros, a fin de simplificar, siempre consideraremos fuentes de símbolos equiprobables.

Una forma de reducir el tamaño de los mensajes es, justamente, valerse de este tipo de características de fuente no igualmente probables, pudiéndose codificar las letras que mayor probabilidad tienen de salir, con menor cantidad de símbolos. Tal es el caso del código Morse para telegrafía, en donde justamente, las letras con mayor probabilidad de salida como la "a" y la "e" son codificadas con la menor cantidad de símbolos.

A título de ejemplo de codificación, donde cada símbolo se codifica de manera distinta, se da a continuación el CÓDIGO MORSE:

### CÓDIGO MORSE

Letra	Código Binario
A	. -
B	- . . .
C	- . . -
D	- . . .
E	.
F	. . . -
G	- - .
H	. . . .
I	..
J	. - - -
K	- . -
L	- . . -
M	- -
N	- .
Ñ	- - . - -
O	- - -
P	. - - .
Q	- - - -
R	- . -

Letra	Código Binario
S	... .
T	-
U	... -
V	... . -
W	. - -
X	- . . -
Y	- . - -
Z	- - - .
1	. - - - -
2	. . - - -
3	. . . - -
4	. . . . -
5	. . . . .
6	- . . . .
7	- - . . .
8	- - - . .
9	- - - - .
0	- - - - -

"Código Morse" | Elaboración DEPROE, IES siglo21

# REFERENCIAS 2

## 2.1 : Sistema binario [NJC2]

Sistema binario [NJC2] :

Es conveniente repasar los sistemas de numeración de notación posicional, como el sistema numérico decimal que conocemos. El sistema binario es un caso particular de los sistemas de notación posicional, y es el más simple de todos dado que su base es 2 (0 y 1).

---



¿Estás listo para un desafío?

**1. Indique la opción correcta**

La cantidad de información depende de la longitud del mensaje.

- Verdadero
- Falso

**2. Indique la opción correcta**

La medida de la información está relacionada con la incertidumbre.

- Verdadero
- Falso

**3. Indique la opción correcta**

¿Cómo se llama al límite de la tasa de información que puede ser transmitida?

- Cantidad de información contenida en un mensaje.
- Tamaño máximo del mensaje.
- Capacidad del sistema de comunicaciones.
- Mínima incertidumbre.

**4. Indique la opción correcta**

¿Cómo es la expresión que relaciona la Información con la Probabilidad? Vea las opciones en la imagen.

- a.** La medida de la información no está relacionada con la incertidumbre
- b.** La medida de la información no es una indicación de la libertad de elección al seleccionar el mensaje.
- c.**  $I = \log_2 1/P$
- d.**  $I = \log_2 N^E$

- Opción A
- Opción B
- Opción C
- Opción D

**5. Indique la opción correcta**

En caso de posibilidades igualmente probables, la cantidad de información: Vea las opciones en la imagen.

- a.** No está relacionada con la incertidumbre
- b.** No reduce la incertidumbre
- c.** Esta indicada por la expresión  $I = \log_2 1/P$
- d.** Esta indicada por la expresión  $I = \log_2 N^E$

- Opción A
- Opción B
- Opción C
- Opción D

**6. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Componentes de un sistema de comunicación

Funcionamiento coordinado en cuanto al tiempo

Concepto de Protocolo

Transmisor - Canal de comunicación – Receptor – Ruido

Conceptos básicos de la teoría de la información

Codificación acordada previamente

Concepto de sincronización

La medida de la información - La capacidad del canal - La codificación

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

La cantidad de información depende de la longitud del mensaje.

Verdadero

Falso

## 2. Indique la opción correcta

La medida de la información está relacionada con la incertidumbre.

Verdadero

Falso

## 3. Indique la opción correcta

¿Cómo se llama al límite de la tasa de información que puede ser transmitida?

Cantidad de información contenida en un mensaje.

Tamaño máximo del mensaje.

Capacidad del sistema de comunicaciones.

Mínima incertidumbre.

## 4. Indique la opción correcta

¿Cómo es la expresión que relaciona la Información con la Probabilidad? Vea las opciones en la imagen.

Opción A

Opción B

Opción C

Opción D

## 5. Indique la opción correcta

En caso de posibilidades igualmente probables, la cantidad de información: Vea las opciones en la imagen.

Opción A

Opción B

Opción C

Opción D

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Componentes de un sistema de comunicación

Transmisor - Canal de comunicación – Receptor – Ruido

Concepto de Protocolo

Codificación acordada previamente

Conceptos básicos de la teoría de la información

La medida de la información - La capacidad del canal – La codificación

Concepto de  
sincronización

Funcionamiento coordinado en  
cuanto al tiempo

# SP2 / H3: Entropía, capacidad de los sistemas y ley de Shannon

## Entropía

En la mayoría de las aplicaciones prácticas, hay que elegir entre mensajes que tienen diferentes probabilidades de ser enviados. El término entropía ha sido tomado prestado de la termodinámica, para designar la cantidad de información media de estos mensajes. La entropía puede ser intuitivamente entendida como el grado de "desorden" en un sistema. En la teoría de la información, la entropía de un mensaje es igual a su **cantidad de información media**. Si en un conjunto de mensajes, sus probabilidades son iguales, la fórmula para calcular la entropía total sería:

$$H = \log_2 (N)$$

Donde N es el **número de mensajes posibles en el conjunto**.

## Codificación y redundancia

Si se transmiten mensajes que están formados por combinaciones aleatorias de las 27 letras del alfabeto, el espacio en blanco y cuatro signos de puntuación, y si suponemos que la probabilidad de cada mensaje es la misma, la entropía sería:

$$H = \log_2 (32) = 5$$

Esto significa que se necesitan 5 bits para codificar cada carácter o mensaje: 00000, 00001, 00010, 11111, etc.

Una transmisión y almacenamiento eficiente de la información exige la **reducción del número de bits utilizados en su codificación**. Esto es posible cuando se codifican textos, porque la colocación de las letras no es aleatoria. Así, por ejemplo, la probabilidad de que la letra que suceda a la secuencia información sea una n es muy alta.

Se puede demostrar que la entropía del lenguaje español normal escrito es aproximadamente de un bit por palabra. La lengua española tiene una gran cantidad de redundancia incorporada, que se denomina redundancia natural. Esta redundancia permite, por ejemplo, a una persona entender mensajes en los cuales faltan vocales, así como descifrar escritura poco legible. **En los sistemas de comunicación modernos, se añade redundancia artificial a la codificación de mensajes, para reducir errores en la transmisión de los mismos.**

## Binit y Bit

Es interesante observar que la palabra dígito binario (binary digit), cuya contracción es [bit], indica que dos estados pueden ser representados por los dígitos binarios: "0" y "1". Pero un **dígito binario puede llevar más de un bit de información, o menos, dependiendo de su probabilidad de ocurrencia**.

Por ello no siempre es correcto decir que un "1" ó un "0" es un bit, ya que esto puede interpretarse como la unidad de información. Esto sólo es cierto para sucesos equiprobables, o sea que la probabilidad de que ocurra un "0" es igual a la probabilidad de que ocurra un "1" y es igual al 50 %.

Pero, sí por ejemplo:

$$P_A = 1/4 \quad P_B = 3/4$$

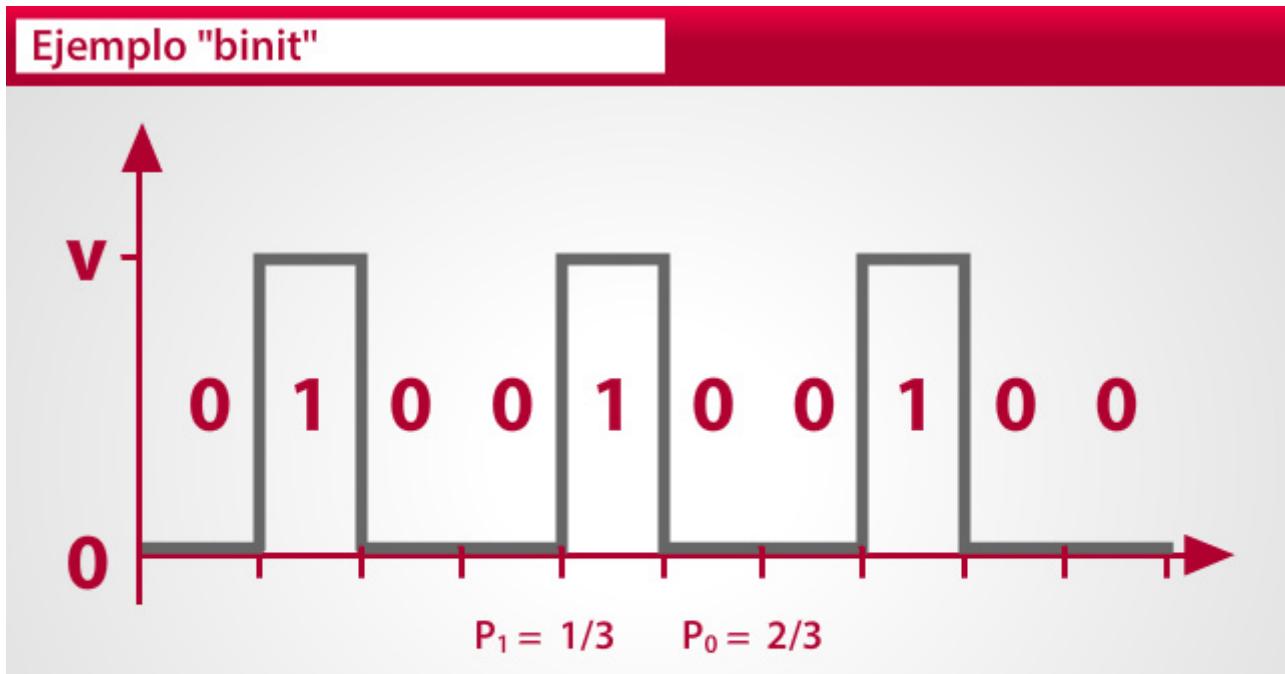
Entonces:

$$I_A = \log_2 (4) = 2 \text{ [bit]}$$

$$I_B = \log_2 (4/3) = 0,414 \text{ [bit]}$$

Para evitar errores de interpretación, a los dígitos binarios como elementos de mensajes se los llama "*binit*", en lugar de bit (aunque esta última es la que se usa habitualmente).

Por ejemplo, un tren de pulsos eléctricos como el de la siguiente figura, está compuesto de binites 1 y binites 0.



La aparición de cualquier binit 1 da una información de:

$$I_1 = \log_2 3 = 1,58 \text{ [bit]}$$

La aparición de cualquier binit 0 da una información de:

$$I_0 = \log_2 3/2 = 0,58 \text{ [bit]}$$

"Ejemplo binit" | Elaboración DEPROE, IES siglo21

Esta aclaración es para evitar que a un dígito de este tren de pulsos lo llamemos 1 bit, pues esto puede interpretarse como unidad de información, cuando en realidad ésta depende de la probabilidad. En la práctica, es frecuente llamar erróneamente bit a los binit.

Veamos algunos ejemplos:

#### Ejemplo 1

Calcular la cantidad de información de una fuente telegráfica teniendo por probabilidades y duración promedio lo siguiente:

$$P_{\text{punto}} = 2/3 \quad P_{\text{raya}} = 1/3$$

**Respuesta**

$$I_p = \log_2 (1/P_p) = \log_2 (1/2/3) = \log_2 (3/2) = \log_2 (3) - \log_2 (2) = 1,5851 - 1 = 0,5851 \text{ bit}$$

$$I_r = \log_2 (1/P_r) = \log_2 (1/1/3) = \log_2 (3/1) = \log_2 (3) = 1,5851 \text{ bit}$$

Nota: Para calcular el  $\log_2 3$  usamos:

$$\log_b(X) = 1 / \log_b(a) \cdot \log_b(X)$$

O sea, para nuestro caso tomaremos la base 10 que es un logaritmo conocido:

$$\log_2(3) = (1 / \log_{10}(2)) \cdot \log_{10}(3) = (1 / 0,301) \cdot 0,4771 = 1,5851$$

### Ejemplo 2

Calcular la información asociada a la caída de una moneda (suceso estadísticamente independiente).

**Respuesta**

$$P_A = P_B = P = 1/2,$$

entonces la cantidad de información será:

$$I_A = I_B = I = \log_2 (1/P) = \log_2 (2) = 1 \text{ [bit]}$$

### Ejemplo 3

Calcular la información entregada por la aparición de una letra entre 32 equiprobables posibles.

**Respuesta**

Suponiendo que todas las letras tienen igual probabilidad de aparición ( $P = 1/32$ ) la información entregada con la aparición de una letra es:

$$I = \log_2(32) = 5 \text{ [bit]}$$

Haciendo el cálculo con el concepto de entropía (cantidad de información media):  $H = \log_2(32) = 5$

Esto significa que se necesitan 5 bits para codificar cada carácter.

### Ejemplo 4

Un sistema de facsímil transmite una imagen que tiene 250 líneas horizontales y 200 puntos por línea. Si cada punto puede tomar 32 niveles equiprobables de brillo, calcular la cantidad de información de la imagen.

**Respuesta**

Cantidad total de puntos:  $250 \times 200 = 50.000$

$$I = \log_2 N^E = \log_2 (3250.000) = 50.000 \times \log_2 (32) = 50.000 \times 5 = 250.000 \text{ [bit]}$$

### Ejemplo 5

Se envía un mensaje usando 5 puntos cada uno (1 mseg) y dos niveles equiprobables de tensión posibles (0 y V).

Pregunta: ¿Qué cantidad de mensajes diferentes se pueden enviar?

Respuesta: La cantidad de mensajes diferentes que se pueden enviar es de  $2^5 = 32$ .

Pregunta: ¿Si en lugar de dos valores equiprobables, cada pulso puede tomar 4 valores distintos, ¿qué

cantidad de mensajes provee esa fuente?

**Respuesta:** La cantidad de mensajes diferentes que se pueden enviar con este tren de pulsos es de  $4^5 = 1024$ .

Como podemos apreciar, en el segundo caso la cantidad de información es bastante mayor.

A continuación le ofrecemos otros ejercicios para resolver:

#### Ejercicio 1

Supongamos que una fuente produce los símbolos A, B, C y D, con probabilidades  $1/2$ ,  $1/4$ ,  $1/4$  y  $1/8$ , respectivamente. Calcular:

- La información en cada caso.
- Si los símbolos son independientes, calcular los bit de información del mensaje CADA.

#### Ejercicio 2

Supongamos una imagen formada por 400 líneas horizontales y cada línea con 300 puntos discretos, con una posibilidad de variación de su brillo de 8 niveles distintos.

¿Cuántas imágenes distintas se podrán formar y qué cantidad de información proveerán?

#### Ejercicio 3

Una fuente produce 5 símbolos con probabilidades:  $1/2 - 1/4 - 1/8 - 1/19 - 1/16$

Calcular la información que provee cada símbolo.

#### Ejercicio 4

Una imagen de TV tiene 625 líneas con 500 puntos por línea y 128 niveles equiprobables de brillo cada punto.

Indicar: ¿Cuántas imágenes distintas pueden generarse? y ¿Qué cantidad de información tiene cada imagen?

## Obtención de la información

La información puede obtenerse por distintas vías, siendo las más comunes:

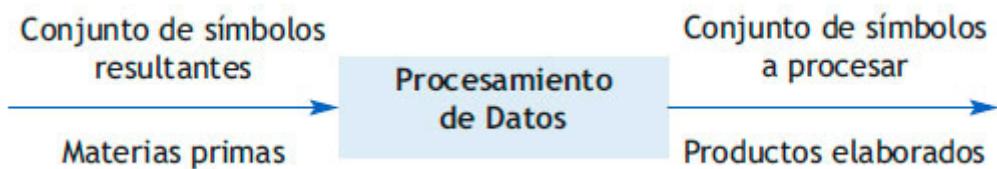
- La percepción de fenómenos naturales: por ejemplo cuando observamos el cielo, o registramos a través de nuestros sentidos la temperatura ambiente, de manera de saber si hace frío o calor y, de esta forma, adaptar nuestro cuerpo a esas condiciones.
- La decodificación de lenguajes creados por el hombre: mediante la lectura de símbolos escritos, o la audición de sonidos producidos por el habla. Esto supone la transmisión de la información a través de distintos medios y hacia un receptor que le asigna el mismo significado de quien transmite.
- El procesamiento de datos: que permite obtener nuevos datos (información para alguien) a partir de la elaboración o transformación de otros datos mediante operaciones específicas, tales como el cálculo, el ordenamiento, la traducción, etc. Por lo tanto, decimos que la información es susceptible de ser transformada.

Es frecuente que el resultado de un proceso de datos sea, a su vez, dato de entrada para otro proceso y así sucesivamente.

El procesamiento que realiza una computadora servirá para definir en qué consiste un proceso de datos, independiente de su forma de realización.

Esencialmente en un procesamiento de datos, un conjunto de símbolos se transforma en un nuevo conjunto de símbolos, o en otra estructura de datos.

La siguiente figura esquematiza el concepto anterior: un conjunto de símbolos *datos de entrada*, serán procesados para dar lugar a otro conjunto de símbolos *datos de salida* requeridos.



"Procesamiento de datos" | Elaboración DEPROE, IES siglo21

Cualquier proceso, ya sea industrial, biológico, químico, físico, etc., supone materias primas específicas (entradas), que serán transformadas a fin de lograr un cierto producto requerido (salidas).

Los procesos de datos son el medio para obtener datos a partir de otros datos, considerados primarios.

Los datos resultantes de un proceso, convenientemente ordenados representarán información para quien les asigne una significación que permita encarar una decisión.

Debe tenerse presente que el concepto de *estructura* alude a los *elementos* que la conforman y a las *relaciones* o conexiones entre ellos.

La palabra *computar* también se refiere al proceso de efectuar operaciones con el objeto de obtener un resultado.

Un *cálculo* es un conjunto finito de operaciones aplicadas a un conjunto finito de datos, con el fin de resolver un problema. Si esto se consigue, obtenemos un *algoritmo*.

Un *algoritmo* es un procedimiento que asegura, mediante un número finito de pasos, una salida requerida a partir de una entrada dada, independientemente del tiempo en que se realiza.

Un procedimiento es un método preciso, paso a paso, para concretar una solución a un problema.

Las *operaciones* pueden definirse como las reglas para manipular o transformar datos.

Una forma de definir o describir una operación es mediante una regla computacional que involucre una sucesión finita de operaciones más sencillas.

Las operaciones de una computación deben llevarse a cabo según un cierto orden de precedencia, de manera que los resultados de unas operaciones puedan ser usados por otras.

La forma más sencilla de precedencia es la ejecución de las operaciones en estricto orden secuencial en el tiempo. Este tipo implica *procesos secuenciales*, con operaciones totalmente ordenadas en el tiempo.

Dos o más procesos son *concurrentes*, si su ejecución se superpone en el tiempo.

## Capacidad de los sistemas

Si bien a priori puede verse que esta teoría está relacionada con los sistemas de comunicaciones, dado que su procedencia nació del estudio de éstos, la misma es aplicable a cualquier tipo de sistema, cualquiera sea la característica del mismo, de la misma forma que una ecuación matemática es aplicable a la física, a la mecánica, a la electrónica o a la medicina. Por ello, cuando hablamos de capacidad de un canal de comunicaciones, debemos tener en cuenta que el canal es un caso particular de sistema.

Nyquist \* 3.1 dedujo una ecuación que expresa la velocidad máxima de datos a través de un canal sin ruido, con un ancho de banda finito.

Shannon lo amplió para el caso de un canal sujeto a ruido aleatorio (térmico).

**Según Nyquist**, "si una señal arbitraria se la hace pasar a través de un filtro con un **Ancho de Banda** \* 3.2 B, la señal filtrada puede reconstruirse por completo mediante la obtención simple y sencilla de por lo menos  $2B$  muestras por segundo".

El llevar a cabo muestreos de la línea a frecuencias más altas no tiene sentido, porque los componentes de frecuencias más altas no pueden recuperarse por haber sido filtradas.

Si la señal contiene "V" niveles discretos, el teorema de Nyquist establece que:

$$\text{Velocidad máxima de datos} = 2B \log_2 V \text{ [bits/seg]}$$

Por ejemplo, un canal sin ruido de 3,3 KHz (canal telefónico típico) no puede transmitir señales binarias (de dos niveles lógicos) a más de 6600 bps.

$$\text{Velocidad máxima de datos} = 2 \times 3300 \log_2 2 \text{ [bits/seg]}$$

$$\text{Velocidad máxima de datos} = 2 \times 3300 \times 1 \text{ [bits/seg]}$$

$$\text{Velocidad máxima de datos} = 6600 \text{ [bits/seg]}$$

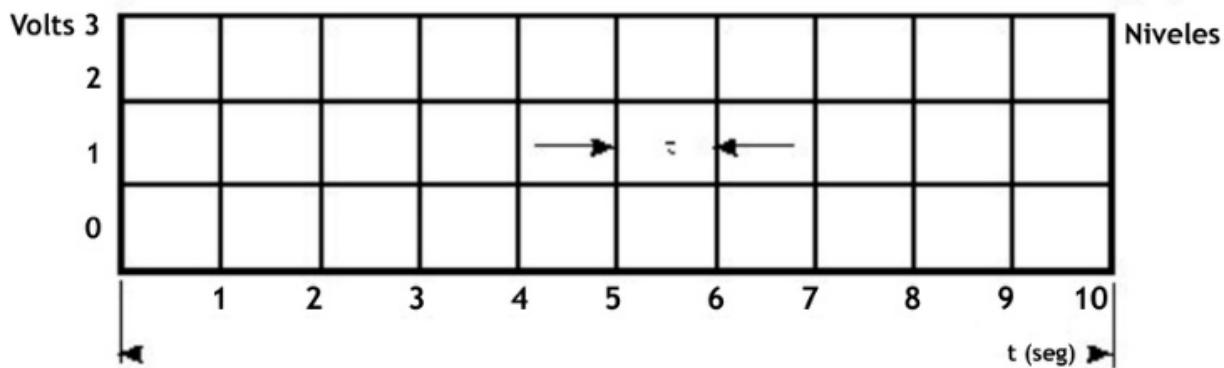
Esto sin considerar el ruido, y teniendo en cuenta que sólo se transmiten 2 niveles de tensión por cada pulso.

Al diseñar un sistema de transmisión, se debe tener en cuenta la cantidad de información que puede transportar el sistema.

Para ver la forma en que estos conceptos se ajustan a las comunicaciones, consideraremos el diagrama tensión - tiempo que sigue:

Supongamos un intervalo de "T" segundos de duración en el cual se transmite información y una amplitud máxima de 3 voltios.

- ¿Cuánta información puede transmitirse en este intervalo?
- ¿Por qué existe un límite en la cantidad de información?



"Capacidad de los sistemas" | Elaboración DEPROE, IES siglo21

$$n = \text{niveles} \quad T = \text{período} = 10 \text{ seg} \quad V = 3 \text{ Voltios}$$

Si la información está relacionada con señales que cambian impredeciblemente en el tiempo,

**¿Por qué no hacer que la señal cambie tan rápidamente y con tantas subdivisiones de la amplitud máxima como se quiera?**

Esto implicaría el aumento del contenido de información en forma indefinida.

Como estamos ante sistemas físicos, éstos no podrán aumentar indefinidamente la velocidad de cambio de una señal, ni distinguir infinitos valores de tensión o niveles por lo siguiente:

1. Todos los sistemas tienen dispositivos de almacenamiento de energía, por lo que cambiar una señal implica modificar dos de energía.
2. Todo sistema provoca variaciones inherentes o fluctuaciones de tensión para medir la amplitud de la señal, por lo que no puede subdividirse indefinidamente la señal. Estas variaciones indeseadas de los parámetros que varían se llaman ruido.

Hay, entonces, un tiempo mínimo "t" que se requiere para que la energía cambie, y una variación mínima detectable de la amplitud.

Por ejemplo, en la figura anterior:  $t = 1 \text{ seg}$ ; y las variaciones de tensión son  $\pm 1 \text{ Voltio}$ .

Como la amplitud máxima es de  $3 \text{ V}$ , sólo existen 4 niveles detectables.

Si la señal varía menos de 1 voltio, no podrá ser distinguida entre las variaciones indeseables del ruido.

Se entiende por *Cantidad de Información* el número de combinaciones diferentes de amplitudes de la señal a transmitirse en ese tiempo.

Fueron éstos los argumentos que empleó Shannon para desarrollar su concepto de capacidad de un canal.

La capacidad del sistema, o velocidad máxima a la que puede transmitirse información, debe ser medible en términos de "t" y de "n".

Una medida cuantitativa de la capacidad del sistema puede deducirse si se supone que la información transmitida en el intervalo de 10 segundos de la figura, está directamente relacionada con el número de combinaciones diferentes de amplitud de la señal.

## ¿Cuántas combinaciones pueden ser especificadas?

En el ejemplo, existen 4 posibilidades por cada intervalo.

Para un intervalo tendremos 4 combinaciones; para dos intervalos,  $4^2 = 16$  combinaciones; para 3 intervalos,  $4^3 = 64$  combinaciones y así sucesivamente.

Para "n" niveles en intervalos de "t" segundos, el número total de combinaciones en un tiempo T (seg) será:

$$n^{T/t}$$

Con esta suposición básica, la información transmitida en T, segundos se relaciona con el número de combinaciones de señales.

Sin embargo, intuitivamente puede notarse que la información debe ser proporcional al tiempo de transmisión. Al duplicar T se debería doblar el contenido de información.

Entonces, el contenido de información puede hacerse proporcional si tomamos el **logaritmo** \* 3.3 de  $n^{T/t}$ , con lo que resulta:

$$\text{Información transmitida en T (seg)} \propto * 3.3 \log (n^{T/t})$$

$$\text{Información transmitida en T (seg)} \propto T/t \log (n)$$

El factor de proporcionalidad dependerá de la base de los logaritmos empleados. La base más simple y la más usada es 2.

$$\text{Información} = (T/t) \log_2 (n) [\text{bit}]$$

La unidad de información definida de esta manera es el "bit".

Para nuestro ejemplo será:

$$\text{Información} = (10/1) \log_2 (4) = 20 \text{ bits}$$

Si hubiéramos tenido dos niveles de tensión:

$$\text{Información} = (10/1) \log_2 (2) = 10 \text{ bits}$$

La capacidad del sistema puede definirse como la máxima velocidad de transmisión de información:

$$C = \frac{\text{Información}}{T} = \frac{1}{t} \log_2 n \text{ [bits/seg]}$$

La capacidad es, pues, inversamente proporcional al mínimo intervalo de tiempo de commutación (t), y proporcional al logaritmo de "n".

Esto es fácil de ver intuitivamente, ya que cuando más estrecho es el pulso, o sea cuando más pequeño es t, mayor será la cantidad de pulsos por unidad de tiempo, por lo tanto mayor será la velocidad del canal.

Por otro lado, cuanto mayor es la cantidad de niveles de codificación, mayor será la cantidad de información, por lo que ésta influye en forma directamente proporcional.

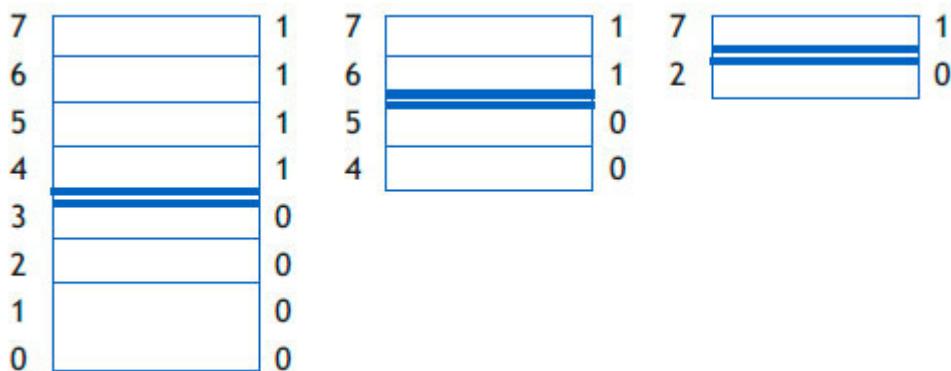
## Dígitos binarios en la transmisión de Información

## Información = $T/t \log_2 n$ [bit]

El uso de log en base 2 lo podemos explicar como sigue: Supongamos una señal que varía entre 0 y 7 voltios. A causa de las limitaciones del sistema, en el intervalo "t" no hay variaciones sensibles de la señal.

¿Puede enviarse esta información con menos de 8 niveles? La respuesta es SÍ. La forma más sencilla es la de especificar si existe o no un nivel. Para 8 niveles de tensión se necesitan 3 instrucciones SÍ - NO.

Veamos la siguiente imagen:



"8 niveles de tensión" | Elaboración DEPROE, IES siglo21

Supongamos que la señal está en 7 voltios. Primero se pregunta si está en los cuatro niveles superiores o inferiores:

1 = superior

0 = inferior

Luego, se elige dentro del grupo si es superior o inferior, y así sucesivamente.

O sea que el nivel 7 voltios = 111

Nivel	Código binario
7	111
6	110
5	101
4	100
3	011
2	010
1	001
0	000

"Niveles y códigos binarios" | Elaboración DEPROE, IES siglo21

De esta forma, en vez de transmitir un valor de "7 voltios", se transmiten tres intervalos SÍ - NO.

Esto se llama **codificación binaria**.

Cada etiqueta SÍ - NO es un bit.

Para "n" niveles se requiere

$$\log_2 n \text{ [bits]}$$

## Ley de Shannon - Hartley

SHANNON demostró que la capacidad tiene relación con la potencia de la señal y la de ruido, en la forma:

$$C = B \log_2 (1 + S/R) \text{ [bits/seg]}$$

Donde S es el nivel de señal y R el nivel de Ruido, y B es el ancho de banda del canal de comunicaciones.

La demostración es más compleja de los alcances de este libro; sin embargo, podemos decir que está basada en la expresión de Nyquist, pero teniendo en cuenta el ruido, y para ello debe considerarse en cuenta la energía puesta en juego en las señales eléctricas.

Según el teorema de Nyquist:

$$C = 2B \log_2 (n) = B \log_2 (n^2) \text{ [bits/seg]}$$

Pero n tiene que ver con los valores de tensión posibles y por lo tanto con la energía de la señal. Si se reemplaza el valor de  $n^2$ , se tiene una expresión que tiene en cuenta la relación entre la señal y el ruido, o sea, la relación S/R que aparece en la fórmula:

Como ya dijimos anteriormente, el espaciamiento entre niveles de señal depende de la relación S/R.

En última instancia, esto depende del ruido al tratar de decodificar las señales recibidas, y éste depende de condiciones exógenas (externas) al sistema.

*Veamos un ejemplo:*

Un canal telefónico de Ancho de Banda de 3300 Hz, y una S/N = 30 dB \* 3.5 (parámetros típicos del sistema) tiene una capacidad teórica de:

$$C = 3300 \log_2 (1 + 1000) \text{ [bits/seg]}$$

Recordar que:

$$\log_2 1001 = 1/\log_{10} 2 \cdot \log_{10} 1000 = (1/0,30103) \times 3 = 9,9657$$

$$C = 3300 \times 9,9657 = 32886 \text{ [bps]}$$

En la práctica es imposible siquiera aproximarse al límite de Shannon.

Una velocidad de 9600 bps se considera excelente, y ésta se obtiene enviando 4 bits a 2400 baudios.

Las velocidades superiores, por ejemplo en los módem actuales (56KB), se logran actuando sobre la información, ya sea comprimiéndola, codificándola, corrigiendo errores, etc., de manera de lograr velocidades de bit por segundo más altas.

# REFERENCIAS 3

## 3.1 : Harry Nyquist

Harry Nyquist

(Nilsby, 1889-Harlingen, 1976) Ingeniero estadounidense de origen sueco. Especializado en cibernética, enunció el criterio de estabilidad de un servomecanismo. Se le debe la teoría matemática de los amplificadores de reacción negativa, que se generalizó durante la II Guerra Mundial en los servomecanismos lineales.

---

## 3.2 : Ancho de banda

Ancho de banda:

En comunicaciones, un indicador de la cantidad de datos que pueden transmitirse en determinado periodo de tiempo por un canal de transmisión, por ejemplo un radiotransmisor, una antena parabólica o el cableado que conecta a dos computadoras.

Por lo general, el ancho de banda se expresa en ciclos por segundo (herz, Hz), o en bits por segundo (bps). Por ejemplo, un módem de 14.400 bps es capaz, en teoría, de enviar 14.400 bits de datos por segundo, mientras que una conexión Ethernet con un ancho de banda de 10 megabits por segundo, puede enviar casi 700 veces más datos en el mismo periodo de tiempo.

---

## 3.3 : Función logarítmica

Función logarítmica: Tomamos la función logaritmo porque tenemos que resolver una función exponencial. Una de las propiedades del logaritmo es que el exponente queda multiplicando a la base. La razón de por qué tomar logaritmo ya fue explicada anteriormente, cuando se trató "cantidad de Información".

---

## 3.4 : Proporcionalidad

El símbolo  $\propto$  significa proporcionalidad. No es una igualdad. Sólo sabemos que es proporcional. Y no confundir con el signo de infinito  $\infty$ .

---

## 3.5 : dB

Es una unidad de medida que está expresada por.

$$\text{dB (decibel)} = 10 \log_{10} V_1/V_2$$

Siendo  $V_1$  y  $V_2$  dos valores que pueden ser tensiones eléctricas o niveles de energía.

Si  $V_1$  es la señal a transmitir y  $V_2$  es el ruido, se puede determinar que para que haya una buena transmisión la señal debe ser mil veces superior al ruido, o sea la relación:

$$V_1/V_2 = S/R = 1000$$

Entonces tendremos:

DB (decibel) =  $10 \log_{10}$

$1000 = 10 \times 3 = 30$

En ton ces tendremos que una variación de 30 dB equivale a una relación S/R = 1000.

---



¡Vamos a comprobar cuánto aprendiste!

**1. Indique la opción correcta**

Un binit puede llevar más de un bit.

- Verdadero
- Falso

**2. Indique la opción correcta**

¿A qué llamamos entropía?

- A la totalidad de información de una fuente.
- A la información que almacena una fuente.
- Al flujo de información promedio de una fuente.
- A la información instantánea de una fuente.

**3. Indique la opción correcta**

La tasa de información es la velocidad de:

- La información.
- Los binites.
- Los bytes.
- Los símbolos.

**4. Indique la opción correcta**

Según la ley de Shannon, la capacidad del canal es proporcional a:

- El ancho de banda y el nivel de ruido.
- El ancho de banda y el logaritmo de la relación señal/ruido.
- La relación señal/ruido y la amplitud de la señal.
- El ancho de banda y la amplitud de la señal.

**5. Indique la opción correcta**

¿A qué llamamos ancho de banda?

- Al rango entre la frecuencia más baja y más alta de un canal de transmisión.
- Al rango entre la frecuencia media y más alta de un canal de transmisión.
- Es el rango entre la frecuencia media y más baja de un canal de transmisión.
- Es el rango entre la frecuencia de la portadora.

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Un binit puede llevar más de un bit.

Verdadero

Falso

## 2. Indique la opción correcta

¿A qué llamamos entropía?

A la totalidad de información de una fuente.

A la información que almacena una fuente.

Al flujo de información promedio de una fuente.

A la información instantánea de una fuente.

## 3. Indique la opción correcta

La tasa de información es la velocidad de:

La información.

Los binitos.

Los bytes.

Los símbolos.

## 4. Indique la opción correcta

Según la ley de Shannon, la capacidad del canal es proporcional a:

El ancho de banda y el nivel de ruido.

El ancho de banda y el logaritmo de la relación señal/ruido.

La relación señal/ruido y la amplitud de la señal.

El ancho de banda y la amplitud de la señal.

## 5. Indique la opción correcta

¿A qué llamamos ancho de banda?

Al rango entre la frecuencia más baja y más alta de un canal de transmisión.

Al rango entre la frecuencia media y más alta de un canal de transmisión.

Es el rango entre la frecuencia media y más baja de un canal de transmisión.

Es el rango entre la frecuencia de la portadora.

## SP2 / Ejercicio resuelto

Utilizando las herramientas precedentes, aplicaremos lo aprendido a la resolución de la situación profesional.

Una imagen de 5 megapixels está compuesta por 5.000.000 de pixeles y cada punto tiene 256 valores equiprobables de color.

Estamos en condiciones de calcular entonces:

a) ¿Cuántas imágenes distintas pueden generarse?

$$N = \text{valores de brillo} = 256$$

$$E = \text{puntos} = 5.000.000$$

$$N^E = 256^{5.000.000}$$

b) ¿Qué cantidad de información contiene cada una?

Si todas son igualmente probables, la cantidad de información será, aplicando la fórmula:

$$\begin{aligned} I &= \log_2 N^E = \log_2 256^{5.000.000} = 5.000.000 \times \log_2 256 = 5.000.000 \times \log_2 2^8 = \\ &= 5.000.000 \times 8 \log_2 2 = 5.000.000 \times 8 \times 1 = 40.000.000 \text{ [bit]} \end{aligned}$$

c) Si se transmite a una velocidad de 100.000.000 bps, ¿cuántos minutos se tarda en trasmitir una imagen?

Partiendo de que nuestra red LAN fue instalada para funcionar a la velocidad típica de 100 mbps (100.000.000 bits/seg), aplicamos regla de tres simple:

100.000.000 bits tardan 1 segundo

40.000.000 bits tardan "X" segundos

entonces,

$$40.000.000 \text{ bits} / 100.000.000 \text{ bits/seg} = 0,4 \text{ segundos}$$

Como podemos observar, el tiempo calculado es una fracción de segundo.

Para completar el análisis deberíamos observar el comportamiento de los usuarios, pues no podemos determinar las cantidades de requerimientos que se pueden producir al mismo tiempo, por lo que nuestro asesoramiento será:

- No basar la estrategia de marketing sobre el hecho de mostrar las imágenes en tiempo real tomadas de las computadoras de los arquitectos de la empresa.
- Tener copias de las imágenes a utilizadas con mas frecuencia.
- A fin de minimizar el espacio de almacenamiento y agilizar la velocidad, utilizar formatos de imágenes que incluyan compresión (tales como archivos del tipo JPG por ejemplo) en vez de formatos que contengan la información completa (tales como archivos del tipo bitmap o bmp)

## SP2 / Ejercicio por resolver

Las imágenes que quiere mostrar la empresa a sus clientes estarán presentadas en un monitor LED que tiene una resolución FULL HD (1920 pixeles de ancho x 1080 píxeles de alto) de 1920 por 1080 pixeles y cada pixel tiene 24 niveles equiprobables de color.

Determine:

- a) ¿Cuántas imágenes distintas pueden generarse?
- b) ¿Qué cantidad de información contiene c/u?
- c) Si se transmite a 100 Mbps, sin utilizar compresión de imágenes, ¿Cuánto tarda en transmitirse cada imagen?



¿Te animás a medir cuánto aprendiste?

**1. Indique la opción correcta**

La Teoría de la información fue desarrollada inicialmente por Claude E. Shannon.

- Verdadero
- Falso

**2. Indique la opción correcta**

La cantidad de información no depende del tamaño del mensaje.

- Verdadero
- Falso

**3. Indique la opción correcta**

Un dígito binario puede llevar mas de un bit de información o menos, dependiendo de su probabilidad de ocurrencia.

- Verdadero
- Falso

**4. Indique la opción correcta**

¿A qué llamamos información?

- A todo aquello que por convención nos remite a algo que no necesariamente necesita estar presente.
- A la propiedad o calidad de los entes al ser representados simbólicamente.
- A todas aquellas representaciones simbólicas que contribuyen a disminuir la incertidumbre.
- A la representación simbólica de entes y sucesos.

**5. Indique la opción correcta**

Para relacionar la cantidad de información con la probabilidad, Shannon presentó la siguiente fórmula:  
Vea formulas en la imagen adjunta.

**Opción A.**  $I = \log_2 1/p$

**Opción B.**  $P = 1/N^E$

**Opción C.**  $I = \log_2 N^E$  [bit]

**Opción D.**  $H = \log_2 N$

- Opción A
- Opción B
- Opción C
- Opción D

**6. Indique la opción correcta**

La cantidad de información es: Vea formulas en la imagen adjunta.

**Opción A.**  $I = \log_2 1/p$

**Opción B.**  $P = 1/N^E$

**Opción C.**  $I = \log_2 N^E$  [bit]

**Opción D.**  $H = \log_2 N$

- Opción A
- Opción B
- Opción C
- Opción D

**7. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Entropía

Rango entre la frecuencia más baja y

más alta de un canal de transmisión

Cantidad de  
Información

Proporcional al ancho de banda y al  
logaritmo de la relación señal/ruido

Ancho de banda

El número de símbolos necesarios

para codificar un mensaje

Capacidad de un  
canal

Cantidad de información media de los  
mensajes

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

La Teoría de la información fue desarrollada inicialmente por Claude E. Shannon.

Verdadero

Falso

## 2. Indique la opción correcta

La cantidad de información no depende del tamaño del mensaje.

Verdadero

Falso

## 3. Indique la opción correcta

Un dígito binario puede llevar mas de un bit de información o menos, dependiendo de su probabilidad de ocurrencia.

Verdadero

Falso

## 4. Indique la opción correcta

¿A qué llamamos información?

A todo aquello que por convención nos remite a algo que no necesariamente necesita estar presente.

A la propiedad o cualidad de los entes al ser representados simbólicamente.

A todas aquellas representaciones simbólicas que contribuyen a disminuir la incertidumbre.

A la representación simbólica de entes y sucesos.

## 5. Indique la opción correcta

Para relacionar la cantidad de información con la probabilidad, Shannon presentó la siguiente fórmula:

Vea formulas en la imagen adjunta.

Opción A

Opción B

Opción C

Opción D

## 6. Indique la opción correcta

La cantidad de información es: Vea formulas en la imagen adjunta.

Opción A

Opción B

Opción C

Opción D

## 7. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Entropía	Cantidad de información media de los mensajes
Cantidad de Información	El número de símbolos necesarios para codificar un mensaje
Ancho de banda	Rango entre la frecuencia más baja y más alta de un canal de transmisión
Capacidad de un canal	Proporcional al ancho de banda y al logaritmo de la relación señal/ruido

# **Situación profesional 3: ¿Qué modelo de referencia utilizaremos?**

## **Modelos multicapa: el modelo de referencia OSI**

La empresa para la que usted trabaja como pasante está muy satisfecha con su trabajo. Debido a expectativas de un mayor crecimiento, le plantea que estudie cuál es la factibilidad de incrementar las conexiones de la red a otro edificio contiguo y, por posibles inversiones futuras, a otra sucursal.

Ante esta situación se le plantea si está en condiciones de afirmar si los servicios que corren sin problemas en la red actual (tales como la transferencia de archivos, correo electrónico y algunas aplicaciones) podrán seguir siendo prestados en una red más grande. Además, está la inquietud de adquirir programas de administración empresarial, para lo cual le preguntan a usted si esta nueva aplicación se puede agregar a las que actualmente están ejecutándose en la red.

# SP3 / H1: Principio de funcionamiento de los modelos multicapa

A fin de poder dar una respuesta a la situación planteada, investigaremos cómo es la estructura y cuáles son los principios sobre los cuales está asentado el modelo de referencia utilizado para diseñar las redes. De esta forma podremos comprender y explicar cómo funcionan las redes y cuáles serán sus capacidades y limitaciones.

Por esto es que necesitamos conocer cómo es un modelo de comunicaciones. En esta situación profesional le presentaremos el Modelo de Referencia OSI.

Las redes permiten compartir información a través de caminos comunes y posibilitan la conexión de unos con otros.

El objetivo de toda red de computadoras es que los usuarios puedan establecer comunicaciones a fin de compartir recursos e información.

Lo que queremos para los usuarios es que su trabajo sea tan sencillo como interactuar con una interfaz simple y versátil de un programa de aplicación.

El diseño e instalación de una red implica múltiples consideraciones, entre las cuales podemos mencionar: velocidades de transferencia, costos, confiabilidad y seguridad en el movimiento de los datos, cantidad de usuarios, etc. Cada uno de estos interrogantes puede ser respondido de una forma diferente, dependiendo del objetivo que se persiga al construir la red.

Por ejemplo, años atrás la respuesta estaba en función del armado de grandes redes entre grandes equipos, verdad que fue cambiando, especialmente con la aparición y uso comercial extensivo de las PC.

De esta forma se comenzó a pensar cómo integrar estos equipos más pequeños; así se extendió el concepto de redes amplias a redes locales.

Una red local (LAN=Local Area Network) es utilizada dentro de un área geográfica limitada, siendo por lo general privada.

Las redes amplias (WAN=Wide Area Network), son utilizadas para grandes distancias, y muchas veces sus vínculos son compartidos entre múltiples usuarios relacionados o no.

Pensemos en la siguiente situación: usted es un usuario de una sencilla red LAN peer-to-peer, por ejemplo Windows 7, y está colaborando en un proyecto con otros compañeros de trabajo. Uno de sus compañeros de trabajo ha guardado en el disco rígido de su computadora un informe realizado en un procesador de textos y le pide que lo revise. Ud. quiere acceder a dicho archivo directamente desde su máquina; digamos más técnicamente que quiere efectuar una transferencia de archivos desde la computadora de su compañero a la suya. Por lo tanto, espera poder transferir el informe con sólo un par de clicks de su mouse, y eso es lo que consigue.

En el caso mencionado, el Explorador de Windows le permitirá acceder al disco rígido de su compañero a través de la carpeta de Entorno de Red (siempre que su compañero la haya asignado como un recurso compartido). El usuario pretende acceder a los archivos remotos almacenados en otras computadoras de la red de forma tan sencilla como acceder a su propio disco rígido.

Sin embargo, sabe que en realidad los bytes que componen dicho archivo deben viajar por los cables de la red, quizás atravesando dispositivos como concentradores (*hub*), puentes (*bridges o switches*), enruteadores (*routers*) y algunos otros elementos constitutivos de una red hasta llegar a las placas de red. Obviamente, Ud. no desea

tener que especificar las características de cada uno de estos medios. Sería prácticamente imposible trabajar en un entorno de red si cuando quisiera transferir el archivo mencionado, además de indicar de dónde lo quiere bajar (la dirección o el nombre de la computadora de su compañero), debe indicar el tipo de placa de red que utiliza, la que utiliza su compañero, el tipo de cableado (por ejemplo, indicando si es coaxial, UTP o fibra óptica), la longitud de los mismos, y muchas más características (como por ejemplo, el control de la integridad de los bits transferidos: ¿Son los bits que recibió su placa de red los mismos que estaban guardados en el disco rígido de su compañero?). El usuario espera que "todas estas cosas se hagan solas" y así debe ser.

El usuario espera que todas las funciones inherentes al funcionamiento de la red sean transparentes para él: esto quiere decir que él sólo deberá "ver" del otro lado de la red al otro usuario y no la red que hay en medio. Esto también significa que él quiere ser independiente de las características específicas de la red que los comunique: si se rompe su placa de red y debe cambiarla por otra, espera que funcione exactamente igual y que no tenga que hacer ningún cambio en su forma de trabajar; si el día de mañana cambia el cableado coaxial por UTP, con Hub no debería tener que variar en nada sus programas ni la forma de usarlos.

Esto se consigue gracias a la estratificación por capas, concepto sobre el cual están diseñadas las redes.

## Arquitectura de Redes

Las redes se organizan en capas o niveles a fin de reducir la complejidad. Cada capa se construye sobre su predecesora, y sirve a la siguiente. El número de capas, el nombre y contenido, varían de una a otra red.

En cualquier red, el propósito de cada capa es ofrecer ciertos servicios a las capas superiores, liberándolas del conocimiento detallado de "ómo" se realiza ese servicio.

La capa "n" de una máquina dialoga con la capa "n" de otra.

Al conjunto de capas y protocolos se los denomina ARQUITECTURA DE RED. Ésta deberá contener la información necesaria y suficiente que permita construir el software y el hardware de cada capa siguiendo el protocolo apropiado.

En la parte (la capa) más alta de toda pila de protocolos estratificados en capas, se encuentra el usuario final; "debajo" se encuentra el sistema de red (su computadora conectada a la red física). Ud. quiere comunicarse con otro usuario, que también se encuentra en la capa más alta de su sistema, a su misma altura o de la misma jerarquía (técnicamente se dice que son entidades homólogas); sin embargo, para hacerlo sabe que necesita utilizar los servicios que le proveen los programas de aplicación que tiene cargados en su computadora. No le interesa cómo hacen las computadoras para comunicarse entre sí, quiere que lo que ocurre en las capas inferiores a la suya sea transparente.

Para comunicarse con su compañero (la entidad homóloga), por ejemplo, mediante un e-mail, debe acordar algunos detalles de antemano, por ejemplo en qué idioma lo harán, es decir se ponen de acuerdo en un protocolo de comunicación.

Si bien la comunicación que se desea establecer es entre dos capas homólogas, que se encuentran "a la misma altura", para poder establecer la comunicación, las entidades de las capas superiores utilizan los servicios de las capas que se encuentran por debajo. Este proceso es totalmente transparente para la entidad de la capa superior, de tal forma que se mantiene independiente de la forma en la cual las capas de nivel inferior establecen la comunicación.

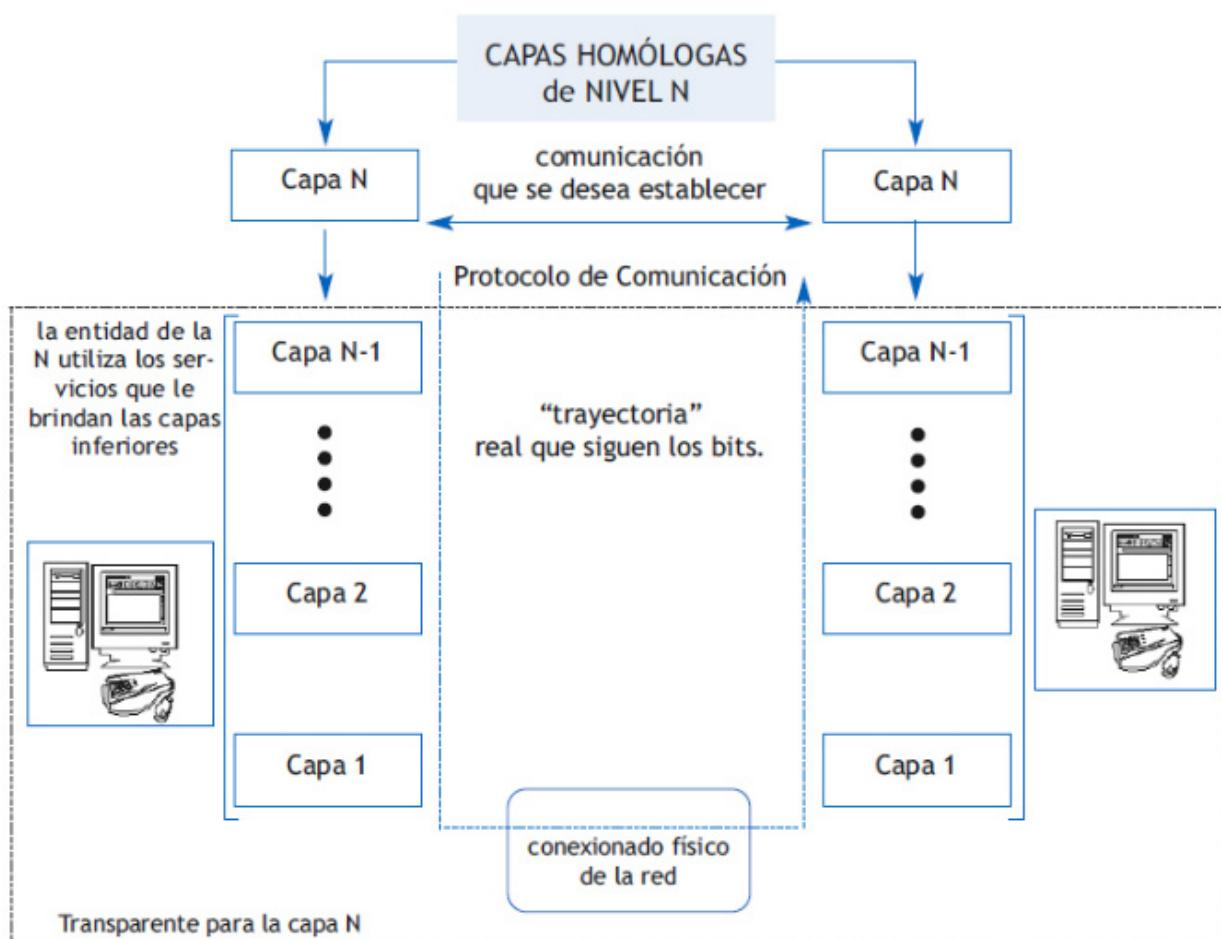
## Las Capas

Ahora que tiene una visión general sobre los objetivos y el funcionamiento aproximado de los modelos de redes estratificados en capas, vamos a aclarar algunos puntos:

Habitualmente no se ubica una capa especial para el usuario; sin embargo, éste siempre se encuentra en un nivel superior al de la capa superior del modelo.

Todo lo dicho en el ejemplo anterior es intrínsecamente cierto y se extiende a todos los niveles de capas. Por ejemplo, si el modelo consta de 5 capas, enumeradas de 1 a 5 de abajo hacia arriba, la capa superior (la 5) del emisor se comunica con su capa homóloga en el receptor, en forma horizontal mediante el uso de un protocolo de comunicación. En realidad, la entidad de la capa 5 utiliza los servicios que le ofrece la capa 4, y la capa 4 utiliza los servicios que le ofrece la capa 3, y así sucesivamente. A ninguna de las capas le interesa cómo realiza el servicio la capa inferior. "Los Bytes" siguen una trayectoria "hacia abajo" en la pila de capas del emisor hasta llegar a la parte física de la red, luego siguen un camino ascendente en el receptor. Como lo habíamos comentado anteriormente, lo que ocurre debajo de una capa es transparente para la capa de nivel superior, la cual sólo desea establecer una comunicación con su homóloga a nivel horizontal.

La siguiente figura es equivalente a la anterior, pero un tanto más formal:



La comunicación se establece entre las capas homólogas, de Nivel N pero éstas se valen de los servicios que les brindan las capas inferiores. Este proceso es totalmente transparente para las entidades de la capa N.

"CAPAS HOMÓLOGAS de NIVEL N" | IES siglo 21: elaboración propia

Lamentablemente no existe uniformidad en cuanto a la cantidad de capas, los nombres de las mismas e inclusive la funcionalidad de cada capa en distintos modelos de red; sin embargo, en todos los casos las capas existen para cumplir con lo presentado en los apartados anteriores: brindar servicios a las capas superiores, de tal forma que las capas superiores no deban ocuparse de lo que ocurre "debajo de ellas".

Es hora de que comencemos a ser más precisos.

Si bien es muy habitual utilizar frases como las anteriores donde decimos: "*las capas inferiores brindan servicios a las capas superiores*" hay que tener en cuenta que las capas en sí no hacen nada. Las que sí hacen cosas, y tienen funciones son las entidades que residen en las capas. Una entidad puede ser un elemento de software, de hardware o firmware; eso depende del caso, pero debe quedar claro que quienes llevan adelante las tareas son las entidades, y éstas "residen" en las capas. La frase a la que hacíamos alusión debería leerse, entonces, como "*las entidades de las capas inferiores brindan servicios a las entidades de las capas superiores*". Es muy posible que sigamos utilizando frases como la original, en pos de ganar en facilidad de comprensión.

Volviendo a la frase de la que hablábamos, ya debemos saber de memoria que "*las entidades de las capas inferiores brindan servicios a las de las capas superiores*", pero ¿de qué servicios estamos hablando?

En general podemos decir que las entidades brindan servicios a través del uso de funciones, las cuales están estandarizadas en los protocolos.

Existen algunas funciones que son comunes a la mayoría de los modelos de redes de comunicación; es más, muchas de ellas se repiten en protocolos de capas distintas. Veamos de qué se trata con un ejemplo introductorio.

## Ejemplo sobre las funciones de los protocolos de comunicación



Interactiva "Ejemplo sobre las funciones de los protocolos de comunicación"

Vamos a suponer una pila de protocolos sencilla e irreal, una formada por 4 capas, como la indicada en la imagen.

Supongamos que está chateando con otra persona a través de una red cualquiera (pensemos en chateo por medio del teclado, no de voz; eso facilitará el ejemplo). Recordemos que la finalidad del chat por intermedio del teclado es que mientras Ud. escribe en su programa de chat, la otra persona recibe el texto y lo ve en una ventana de su propio programa, en su computadora; de esta forma es posible establecer una comunicación casi oral e interactiva con la otra persona.

Muy bien, supongamos que escribe en su aplicación: Hola.

Dado que el usuario interactúa directamente con la aplicación, es muy habitual denominar a la capa más alta de las pilas de protocolos simplemente Capa de Aplicación y, como la capa más baja siempre se encuentra en contacto con el medio físico de transporte (por ejemplo el cable de red), se la suele denominar Capa Física.

Muy bien, escribió "Hola" y quiere que la otra persona reciba estas palabras y las vea en su monitor. Seguramente la aplicación de chat que utiliza capture el código ASCII de los caracteres de la palabra Hola y los "traduzca a bits". Nosotros obviaremos esta traducción, pero debe tener en cuenta que donde pongamos Hola, en realidad deberían ir los bits correspondientes.

Los bits de palabra Hola constituyen lo que se suele denominar Datos del Usuario.

La figura que se presenta le ayudará a orientarse a lo largo del ejemplo.

Seguramente hay un protocolo de comunicación en el nivel de la capa de aplicación que indica si los caracteres remitidos están en código ASCII (acrónimo inglés de American Standard Code for Information Interchange – Código Estándar Estadounidense para el Intercambio de Información) u otro, y que, por ejemplo, esta información debe ir al inicio de los datos, en lo que se denomina cabecera. A esta función podríamos llamarla Presentación, ya que define cual es el formato que tendrán los datos a transmitir (Podrían ser de codificación ASCII u alguna otra codificación, por ejemplo EBCDIC (Extended Binary Coded Decimal Interchange Code))

La capa de aplicación conforma, entonces, el mensaje de la siguiente forma, de acuerdo al Protocolo de la Capa de Aplicación: (no se olvide que en realidad Hola estará traducida a Bytes y que para indicar que el código es ASCII seguramente se utilizará una cadena de bits previamente establecida).

La Capa de Aplicación quiere remitir este mensaje a su capa homóloga en el receptor, pero en realidad la enviará a la de abajo.  
¿Pero, por qué? Porque antes de enviar este mensaje hacen falta definir algunas cuestiones mas.

Una de las funciones típicas de los protocolos de comunicaciones es la que se denomina Envío Ordenado. Esta función debe garantizar que los mensajes se entregan al receptor en el orden en que los remitió el emisor; esto se debe a que existen formas de transmisión en las cuales los mensajes pueden llegar fuera de orden porque los mismos pueden seguir caminos distintos dentro de la red (un caso típico es Internet). Obviamente que en el caso del chat, es fundamental contar con un servicio de Envío Ordenado (no tendría sentido que el receptor recibiera la siguiente frase: "estás como, Hola").

Supongamos que la Capa 3 de nuestro modelo tiene una entidad que ofrece a las entidades de la Capa de Aplicación (como el programa de chat), el servicio de Envío Ordenado. Es muy probable que el diseñador del software de chat decida utilizar este servicio. Por lo tanto, la entidad de la capa de Aplicación (el programa de chat) solicita a la entidad de la Etapa 3 que le provea dicho servicio.

La entidad encargada del Envío Ordenado de la Capa 3 puede proceder de muchas formas para garantizar el envío ordenado; simplificando, digamos que el protocolo establece que simplemente agregue un encabezado donde simplemente conste el número de orden del mensaje. En este caso agregaría el número 1 (por supuesto, que en bits), ya que Hola es el primer mensaje enviado.

Un servicio que podría ofrecer alguna entidad de la Capa 2 a las de la Capa 3 podría ser algún tipo de Control de Errores; otra función típica de los protocolos de comunicaciones.

Como la entidad de la Capa 3 pretende que el mensaje llegue sin errores al receptor, solicita dicho servicio a la entidad que lo proporciona en la Capa 2.

Una forma sencilla de implementar un Control de Error es utilizar alguna forma de suma de verificación. Diremos que en forma simplificada se realiza la suma de todos los bits que recibe la entidad, obteniendo un valor (luego cuando la capa 2 del receptor reciba el mensaje realizará nuevamente el cálculo y lo comparará con éste; si no coinciden supondrá que se ha producido un error en la transmisión y solicitará que le envíen de nuevo el mensaje). Supongamos que el protocolo establece que dicho valor se debe agregar como un encabezado. Supongamos que en este ejemplo dicha suma de verificación da por resultado el número 342 (no realizamos los cálculos, así que no los verifique, es sólo a modo de ejemplo).

Una vez hecho esto, todavía falta algo muy importante: indicar a quién va dirigido el mensaje y cómo se debe hacer para entregarlo. Esta función suele denominarse Direccionamiento y es típica de los protocolos de comunicaciones. Supongamos que el protocolo de direccionamiento posee alguna forma de identificar a los usuarios de la red, y que establece que dicha dirección debe agregarse en la cabecera del mensaje. Para nuestro ejemplo bastará con que pongamos el nombre del destinatario, que como en la figura es una mujer supondremos que se llama Ana (por supuesto, que esta dirección irá "traducida" a bits).

El mensaje viajará de esta forma a través del medio que conforme la red (por ejemplo, algún tipo de cableado o vía infrarrojo), hasta que de alguna forma la capa física de la computadora de Ana reciba el mensaje.

La figura que verá le ayudará a entender qué ocurre luego.

La capa física, inspeccionará el encabezado (ya que el protocolo que comparte con la capa física del emisor le indica que allí se encuentra la dirección de destino), verá que la dirección es la propia, quitará el encabezado que dice Ana (ya que sólo es de utilidad para la entidad de la Capa Física) y enviará "lo que queda" a la Capa 3.

La entidad de la Capa 3, que es la que se encarga del Control de Errores, lee el encabezado, que dice 342 y procede según le indica su protocolo, que -como habíamos anticipado- le indica que debe realizar la suma de todos los demás elementos y compararla con 342. Si el resultado es 342, quitará el encabezado y enviará "lo que queda" hacia la Capa 2. Si el resultado no fuera 342, el protocolo seguramente le indicaría que envíe un mensaje al emisor solicitando el reenvío del mensaje.

La entidad de la Capa 2, la que se encargaba del envío Ordenado, lee el encabezado, que en este caso dice 1, y el protocolo le indicará cómo proceder, seguramente podría decirle que compare con otros mensajes que pudiera haber recibido antes y los ordene.

Finalmente, la entidad de la Capa 2 quita su encabezado y envía "lo que queda" a la Capa de Aplicación, la cual lee el encabezado y reconoce que el mensaje está en Código ASCII; la aplicación transformará esta información en caracteres y la presentará en una ventana en la interfaz gráfica del Ana.

El ejemplo anterior nos ha servido para introducir algunos elementos comunes a la mayoría de las pilas de protocolos:

IES siglo 21: Elaboración propia

El ejemplo anterior nos ha servido para introducir algunos elementos comunes a la mayoría de las pilas de protocolos

Es muy habitual que los Datos del Usuario fluyan hacia abajo en la pila de protocolos, estratificados por capas de la misma forma que se mostró en el ejemplo, es decir, la entidad que actúa en cada capa agrega algo de información, cuyo destinatario es la entidad correspondiente en la capa homóloga del receptor en forma de encabezado y, en algunos casos, también en forma de cola. El protocolo de dicha capa indicará qué información debe utilizarse, en qué forma debe agregarse y cómo debe ser interpretada por la entidad homóloga en el destinatario. También es muy habitual el tratamiento que se da a los datos en el lado del receptor, al subir por las capas se van quitando los encabezados y en algunos casos también la cola de los mensajes, ya que la información contenida en ellos tiene por destinatario una entidad específica en una capa y,

por ende, esa información no debe trascender hacia las superiores.

En este ejemplo hemos introducido algunas funciones típicas de los protocolos, como la **Presentación**, el **Envío Ordenado**, el **Control de Errores** y el **Direccionamiento**. Es importante destacar que hay muchas más funciones típicas y que cada una de ellas puede ser implementada en más de una capa. Por ejemplo, es típico que el Control de Errores forme parte del *firmware* (*software* grabado directamente en los chips) incorporado en las placas de red (es decir, en las capas más bajas de la pila); pero, en general, las pilas de protocolos incorporan funciones de Control de Errores también en las capas superiores. Lo mismo ocurre con otras funciones. Un listado que incluye otras funciones típicas de los protocolos es el siguiente:

Funciones Típicas de los Protocolos
Segmentación y reensamblado
Encapsulado
Control de Conexión
Envío Ordenado
Control de Flujo
Control de Errores
Direccionamiento
Multiplexación
Servicio de Transporte

"Otras funciones típicas de los protocolos" | Elaboración DEPROE, IES siglo21

Cada una de ellas se verá específicamente cuando analicemos con más profundidad los modelos reales.

Nosotros nos ocuparemos fundamentalmente de dos modelos:

- El modelo OSI (*Open System Interconnection–Interconexión de Sistemas Abiertos*) de ISO y,
- El modelo TCP/IP, o mejor dicho, la Pila o *Suite* de Protocolos de Internet.

Nos orientaremos a ellos por razones bien distintas: OSI por su importante valor académico, aunque no se haya masificado su uso y TCP/IP, por ser el modelo que siendo masivo, ha permitido la implementación de Internet, aunque haya presentado ciertas falencias a nivel de modelo académico. Dado que TCP/IP es un protocolo que sirve para establecer redes locales y es el protocolo de Internet, todo parece indicar que la estrella en los próximos años seguirá siendo el modelo TCP/IP.

## El Modelo de Referencia OSI

Cuántas veces nos hemos hecho la pregunta ¿QUÉ ES UNA RED?, y no siempre tuvimos una respuesta del todo acertada. No se preocupe, existen muchas respuestas a esta pregunta. Por ello nosotros tomaremos la siguiente definición:

*Se llama red a todo sistema de comunicación que soporta múltiples usuarios.*

Como vemos, es una definición muy amplia y tomará un significado diferente dependiendo del ambiente en el que se la ubique.

Una red, en general, consiste en **dos componentes**:

- **Los elementos de conmutación**, que son ordenadores especializados para conectar dos o más líneas de transmisión (*Hub, Switch, Router, etc.*).
- **La línea de transmisión** (circuitos, canales, etc.).

A su vez, en términos generales, tenemos dos *tipos de canales*:

- **Punto a punto.** En este caso el mensaje va de un extremo a otro íntegramente. Estas redes son conocidas como Punto a Punto, Almacenamiento y reenvío, conmutación de paquetes, etc. Cada cable conecta un *host* o dispositivo de conmutación (a veces se lo llama IMP (*Interchange Message Processor*)). El mensaje va de uno a otro *Host* íntegramente. Estas redes pueden ser Punto a Punto, Almacenamiento y Envío, Conmutación por Paquetes, etc.
- **De difusión.** Estas redes tienen un solo canal compartido por todos los *Host*. Los mensajes de una máquina se envían al canal y son recibidos por todas las demás. Aquélla a la cual va dirigida es la que lo leerá. Las redes locales en general son las que usan los canales de difusión.

Una red debe brindar servicios a varios usuarios, pero no necesariamente al mismo tiempo. Por ejemplo, considerando la red telefónica, cuyos usuarios son todos aquellos que tengan un teléfono, no es utilizada por todos al mismo tiempo.

Tenemos que entender que al definir una red estamos definiendo algo más que una terminal conectada a distancia con un sistema de computación central; por lo tanto, habrá más cuestiones por resolver.

Estas cuestiones pueden ser tales como:

- ¿Se permitirá que un usuario se comunique con varios al mismo tiempo?
- ¿Qué sucederá si varios usuarios tratan de usar la red al mismo tiempo?
- ¿Cómo manejarán la red la detección de ruidos y errores de transmisión?
- ¿Cómo se manejará las fallas de vínculos de interconexión? ¿Solo se dejará fuera de servicio una parte, o toda la red se verá afectada?
- ¿Cómo se asegurara que los mensajes lleguen a destino sin demora excesiva debido a la operación de la red?

Afortunadamente existen diferentes elementos de software y hardware para administrar las redes, quedando a nuestro criterio seleccionar la solución que mejor se adapte a nuestras necesidades.

Sin embargo, para contestar las preguntas formuladas más arriba, es imprescindible analizar en forma técnica algunos **aspectos de la red**, como ser:

- **TOPOLOGÍA**: determina la interconexión entre los usuarios.
- **PROTOCOLO**: sincrónico o asincrónico, formato de los mensajes, etc.
- **INTERFACES ELÉCTRICAS**: RS232, RS422, V.35, V.24/V.28, etc.
- **VÍNCULOS SELECCIONADOS**: este elemento condiciona la velocidad, distancia, confiabilidad, seguridad, facilidad de incorporar nuevos usuarios. Entre otros, podemos mencionar: par telefónico, cable coaxil, radioenlaces (VHF, UHF, Microondas), enlaces satelitales, fibras ópticas, etc.
- **PROCEDIMIENTOS DE RECUPERACIÓN**: procedimientos para el manejo de problemas, tales como errores, ruido, etc.

Dada una red, debe poder integrar equipos de múltiples proveedores, y con el fin de evitar situaciones confusas, la International Standard Organization (ISO) definió un modelo de red por niveles o capas.

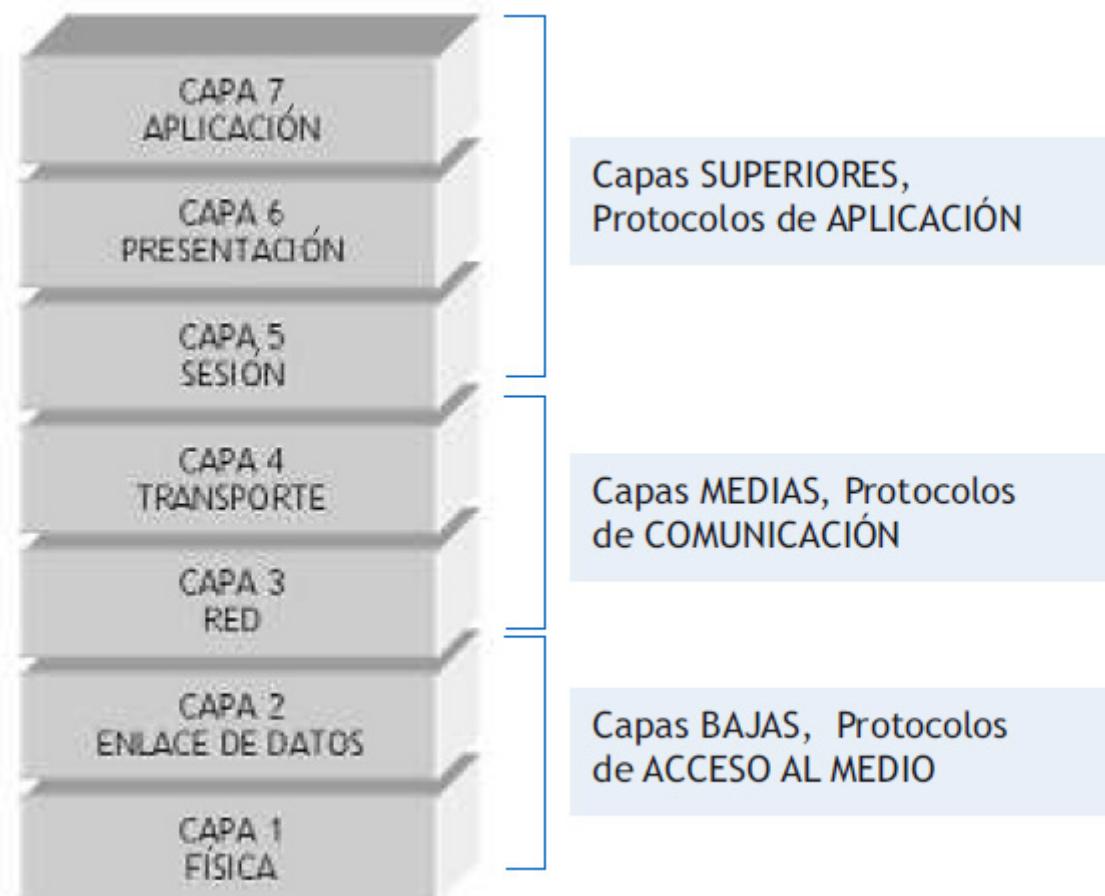
Este se conoce como el **modelo de referencia OSI (Open System Interconnection)**, o Interconexión de Sistemas Abiertos (ISA).

En una red existe una colección de máquinas destinadas a ejecutar programas de usuario. Utilizamos el término *HOST* para hacer referencia a computadoras conectadas en red, que proveen y utilizan servicios de ella.

El trabajo de la red consiste en enviar mensajes (comunicación o diálogo) entre *HOST*.

El diseño se simplifica si separamos los aspectos de comunicación de los de aplicación.

Es importante destacar que OSI es un Modelo de Referencia, y tiene un alto valor académico; sin embargo, no existe como una arquitectura de red.



"Modelo de Referencia" | IES siglo 21: elaboración propia

Usando un lenguaje más llano, el Modelo de Referencia define qué es lo que debe hacer cada capa, pero no siempre especifica los protocolos y servicios exactos que deben llevar a cabo dichas tareas, es decir, cómo deben hacerse. La ISO ha elaborado estándares para algunos protocolos, pero los mismos no han tenido gran trascendencia en el mercado.

En el otro extremo, se encuentra el Modelo TCP/IP, que a diferencia de OSI, es más bien "escaso" en cuanto a las definiciones de las capas, pero cuenta con una gran cantidad de protocolos muy desarrollados, plenamente operacionales y de gran uso en la industria actual, a tal punto que es el modelo que se utiliza en Internet.

Resumiendo, podemos decir que la tendencia actual es la de utilizar el Modelo de Referencia OSI como estructura conceptual y usarlo como una "*regla*" para comparar otros modelos o simples pilas de protocolos.

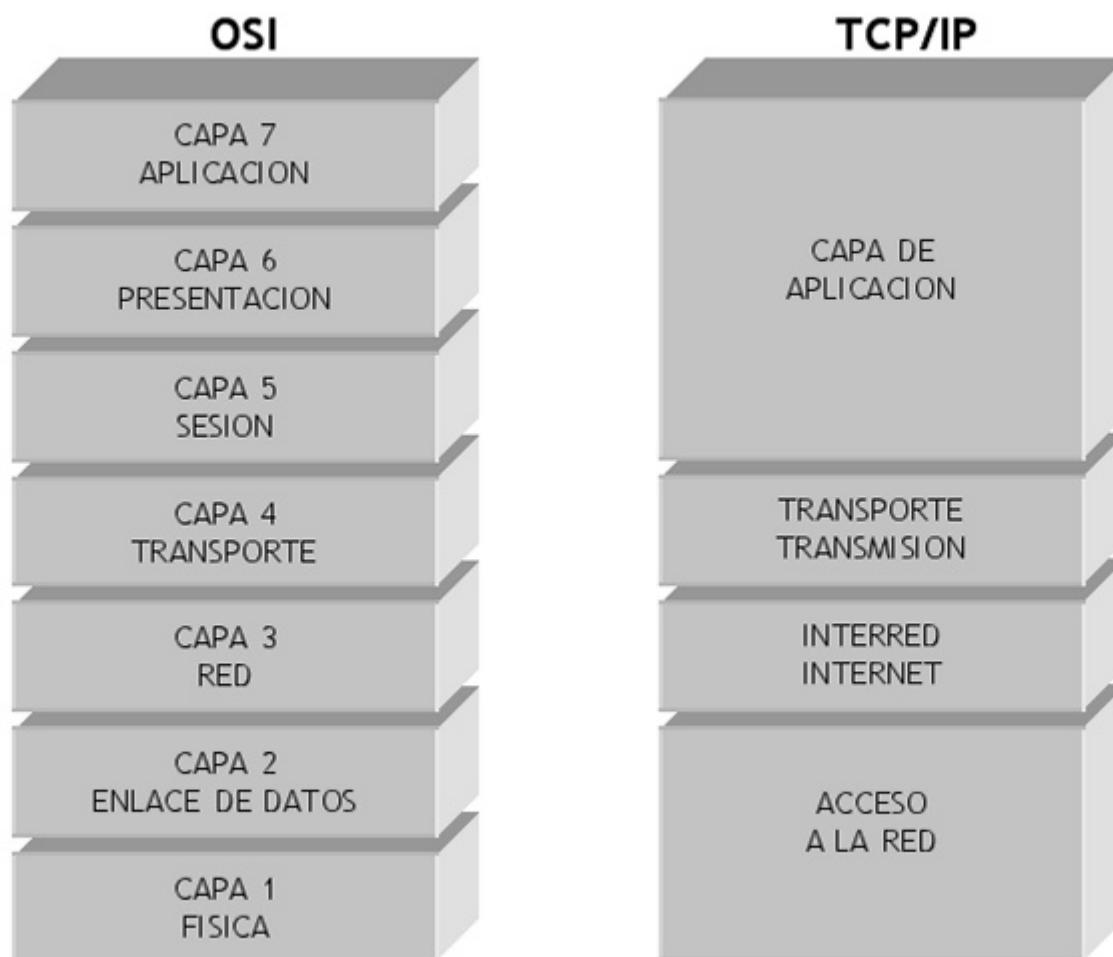
A diferencia del sencillo modelo presentado anteriormente a modo de ejemplo, OSI cuenta con 7 capas:

Para facilitar el análisis, es preferible considerar a las 7 capas de OSI agrupadas en "Capas Superiores", "Capas Medias" y "Capas Inferiores" como se muestra en la siguiente figura.

Antes de comentar las funciones encomendadas a cada capa por la gente de la ISO, comparemos el Modelo de referencia OSI con el modelo TCP/IP.

El Modelo TCP/IP consta de menos capas que el OSI, sólo tiene 4. Esto no significa que TCP/IP tenga que realizar menos funciones, sino que varias de estas funciones no se encuentran discriminadas en capas distintas. La equivalencia entre ambos modelos se muestra en la siguiente figura:

## Comparación de los modelos OSI y TCP/IP



"Comparación de los modelos OSI y TCP/IP" | IES siglo21 elaboración propia

Como se puede observar, las diferencias fundamentales se producen en las capas superiores, y de acceso a la red o capa de acceso al medio ya, que en el modelo TCP/IP las 3 capas superiores de OSI se encuentran englobadas en una única capa, y sobre las 2 capas inferiores, TCP/IP no revela detalles, dejando a los protocolos ya estandarizados la función de presentar el acceso al medio. Como mencionamos anteriormente, esto no significa que en TCP/IP no sean necesarias las funciones que OSI ha asignado a las capas de

Presentación y Sesión, sino que en el caso de TCP/IP, éstas deben formar parte de los protocolos implementados en la capa de aplicación, es decir, deben "formar parte del mismo paquete".

La otra diferencia fundamental se da en las capas inferiores, ya que TCP/IP no establece características para las capas que se encuentren debajo de la capa de Internet (Red); los diseñadores de TCP/IP confiaron plenamente en las soluciones que la industria había establecido, siempre que sean capaces de comunicarse con la capa Internet, y dado que éstas se apoyan fundamentalmente en OSI, es natural considerar que TCP/IP tiene las mismas capas bajas.

Sin entrar en detalles, simplemente comentaremos (por el momento) que las capas bajas de ambos modelos se encargan de las topologías de red, las placas de red, los cableados y la forma eléctrica en que se transmitirán los bits a través del medio.

Las capas medias establecen los Protocolos de Comunicación (por ejemplo TCP, IP, UDP, ARP, RARP, ICMP, RIP, IGRP, BGPI y otros, en el caso del modelo TCP/IP), que permitirán que la información llegue a la computadora destino, sin importar dónde se encuentre físicamente. Son los protocolos que permiten que Ud., por ejemplo, pueda comunicarse desde su casa con una computadora en otro país utilizando Internet.

En las capas altas encontramos los protocolos de aplicación, que en caso de TCP/IP suelen ser: HTTP, FTP, SMTP, Telnet y otros. Los nombres pueden parecer extraños, pero seguramente ya se ha acostumbrado a alguno de ellos: cuando navega por Internet (o por la intranet de su empresa) con el *Internet Explorer* o el *Netscape Navigator* está utilizando el protocolo HTTP (Hyper Text Transfer Protocol o Protocolo de transferencia de Hipertexto) que es el que permite que vea las páginas Web. El protocolo HTTP especifica cómo debe hacer su navegador para mostrar en pantalla los Bytes enviados desde el sitio web.

¿Ha usado el correo electrónico (e-mail)? ¿Sí? Entonces, ha estado utilizando el protocolo SMTP (*Single Mail Transfer Protocol*, o Protocolo Simple de Transferencia de Correo); este protocolo es el que le permite a su programa cliente de correo electrónico (como puede ser el *Outlook*, *Outlook Express*, *Eudora mail*, *Pegasus* o *Lotus Notes*, entre otros) mostrarle los mails que recibió, qué poner en cada uno de los campos que utiliza habitualmente como la dirección de correo electrónico de destino, el subject (o asunto), el campo CC etc.

En la herramienta siguiente estudiaremos con algo más de detalle las distintas capas del modelo OSI, empezando por las capas bajas. En esta Situación Profesional investigaremos las capas bajas; en las Situaciones Profesionales posteriores nos abocaremos al estudio de las restantes.

## Cuestiones a resolver en el diseño por Capas

Vamos a mencionar algunas de las cuestiones más importantes que deberán ser definidas en el Modelo OSI:

- Cada capa debe tener un mecanismo para el establecimiento de la conexión. Se necesita un medio que permita especificar con quién establecer la conexión. Al tener destinatarios múltiples, se necesita alguna forma de direccionamiento.
- Un mecanismo para finalizar una conexión dentro de la red, una vez que ésta no se necesita. Este punto que parece trivial suele ser bastante complejo.
- Regla para la transferencia de datos:

1. Comunicación unilateral o simplex.
2. Comunicación bilateral o semidúplex.
3. Comunicación bilateral simultánea o dúplex.
  - Número de canales lógicos que corresponden a la conexión.

- Procedimientos para la corrección de errores.
- El receptor debe tener alguna forma de indicar qué mensajes ha recibido, y cuáles de ellos son correctos.
- Incapacidad de aceptar mensajes extensos. Esto nos conduce a la segmentación, transmisión y ensamblaje.



¿Estás listo para un desafío?

**1. Indique la opción correcta**

Los modelos multicapa son planteados para poder "dividir" el problema de las comunicaciones en partes. Cada capa se encarga de ofrecer diversos servicios a las capas superiores, permitiendo que éstas no "deban preocuparse" por estos servicios. De esta forma, los diseñadores de software y hardware pueden trabajar en forma especializada resolviendo los problemas específicos de una sola capa.

- Verdadero
- Falso

**2. Indique la opción correcta**

Las funciones son exclusivas de cada capa del modelo de red; es imposible, por lo tanto, que en dos capas distintas se realice la misma función.

- Verdadero
- Falso

**3. Indique la opción correcta**

¿Quiénes realizan las funciones determinadas de una capa?

- Los usuarios.
- Los administradores de red.
- Las entidades que residen en cada capa.
- El sistema operativo de cada computadora.

**4. Indique la opción correcta**

A medida que la trama recibida por el receptor va ascendiendo a través de las capas, ¿qué acción básica se lleva a cabo antes de transferirla a la capa superior?

- Se agregan encabezados y en algún caso también una cola (trailer); si todo está bien se remiten a la capa superior.
- Se quitan los encabezados (y posibles colas); si todo está en orden se remite a la capa inferior.
- Se agregan encabezados (y posibles colas); si todo está en orden se remite a la capa superior.

- Se interpretan los encabezados (y posibles colas); si todo está en orden se quitan y se remite a la capa superior.

**5. Indique la opción correcta**

Una de las funciones típicas de los protocolos de red, que verifica que los bits recibidos coincidan con los enviados, es llamada:

- Envío ordenado.
- Control de errores.
- Control de flujo.
- Direccionamiento.

**6. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Entre dos capas homólogas se establece un	emisor
La trayectoria "real" de los bits es hacia abajo en el	protocolo de comunicación
La trayectoria "real" de los bits es hacia arriba en el	receptor

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Los modelos multicapa son planteados para poder "dividir" el problema de las comunicaciones en partes. Cada capa se encarga de ofrecer diversos servicios a las capas superiores, permitiendo que éstas no "deban preocuparse" por estos servicios. De esta forma, los diseñadores de software y hardware pueden trabajar en forma especializada resolviendo los problemas específicos de una sola capa.

- Verdadero
- Falso

## 2. Indique la opción correcta

Las funciones son exclusivas de cada capa del modelo de red; es imposible, por lo tanto, que en dos capas distintas se realice la misma función.

- Verdadero
- Falso

## 3. Indique la opción correcta

¿Quiénes realizan las funciones determinadas de una capa?

- Los usuarios.
- Los administradores de red.
- Las entidades que residen en cada capa.
- El sistema operativo de cada computadora.

## 4. Indique la opción correcta

A medida que la trama recibida por el receptor va ascendiendo a través de las capas, ¿qué acción básica se lleva a cabo antes de transferirla a la capa superior?

- Se agregan encabezados y en algún caso también una cola (trailer); si todo está bien se remiten a la capa superior.
- Se quitan los encabezados (y posibles colas); si todo está en orden se remite a la capa inferior.
- Se agregan encabezados (y posibles colas); si todo está en orden se remite a la capa superior.
- Se interpretan los encabezados (y posibles colas); si todo está en orden se quitan y se remite a la capa superior.

## 5. Indique la opción correcta

Una de las funciones típicas de los protocolos de red, que verifica que los bits recibidos coincidan con los enviados, es llamada:

- Envío ordenado.
- Control de errores.
- Control de flujo.
- Direccionamiento.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Entre dos capas homólogas se establece un  
La trayectoria "real" de los bits es hacia abajo en el  
La trayectoria "real" de los bits es hacia arriba en el

protocolo de comunicación  
emisor  
receptor

# SP3 / H2: Las capas de acceso al medio: física y enlace de datos

## La Capa Física

*"La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico en la red."*

El párrafo anterior parece un tanto difícil de entender. Sin embargo, lo escribimos de esa forma porque ésa suele ser la terminología técnica que se usa habitualmente.

Pero no debe preocuparse, porque ya sabe de qué se trata, lo que queremos decir es que:

La capa física define las características que debe tener el medio de transmisión (por ejemplo el cable), cuánto debe medir, con qué velocidad se puede transmitir por él, cada cuántos metros se deben regenerar la señal con un repetidor, cómo se representarán los 0 y 1 lógicos con niveles de tensión eléctrica o voltaje (¿recuerda la codificación Manchester?)

Esperamos que sí porque son detalles que ya hemos visto cuando analizamos los tipos de cableados definidos en la norma IEEE 802.3 y en la norma Ethernet.

La capa física también define cómo deben ser los conectores que vinculan el cable a la placa de red y los conectores que se utilizan para unir distintos segmentos de cable.

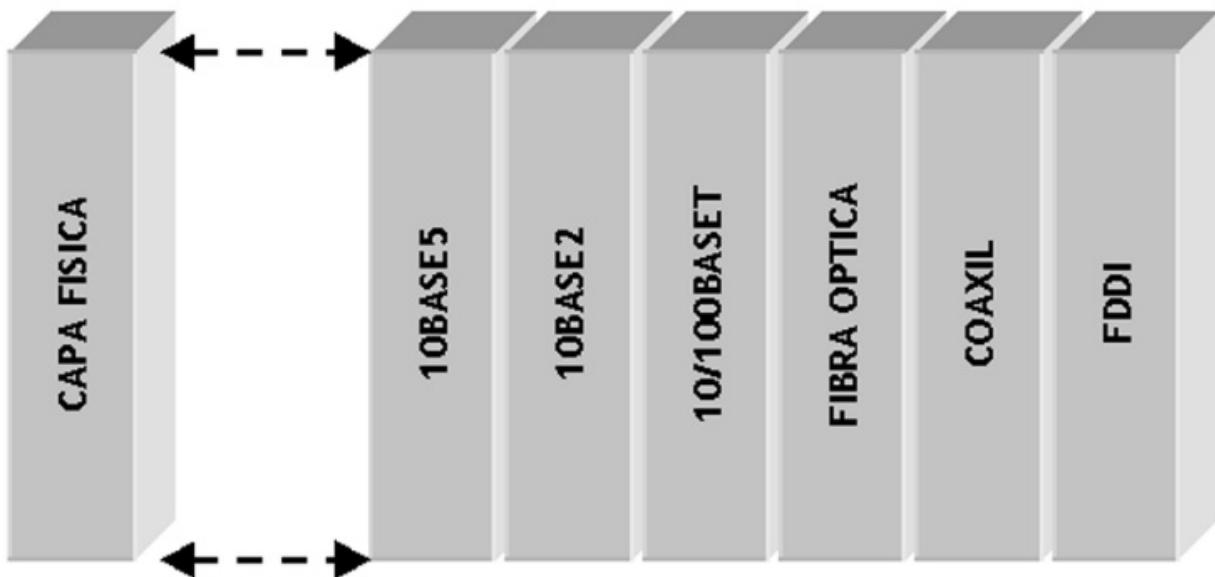
Podemos decir que el objetivo fundamental de la capa física es conseguir **que cuando la computadora emisora envíe un 1 lógico, la computadora receptora reciba un 1 lógico**.

¡Así que cuando le pedimos que defina un tipo de cable para una red LAN hipotética, lo que estamos haciendo es que elija las características de la capa física de su red LAN!

Además del cableado de red, también se encuentra involucrada en los servicios de la capa física y de enlace, la placa de red o NIC (Network Interface Card), ya que ella es la que genera los 1 y 0 lógicos como señales eléctricas, las cuales luego vuelca en el medio de transmisión.

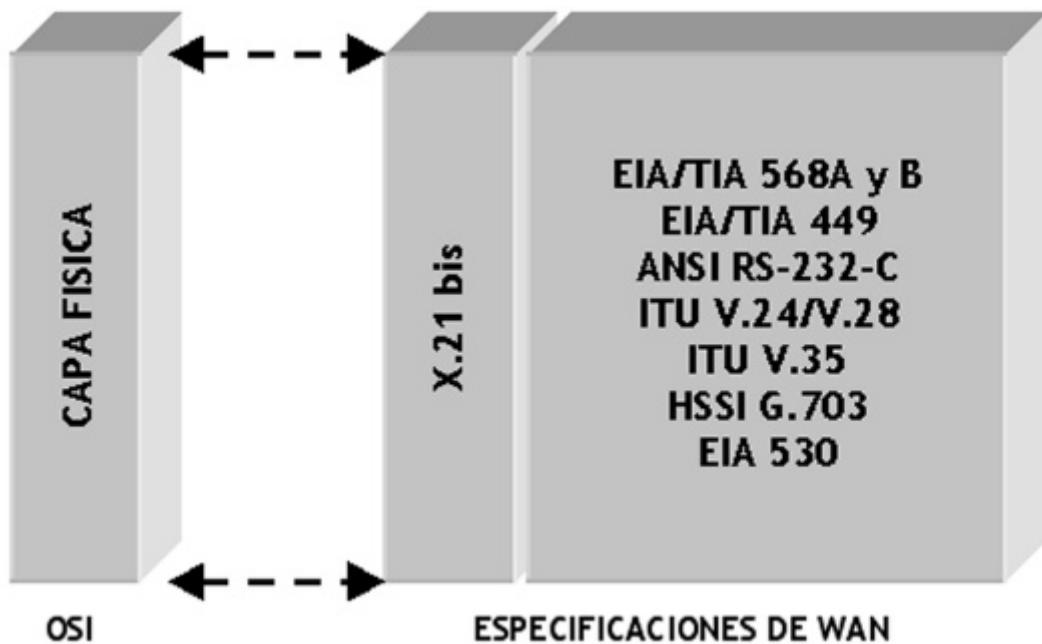
Como puede observar las normas Ethernet, IEEE 802.3, IEEE 802.4, IEEE 802.5 brindan los servicios exigidos por los modelos OSI y TCP/IP para la capa física de redes LAN.

La siguiente figura le muestra la relación que existe entre la capa física del modelo OSI (y también del TCP/IP) y algunas normas que lo implementan para redes LAN.



"Relación" | Elaboración DEPROE, IES siglo21

Hacemos especial hincapié en que las mostradas en la figura son las especificaciones para implementar redes LAN (de área local), ya que las mismas no son utilizables para redes WAN.



"Especificaciones normalizadas" | Elaboración DEPROE, IES siglo21

La figura anterior muestra algunas especificaciones normalizadas para la capa física en redes WAN.

## La Capa de Enlace e Datos

La definición de topología de red forma parte de la normativa de correspondiente a la Capa de Enlace de

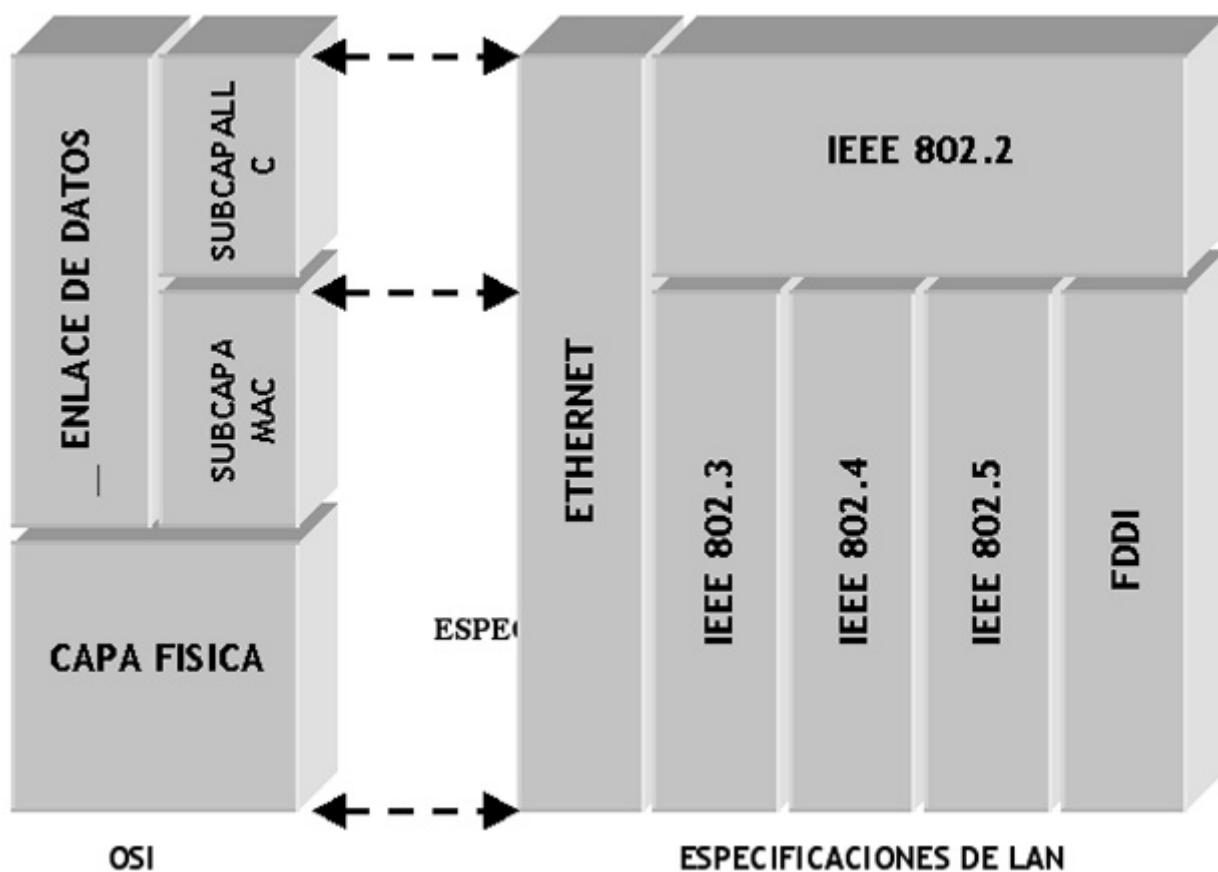
Datos.

En esta capa también se define cómo se establecerán las direcciones físicas de cada computadora (**direcciónamiento físico**), y cómo deberán ser las tramas de bits. También se define cómo se establece la secuencia de tramas enviadas (**secuenciamiento**) y, asimismo, controla cuándo una computadora puede enviar bits a otra sin saturarla (**control de flujo**).

**Lo más importante de esta capa es que especifica el Método de Acceso al Medio** (no nos olvidemos que todas las computadoras de la red usan el mismo medio o cable para comunicarse), como por ejemplo CSMA/CD o Token Ring. Esto lo veremos más en detalle cuando estudiemos Redes LAN.

Por último, también se encarga de detectar posibles errores en la transmisión (**control de errores**), aplicando por ejemplo algoritmos de suma de verificación (al estilo checksum, CRC, etc.).

La mayoría de las funciones mencionadas se implementan directamente sobre la placa de red, es decir, en lo que suele denominarse firmware (software grabado en circuitos integrados).



"Especificaciones de LAN" | Elaboración DEPROE, IES siglo21

En cuanto a las normas que cumplen estos requisitos para redes LAN, podemos decir que la norma *Ethernet* cubre por completo las capas física y de enlace, en tanto que las normas de la IEEE 802 han subdividido la capa de enlace en dos subcapas:

- LLC (Logic Link Control o Control de enlace Lógico) y

- MAC (*Media Access Control* o Control de Acceso al Medio), como se muestra en la figura anterior.

Como puede observarse, según la normativa de la IEEE, las Normas IEEE 802.3 y 802.5 cumplimentan la capa física y la subcapa MAC quedando a cargo de la Norma IEEE 802.2 la subcapa LLC.

Veremos más en detalle estas subcapas cuando estudiemos Redes LAN.

## Ejemplos de Capa de Enlace en Redes Públicas

Casi todos se derivan del protocolo de enlace usado en SNA, conocido como SDLC (*Synchronous Data Link Control*) de IBM.

ANSI lo modificó para generar el ADCCP (Advanced Data Control Communication Protocol), y la ISO generó el HDLC (*High Level Data Link Control*).

Posteriormente el CCITT modificó el HDLC para dar lugar al LAP (*Link Access Procedure*), como parte de la norma X.25, pero más tarde lo modificó creando el LAPB (*Link Access Procedure Balanced*), de manera de hacerlo más compatible con el HDLC.

Todos estos protocolos tienen algo en común: están orientados al bit, y utilizan inserción de bits (inserción de ceros) para la transparencia de datos.

Los protocolos orientados al bit utilizan la estructura de trama como la de la figura que, a continuación, se presenta.

## Trama HDLC de OSI



Interactiva "Trama HDLC de OSI"

El campo Dirección es fundamental en líneas multipunto.

El campo Control se utiliza para los números de secuencia, asentimientos etc.

Hay tres tipos de tramas, variando fundamentalmente el campo control:

- 1 Información
- 2 Supervisoras
- 3 Sin numerar

El campo Datos es la información del usuario, puede ser arbitrariamente largo, pero la eficiencia del CRC decrecerá a medida que el campo de datos aumente, debido a la posibilidad de tener errores de grupo.

El campo CRC (Código de Redundancia Cíclica).

Además se identifica el comienzo y fin de la trama con un campo Flag compuesto de la secuencia 01111110 (7E).

IES siglo 21: elaboración propia



¡Vamos a comprobar cuánto aprendiste!

**1. Indique la opción correcta**

La placa de red o NIC (Network Interface Card), interviene en la Capa Física y Capa de Enlace de Datos.

- Verdadero
- Falso

**2. Indique la opción correcta**

En la Capa de Enlace de Datos se define la topología de la red: la define el Método de Acceso al Medio.

- Verdadero
- Falso

**3. Indique la opción correcta**

¿En cuántas subcapas se divide la Capa de Enlace de Datos según IEEE 802?

- No se subdivide, define las características que debe tener el medio de transmisión.
- Se subdivide en dos: subcapas Control (LLC) y Control De Acceso al Medio (MAC).
- Se subdivide en tres: 802.2, Control (LLC), Control De Acceso al Medio (MAC).
- Se subdivide en tres: Información, Supervisora y Sin numerar.

**4. Indique la opción correcta**

Indique cuál de los siguientes campos NO compone una trama HDLC de OSI.

- Dirección.
- Control.
- Datos.
- HARP.

**5. Indique la opción correcta**

¿En qué capa del modelo OSI se definen las direcciones Físicas o de Hardware?

- Red.
- Transporte.

- o Enlace de Datos.
- o Aplicación.

## 6. Ordene relaciones

En la capa de enlace se definen:

Como se establecerán las direcciones físicas	CSMA/CD
Como se establece la secuencia de las tramas enviadas	Direccionamiento Físico
Cuando una computadora debe enviar bits a otro	Control de Flujo
El método de acceso al medio	Control de errores
Como se detectan posibles errores en la transmisión	Secuenciamiento

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

La placa de red o NIC (Network Interface Card), interviene en la Capa Física y Capa de Enlace de Datos.

Verdadero

Falso

## 2. Indique la opción correcta

En la Capa de Enlace de Datos se define la topología de la red: la define el Método de Acceso al Medio.

Verdadero

Falso

## 3. Indique la opción correcta

¿En cuántas subcapas se divide la Capa de Enlace de Datos según IEEE 802?

No se subdivide, define las características que debe tener el medio de transmisión.

Se subdivide en dos: subcapas Control (LLC) y Control De Acceso al Medio (MAC).

Se subdivide en tres: 802.2, Control (LLC), Control De Acceso al Medio (MAC).

Se subdivide en tres: Información, Supervisora y Sin numerar.

## 4. Indique la opción correcta

Indique cuál de los siguientes campos NO compone una trama HDLC de OSI.

Dirección.

Control.

Datos.

HARP.

## 5. Indique la opción correcta

¿En qué capa del modelo OSI se definen las direcciones Físicas o de Hardware?

Red.

Transporte.

Enlace de Datos.

Aplicación.

## 6. Ordene relaciones

En la capa de enlace se definen:

Como se establecerán las direcciones físicas

Direccionamiento Físico

Como se establece la secuencia de las tramas enviadas

Secuenciamiento

Cuando una computadora debe enviar bits a otro

Control de Flujo

El método de acceso al medio

CSMA/CD

Como se detectan posibles errores en la transmisión

Control de errores



# SP3 / H3: Las capas medias: Red y Transporte

## La Capa de Red (Network Layer)

Esta capa se ocupa del control de la operación de la red. Un punto muy importante en su diseño es la determinación de cómo encaminar los mensajes (o paquetes).

Las rutas podrían basarse en tablas estáticas previamente cableadas en la red, siendo cualquier cambio difícil de realizar. También pueden ser tablas estáticas que se establecen al inicio de cada diálogo.

Por último, pueden ser de tipos dinámicos, determinándose la ruta para cada paquete en el momento en que éste es emitido.

**El control de congestión, por lo tanto, también depende de la capa de red.**

A veces se coloca una función de contabilidad para realizar tareas de facturación.

La responsabilidad para resolver problemas de interconexión de redes heterogéneas recae en la capa de red.

En las redes de difusión, el encaminamiento es simple; por lo tanto, la capa de red es muy pequeña, o a veces no existe.

La capa de red proporciona servicios a la de transporte.

**La capa de red opera esencialmente en los Routers, mientras que la de transporte opera en los HOST;** los límites entre estas capas, es también el límite entre la red y el Host (usuario). Esto implica que los servicios de la capa de red definen los servicios ofrecidos por la propia red.

Cuando la red es operada por un proveedor de servicios portadores, y los Host son operados por los usuarios, el servicio de capa de red se convierte en la interfase entre el proveedor y los usuarios. Como tal, define las obligaciones y responsabilidades del proveedor y del usuario.

Los servicios de la capa de red se han diseñado con los siguientes objetivos:

- 1- Deben ser independientes de la tecnología de la red.
- 2- La capa de transporte debe tener oculto el número, tipo y topología de las redes que se encuentren presentes.
- 3- Las direcciones de red a disposición de la capa de transporte deben utilizar un plan de numeración uniforme, aun a través de redes LAN y WAN.

Hay quienes sostienen que la capa de red sólo debe mover los bits, y nada más. Desde este punto de vista, los Host deben aceptar que la red es poco fiable y llevar a cabo ellos mismos el control de errores y de flujo. Esto nos conduce a que el servicio de red debería ser **no orientado a conexión**.

Otro grupo sostiene (representado por las empresas telefónicas) que la capa de red debe proporcionar un servicio fiable, **orientado a conexión** con las siguientes propiedades:

- 1- Antes de transmitir datos, deberá establecerse la conexión entre las entidades de transporte origen y destino. Esta conexión se utilizará hasta que finalice la sesión.
- 2- Cuando se establezca una conexión, las entidades de transporte y de red negociarán los parámetros de calidad y costo del servicio.
- 3- La comunicación se establecerá en ambas direcciones, y los paquetes se entregará sin errores y en forma secuencial. El modelo conceptual se basa en la cola de espera normal, en donde el primero que entra es el

primero en salir.

4- El control de flujo se proporciona automáticamente para impedir que un emisor rápido inunde de paquetes a la cola de espera.

## Encaminamiento

La función real de la capa de red es la de **proveer encaminamiento o enrutamiento de paquetes desde el origen hasta el destino**. En muchas redes, los paquetes necesitan realizar muchos saltos para completar un viaje. La excepción la dan las redes de difusión (broadcast), pero aun aquí el encaminamiento es interesante cuando el origen y el destino no se encuentran en la misma red.

El algoritmo de encaminamiento es la parte del *software* correspondiente a la capa de red, que es responsable de decidir sobre por cuál línea de salida deberá transmitir un paquete que llega.

Cuando se utilizan datagramas, la decisión deberá tomarse con cada paquete que llegue, mientras que en el caso de circuitos virtuales, las decisiones de encaminamiento sólo se tomarán cuando se establezca un nuevo circuito virtual; después los paquetes seguirán la ruta establecida. A esto último se lo conoce como encaminamiento de sesión, ya que la ruta permanece durante toda la sesión.

## Algoritmos de Encaminamiento

Se pueden agrupar en dos clases principales: **no adaptativos y adaptativos**.

Los algoritmos **no adaptativos** no basan sus decisiones en mediciones o estimaciones del tráfico o topología actual, sino que la elección de la ruta para ir del nodo "i" al nodo "j" se determina anticipadamente, fuera de línea cuando la red se arranca. También se lo denomina *encaminamiento estático*.

Los algoritmos **adaptativos** intentan cambiar sus decisiones de encaminamiento para reflejar los cambios de topología y de tráfico actual.

Existen tres familias de algoritmos adaptativos, que se diferencian de acuerdo con la información que utilizan.

1- Los algoritmos globales utilizan información recogida en toda la red. A esto se lo conoce como encaminamiento centralizado.

2- Los algoritmos locales operan en forma separada sobre cada nodo, y sólo utilizan la información que se encuentra disponible allí, como por ejemplo, la longitud de las colas de espera. A éstos se los conoce como algoritmos aislados.

3- Por último, la tercera clase de algoritmos utiliza una combinación del tipo global y local, y se lo conoce como algoritmos distribuidos.

Tipos de encaminamiento					Interacción
Por el Camino más Corto	De Camino Múltiple	Centralizado	Aislado	Distribuido	

**Encaminamiento por el Camino más Corto**

La idea consiste en construir una gráfica de la red. Para escoger cada ruta el algoritmo sólo debe determinar el camino más corto existente entre ellos.

El concepto de camino más corto es una forma de medir la longitud del camino a través del número de saltos; para ello podemos utilizar varias formas de definirlo, según la métrica que se utilice. Por ejemplo, se puede tomar el camino geográfico, pero también podría etiquetar cada enlace con el retardo promedio de las colas de espera. Con esto, el camino más corto resulta ser el de menor retardo.

En general, las etiquetas podrían calcularse como una función de la distancia, ancho de banda, promedio de tráfico, costo de comunicación, retardo medio, etc. De esta manera, los algoritmos calcularán el camino más corto como una combinación de estos parámetros.

#### Interactiva "Tipos de encaminamiento"

- Encaminamiento por el Camino más Corto

La idea consiste en construir una gráfica de la red. Para escoger cada ruta el algoritmo sólo debe determinar el camino más corto existente entre ellos.

El concepto de camino más corto es una forma de medir la longitud del camino a través del número de saltos; para ello podemos utilizar varias formas de definirlo, según la métrica que se utilice. Por ejemplo, se puede tomar el camino geográfico, pero también podría etiquetar cada enlace con el retardo promedio de las colas de espera. Con esto, el camino más corto resulta ser el de menor retardo.

En general, las etiquetas podrían calcularse como una función de la distancia, ancho de banda, promedio de tráfico, costo de comunicación, retardo medio, etc. De esta manera, los algoritmos calcularán el camino más corto como una combinación de estos parámetros.

- Encaminamiento de Camino Múltiple

Es una variante del anterior, en donde no sólo se calcula el camino más corto, como única alternativa, sino entre varios nodos pueden utilizarse varios caminos igualmente buenos y, con frecuencia, es conveniente dividir el tráfico entre varios caminos. Esto se conoce como encaminamiento múltiple.

- Encaminamiento Centralizado

Los algoritmos vistos anteriormente, necesitan tener información acerca de la topología y el tráfico de la red para poder tomar las mejores decisiones. Si la topología es estática y el tráfico se mantiene más o menos constante, la construcción de las tablas de encaminamiento es sencilla, y se realiza una sola vez fuera de línea.

Sin embargo, si los nodos se desactivan y se restablecen, o, bien si el tráfico sufre variaciones muy grandes durante el día, se necesita de un mecanismo para actualizar las tablas.

Cuando se utiliza un algoritmo centralizado, en algún punto de la red hay un Centro de Control de Encaminamiento o de Red. Periódicamente, cada nodo transmite a este centro información sobre su estado, que al conocer el estado de toda la red puede tomar decisiones.

Esto parece atractivo a primera vista, pero también tiene sus serios problemas. Si la red tiene que adaptarse a tráfico muy variable, el cálculo del encaminamiento deberá efectuarse con demasiada frecuencia. Para una red grande, este cálculo tomará bastante tiempo. Otro problema insalvable se da si el centro de red se ve aislado o se desactiva por fallas propias o de las líneas de enlace.

- Encaminamiento Aislado

En este algoritmo, los nodos toman decisiones basados en la información que ellos mismos tienen. Estos algoritmos lo que hacen es, cuando llega el paquete, ponerlo inmediatamente en la cola de espera de salida más corta, sin tener en cuenta el lugar de dirección de esa línea.

Una variante de éste es el de combinarlo con el algoritmo centralizado; entonces, cada paquete que llegue se colocará en la salida cuyo peso estático y colas de espera sean menores.

Otra variante es la de utilizar el mejor peso estático, a menos que se supere un cierto umbral.

Otra variante es la del aprendizaje hacia atrás. Éste consiste en preguntarle a cada paquete que llega cuál es la situación de donde proviene. Para ello, deberá incluirse la identidad del nodo origen en cada paquete, junto a un contador que se incrementa con cada salto. Si un nodo ve llegar un paquete del nodo "B" por la línea "h" y su contador está en 5, sabrá que el nodo "B" no está más lejos de él que 5 saltos sobre esa línea.

De esta manera, puede estimar cuál es el mejor enlace entre I y el nodo "B".

- Encaminamiento Distribuido

En este algoritmo, cada nodo intercambia información con sus vecinos. Cada nodo mantiene una tabla de encaminamiento con una entrada por cada uno de los demás nodos vecinos. Esta entrada consta de dos partes: la línea preferida de salida que utilice para dicho destino, y alguna estimación del tiempo o distancia hacia él. La métrica utilizada podría ser el número de saltos, el retardo, los paquetes encolados, ancho de banda, etc.

Se supone que el nodo conoce la "distancia" a cada uno de sus vecinos, la que puede estar constituida por algunos o combinaciones de varios de los parámetros anteriores.

IES siglo 21: elaboración propia

## Congestión

Cuando existen muchos paquetes dentro de la red, el rendimiento se degrada. Esta situación se conoce como congestión.

## Algoritmos de Control de la congestión

Existen varias estrategias para el control de la congestión:

- 1- Que asignen recursos anticipados.
- 2- Que desechen paquetes, cuando no se pueden procesar.
- 3- Que se restrinja el número de paquetes en la red.
- 4- Utilizar el control de flujo para evitar la congestión.
- 5- Obstruir la entrada de datos, cuando la red está sobrecargada.

## Bloqueo

La máxima congestión es el bloqueo, también llamado estancamiento. En este caso, los nodos no pueden proseguir hasta tanto su vecino no realice una acción, el que a su vez espera de otro nodo, y éste del primero, creándose un círculo vicioso del cual no podrán salir produciéndose un bloqueo.

Si bien existen varios algoritmos que previenen el bloqueo, todos se basan en la asignación y el control de los

recursos de cada nodo, evitando la transmisión si no se asegura la continuidad del camino del paquete.

## Ejemplo de Capa de Red

Existen varios protocolos de Capa de Red; el modelo más adecuado como ejemplo es el de IP (*Internet Protocol*), utilizado como protocolo de red del modelo TCP/IP y que veremos con más detalles en próximas situaciones profesionales. Otro protocolo bastante común es X.25, utilizado en las redes de conmutación de paquetes (cajeros automáticos y algunos enlaces satelitales).

## Capa de Transporte (Transport Layer)

La función principal de la capa de transporte consiste en **aceptar los datos de la capa de sesión, dividirlos (si es necesario) en unidades más pequeñas, pasarlo a la capa de red y asegurar que todos los pedazos (segmentos) lleguen correctamente al otro extremo**. Además, debe aislar a la capa de sesión de los cambios de tecnología del Hardware.

La capa de transporte es el corazón de la jerarquía de protocolos. **Su tarea consiste en asegurar el transporte de datos desde la máquina FUENTE a la máquina DESTINO, independientemente de la red física en uso.**

Hay muchas aplicaciones que sólo necesitan un método fiable para transmitir un flujo de bits entre dos máquinas. Por ejemplo, en Linux los buses entre máquinas sólo necesitan un proceso de transporte de bits. Para realizar esta función, dichos buses no necesitan ningún servicio de sesión o presentación.

Hay muchas aplicaciones que no tienen capa de sesión y presentación.

Existe sólo un protocolo de transporte, anterior a OSI que está bien establecido y es el TCP.

El objetivo principal de la capa de transporte consiste en proporcionar un servicio a las entidades de la capa de sesión. Para alcanzar este objetivo utilizará los servicios de la capa de red. Al Hardware y Software que hacen este trabajo se los conoce como "*entidades de transporte*".

Así como hay dos tipos de servicios de red, también existen dos tipos de servicios de transporte, es decir orientado a conexión y sin conexión (por ejemplo TCP), o no orientado a conexión (UDP).

El servicio de transporte orientado a conexión es similar al servicio de red orientado a conexión. En ambos casos, las conexiones tienen tres fases:

- la de establecimiento,
- la de transferencia de datos,
- la de liberación.

Los procedimientos de direccionamiento y control de flujo son similares en ambas capas.

El servicio de transporte sin conexión es similar al de red sin conexión.

Por supuesto, surgen las preguntas obvias:

*¿Si el servicio de transporte es tan similar al de red, cuál es la razón de tener dos capas diferentes?, ¿por qué razón una sola capa es inadecuada?*

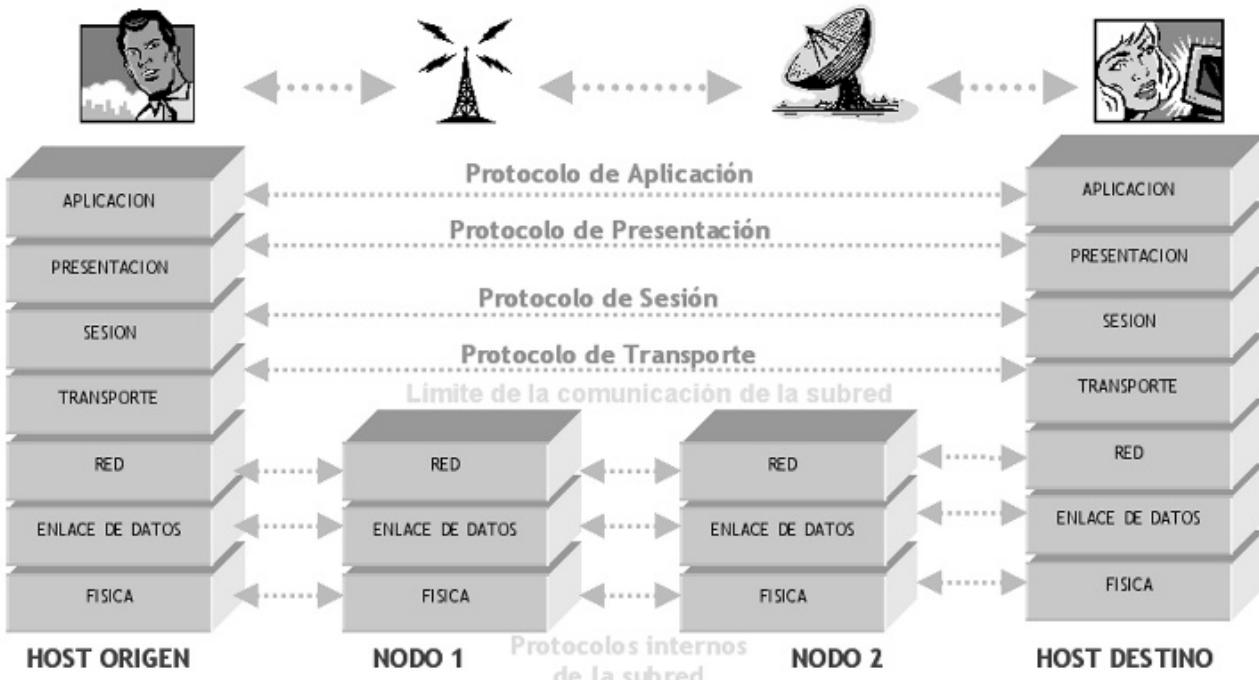
La respuesta es delicada, pero crucial y nos lleva a la siguiente figura del modelo de comunicaciones.

Si trasladamos esto al modelo OSI, podemos ver que las tres capas inferiores se comunican entre adyacentes, o sea del host emisor (origen) al nodo de comunicaciones más cercano, donde están conectadas, desde este nodo al siguiente (puede haber varios en el camino de los mensajes) y de este último, al host receptor (destino),

mientras que desde la capa de Transporte hacia arriba, todas las demás tienen comunicación extremo a extremo.

En esta figura podemos ver que la capa de red es parte de la subred de comunicaciones y es operada por el operador del servicio (al menos, para las redes WAN).

¿Qué pasaría si la capa de red ofreciera un servicio orientado a conexión, pero inseguro?



Supongamos que se perdiessen paquetes frecuentemente.

Como los usuarios no ejercen control sobre la subred, no pueden resolver el problema relacionado con un servicio deficiente, ya que no pueden cambiar los equipos en los nodos (routers o switchs) o incrementando el tratamiento de errores en la capa de enlace.

La única posibilidad, entonces, es la de colocar una capa por encima de la de red que mejore la calidad del servicio.

Si a una entidad de transporte se le avisa, a la mitad de una larga transmisión, que se ha interrumpido su conexión de red sin indicación respecto de los datos en tráfico, ella puede establecer una nueva conexión.

Utilizando esta nueva conexión, la entidad de transporte puede preguntar a su corresponsal qué datos llegaron y cuáles no, y reiniciar la transmisión a partir de allí.

Básicamente, podemos decir que la existencia de la capa de transporte hace más confiable el servicio que el proporcionado por la capa de red, dado que la capa de Transporte realiza un control de extremo a extremo (end-to-end).

Gracias a la capa de transporte, es posible que los programas de aplicación puedan escribirse usando un conjunto de primitivas y hacer que funcionen en una gran variedad de redes, sin preocuparse de tratar con diferentes interfaces de cada red.

Podemos dividir el modelo OSI en dos partes:

- De la capa 1 a la 4 serán proveedoras de servicio de transporte.
- De la capa 5 a la 7 serán usuarios del servicio de transporte.

Esta diferencia entre proveedor y usuario tiene un impacto considerable sobre el diseño de las capas y coloca a la capa de transporte en una posición clave, ya que constituye la frontera entre proveedor y usuario de un servicio de transmisión de datos seguro.

Otra forma de ver la capa de transporte es la de considerar que su función es la de enriquecer la QOS (Quality Of Service) o Calidad de Servicio suministrada por la capa de red.

Si el servicio de red es muy bueno, la capa de transporte puede tener un trabajo muy sencillo.

En otras palabras, la capa de transporte está para contribuir y llenar huecos entre lo que los usuarios desean y lo que el servicio de red ofrece.

Bajo condiciones normales, la capa de transporte crea una conexión de red distinta para cada conexión de transporte solicitada por la capa de sesión.

Si el transporte necesita un gran caudal, esta capa podría crear múltiples conexiones de red, dividendo los datos entre las conexiones de red.

La capa de transporte determina qué tipos de servicio le brindará a la capa de sesión, y en definitiva a los usuarios.

La capa de transporte es una capa del tipo "*origen-destino*" o "*extremo a extremo*". Es decir, un programa en la máquina origen establece un diálogo con uno similar en la máquina destino, usando las cabeceras de los paquetes y mensajes de control.

Los protocolos de la capa de red son entre máquinas inmediatas o vecinas y no entre origen y destino, las cuales podrían estar separadas por varios nodos.

En la figura anterior puede observarse la diferencia entre las capas 1 a 3 que están encadenadas, y las capas 4 a 7 que son extremo a extremo.

Es normal que se tengan múltiples conexiones, por lo que se necesitará alguna forma de decir qué mensajes pertenecen a qué conexión. La cabecera de transporte es un lugar donde se puede colocar esta información.



¿Te animás a medir cuánto aprendiste?

**1. Indique la opción correcta**

La capa de Transporte realiza un control de extremo a extremo.

- Verdadero
- Falso

**2. Indique la opción correcta**

Un punto muy importante en el diseño de la capa de red es la determinación de como encaminar los paquetes.

- Verdadero
- Falso

**3. Indique la opción correcta**

Según el modelo OSI, la función de la Capa de Red se ocupa de:

- Definir las características que debe tener el medio de transmisión.
- Definir como se establecerán las direcciones físicas de cada computadora y como deberán ser las tramas de bits.
- El control de la operación de la red y el enrutamiento de los paquetes.
- Asegurar que todos los segmentos lleguen correctamente al otro extremo.

**4. Indique la opción correcta**

En la capa de red, las rutas pueden determinarse de dos formas:

- Punto a punto o difusión.
- Unilateral o bilateralmente.
- Estáticas y dinámicas.
- Seguras o inseguras.

**5. Indique la opción correcta**

El control de la congestión se realiza en la capa:

- Física.
- Enlace.
- Red.
- Transporte.

#### 6. Ordene relaciones

Las siguientes capas realizan las siguientes tareas:

Capa Física	Controlar la operación de la red y el encaminamiento de los mensajes
Capa de Enlace	Definir como se establecerán las direcciones físicas de cada computadora
Capa de Red	Definir las características que debe tener el medio de transmisión
Capa de Transporte	Asegurar el transporte de datos desde máquina origen a máquina destino

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

La capa de Transporte realiza un control de extremo a extremo.

Verdadero

Falso

## 2. Indique la opción correcta

Un punto muy importante en el diseño de la capa de red es la determinación de como encaminar los paquetes.

Verdadero

Falso

## 3. Indique la opción correcta

Según el modelo OSI, la función de la Capa de Red se ocupa de:

Definir las características que debe tener el medio de transmisión.

Definir como se establecerán las direcciones físicas de cada computadora y como deberán ser las tramas de bits.

El control de la operación de la red y el enrutamiento de los paquetes.

Asegurar que todos los segmentos lleguen correctamente al otro extremo.

## 4. Indique la opción correcta

En la capa de red, las rutas pueden determinarse de dos formas:

Punto a punto o difusión.

Unilateral o bilateralmente.

Estáticas y dinámicas.

Seguras o inseguras.

## 5. Indique la opción correcta

El control de la congestión se realiza en la capa:

Física.

Enlace.

Red.

Transporte.

## 6. Ordene relaciones

Las siguientes capas realizan las siguientes tareas:

Capa Física

Definir las características que debe tener el medio de transmisión

Capa de Enlace

Definir como se establecerán las direcciones físicas de cada computadora

Capa de Red

Controlar la operación de la red y el encaminamiento de los mensajes

Capa de  
Transporte

Asegurar el transporte de datos desde máquina origen a máquina destino



# SP3 / H4: Las capas superiores: sesión, presentación y aplicación

## Capa de sesión (Session Layer)

Esta capa permite que los usuarios establezcan sesiones de trabajo entre ellos.

Por ejemplo, una sesión podrá permitir al usuario acceder a un sistema de tiempo compartido a distancia, o transferir un archivo entre dos máquinas. Otra sesión permitirá acceder a una página web de Internet (protocolo http), mientras otra podrá mantener un diálogo de chat entre varios correspondientes.

Uno de los servicios de la capa de sesión consiste en gestionar el control de diálogo.

Las sesiones controlan el tráfico de los mensajes en ambas direcciones.

La administración del testigo es un servicio de la capa de sesión en las redes TOKEN RING.

Otro servicio de la capa de sesión es la SINCRONIZACIÓN.

La capa de sesión proporciona puntos de verificación en el flujo de datos, con objeto de que después de una caída del enlace sólo se repitan los mensajes desde el último punto de verificación.

El propósito de la existencia de una sesión en OSI consiste en proveer a las capas superiores un canal libre de errores, independiente de la tecnología de las capas inferiores.

## Capa de Presentación (Presentation Layer)

A diferencia de las capas anteriores, preocupadas en el movimiento fiable de los bits de un extremo al otro, la capa de presentación **se ocupa de los aspectos de sintaxis y semántica de la información que transmite**.

Un ejemplo típico de servicio de esta capa es el relacionado con la codificación de datos conforme a lo acordado previamente.

La mayor parte de los programas de aplicación no intercambian trenes de bits aleatorios, sino estructuras de datos constituidos por varios elementos sencillos. Se pueden tener diferentes códigos (ASCII, EBCDIC), enteros, complementos a uno, a dos, etc.

Para posibilitar la comunicación de ordenadores con diferentes representaciones, la estructura de los datos por intercambiar puede definirse en forma abstracta.

El trabajo de manejar estas estructuras abstractas, y la conversión de la representación utilizada en el ordenador a la representación normal de la red, se lleva a cabo a través de la capa de presentación.

Esta capa está ligada también a otros aspectos de representación de la información. Por ejemplo, la COMPRESIÓN DE DATOS, que se utiliza para disminuir el tamaño de los mensajes a transmitir.

Otro aspecto es el de criptografía, o encriptación de datos, usada para cambiar la representación de los datos por razones de seguridad.

## Capa de Aplicación (Application Layer)

Esta capa contiene una **variedad de protocolos necesarios para hacer compatibles las distintas aplicaciones**.

Por ejemplo, considérese un editor orientado a pantalla que deba trabajar en una red con diferentes tipos de terminales, con distintas secuencias de escape, para insertar, borrar, movimientos de cursor, etc.

Una forma de resolver este problema consiste en **definir una Terminal Virtual** de Red abstracta, con la cual los programas pueden ser escritos de forma de tratar con ella.

Para transferir funciones de una terminal virtual de una red a una terminal real, se debe escribir un software que permita el manejo de cada tipo de terminal.

Por ejemplo, cuando el editor mueva el cursor del terminal virtual al extremo superior izquierdo, dicho software deberá emitir la secuencia de comandos para que el terminal real ubique al cursor en el sitio indicado.

El software completo del terminal virtual se encuentra en la capa de aplicación.

Otra función de la capa de aplicación es la **transferencia de archivos**.

La transferencia de archivos entre dos sistemas diferentes, requiere de la resolución de las incompatibilidades.

Otros servicios que también corresponden a esta capa son los utilizados por los Navegadores de Internet (Chrome, Mozilla, Explorer, Mosaic, Netscape, etc.) los cuales se tratan de software cliente que permite que un usuario pueda recorrer (navegar) distintos sitios de Internet.

Otros servicios son los utilizados por el de Correo Electrónico y otros.

## Transmisión de Datos en el Modelo OSI

El proceso emisor tiene datos que desea enviar al proceso receptor.

Los datos son generados en la aplicación, que los pasa a la capa de Aplicación, que le agrega la cabecera AH (*Application Header*) (que puede no existir) constituyendo así la PDU (*Unidad de Datos de Protocolo*) de la capa de Aplicación.

Ésta la pasa a la Capa de Presentación (a través del SAP: *Punto de Acceso al Servicio*) que los transforma en diferentes formas, con la posibilidad de incluir una cabecera en la parte frontal (PH: *Presentation Header*) pasando el resultado a la capa de Sesión.

Es importante observar que la Capa de Presentación no sabe distinguir cuáles son datos y cuál es el AH en lo que le pasó la Capa de Aplicación. Ni le corresponde saberlo.

Este proceso se repite hasta que se llega a la capa Física, lugar donde se transmiten definitivamente, en forma de trenes de bits, al receptor.

Así, los datos se empaquetan a través de un proceso que se llama **ENCAPSULAMIENTO**, que produce que, **a medida que los datos se desplazan a través de las capas del modelo OSI, reciben encabezados y en algunos casos trailers (colas) con información**.

En la otra máquina se produce el camino inverso.

La idea fundamental es que si bien la transmisión efectiva de datos es vertical, cada una de las capas está programada como si fuera transmisión horizontal.

# Servicios

La verdadera función de cada una de las capas OSI consiste en proporcionar servicios a las capas superiores.

Se llaman entidades a los elementos activos que se encuentran en cada capa; pueden ser *software* o *hardware*.

Las entidades de la misma capa pero de distintas máquinas se llaman capas homólogas o pares o iguales.

Las entidades de la capa "N" desarrollan un servicio para la capa "N+1". En este caso, la capa "N" se denomina PROVEEDOR DE SERVICIO, y a la capa "N+1" USUARIO DEL SERVICIO.

Los servicios están disponibles en el SAP (SERVICES ACCESS POINT) o punto de acceso al servicio.

Los SAP de la capa "N" son los lugares donde la capa "N+1" puede acceder a los servicios que se ofrecen.

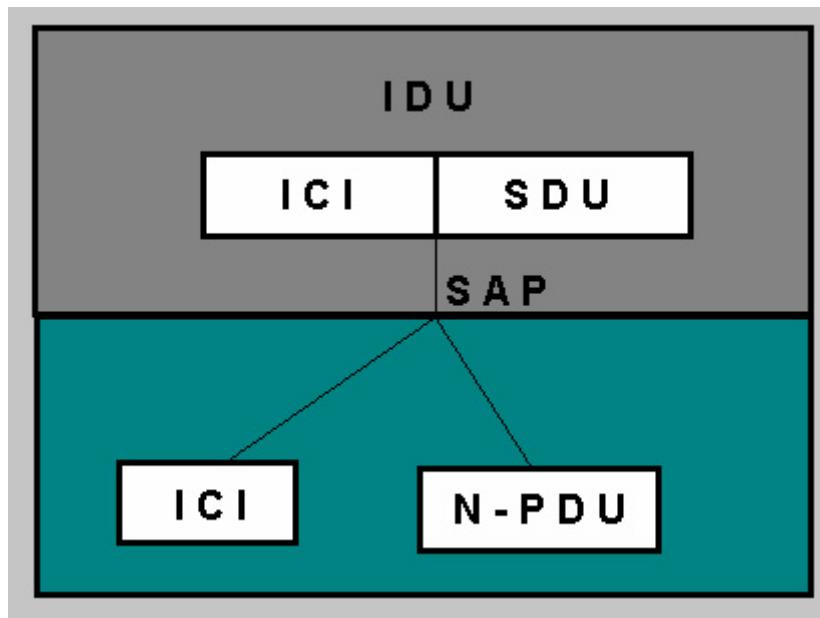
Cada SAP tiene una dirección que lo identifica.

(En el servicio telefónico, los SAP son las cajas en donde se conectan los teléfonos y las direcciones de los SAP son los números de abonado correspondientes a esos enchufes)

Para que haya intercambio de información entre dos capas, debe existir un conjunto de reglas acerca de la interfase.

En una interfase típica, la entidad de la capa "N+1" pasa un IDU (*Interface Data Unit*), o unidad de datos de la interfase a la capa "N", a través del SAP, como se ve en la figura siguiente.

El IDU está formado por una SDU (Service Data Unit) o unidad de datos del servicio y de información de control ICI (*Information Control Interface*).



"SAP" | <http://commons.wikimedia.org/wiki/File:Sap.PNG>

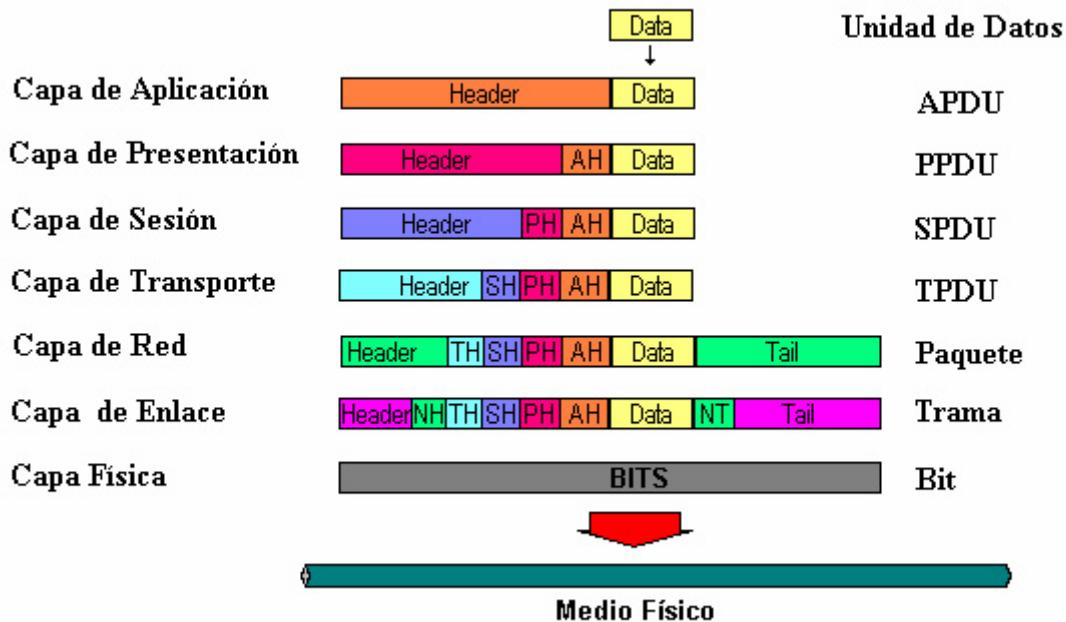
Para hacer la transferencia de una SDU puede ser necesaria o no la fragmentación por parte de la capa "N", de forma que a cada una se le asigne una cabecera y se envíe como PDUs distintas (**PDU = Protocol Data Unit**) o unidad de datos del protocolo.

Las entidades pares o iguales usan las cabeceras de la PDU para llevar a cabo su protocolo de igual a igual.

Las PDU de transporte se conocen como TPDU (*Transport PDU*), o unidad de datos del protocolo de transporte.

En TCP/IP, estas Unidades de Datos del Protocolo se conocen como "Segmentos".

Las de sesión SPDUs (*Sesión PDU*), las de Presentación PPDU (*Presentation PDU*) y las de Aplicación APDU (*Application PDU*).



## Ejemplo de estratificación en capas

Pensemos en el siguiente ejemplo: le pedimos que deje volar un poco la imaginación y que supongamos la siguiente situación con la consiguiente simplificación.

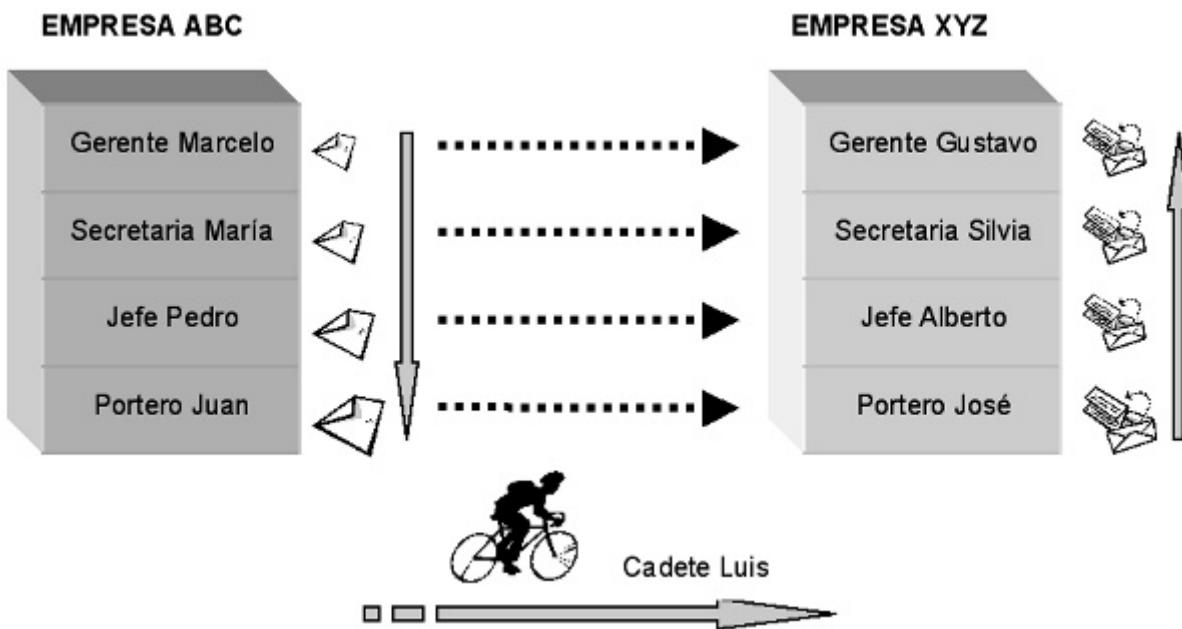
Consideremos dos empresas que llamaremos ABC y XYZ respectivamente.

Imaginemos que cada una de estas empresas está compuesta por cuatro pisos o plantas y que están ubicadas en dos barrios distintos, lo suficientemente separados entre sí.

Supongamos también que en el último piso de cada empresa tienen sus oficinas sendos gerentes, a los que identificaremos como Marcelo para la empresa ABC y Gustavo para la empresa XYZ.

El gerente de ABC necesita enviar un mensaje a su colega, pero no tiene ningún medio de comunicación disponible, ni teléfono, ni fax, ni email, solo dispone de hojas de papel, sobres y lápiz o lapicera. Como es el único medio que dispone, se decide a enviar un mensaje por este medio, y para ello escribe su mensaje, y como no quiere que nadie, excepto Gustavo, se entere del contenido del mensaje, lo introduce en un sobre y coloca al frente el nombre del gerente de XYZ y la dirección, y al dorso, su nombre y la dirección de la empresa ABC.

La figura siguiente muestra esta situación.



Una vez que el gerente de ABC completó su mensaje y lo introdujo en el sobre, le pasó este a su secretaria María, la cual a su vez quiere aprovechar la oportunidad para enviarle algún mensaje relacionado con su trabajo a su colega y amiga, la secretaria de la empresa XYZ, Silvia. Para ello también toma un papel y escribe su mensaje, luego introduce en un sobre más grande su mensaje y el sobre que le hubiera entregado Marcelo, y lo completa con su nombre y el de la otra secretaria; lo pasa al Jefe de Despacho Pedro.

Este, aprovecha, a su vez para enviarle un mensaje al Jefe Alberto utilizando el mismo procedimiento de María, e introduce el sobre recibido junto a su mensaje en otro sobre más grande, al cual le agrega el destinatario Alberto y el remitente Pedro. Luego pasa el sobre al Portero, para que este lo envíe a la compañía XYZ.

El portero Juan, usando el mismo procedimiento, le envía un mensaje al portero José. Por lo tanto, ahora entrega al cadete Luis el último sobre, que lleva el nombre del destinatario José y la dirección de la Empresa XYZ y como remitente, a Juan y la dirección de la empresa ABC.

El cadete, toma su vehículo y realiza el viaje hasta la otra empresa, entregando al destinatario que está registrado en el sobre, o sea José.

Este toma ese sobre y lo abre, encontrándose con otro sobre para el jefe Alberto y con un mensaje para él. Pasa el sobre a su superior y se guarda el mensaje.

Alberto realiza la misma operación, ya que el sobre estaba dirigido a él, y pasa a la secretaria Silvia el sobre que era para ella, la que a su vez, al abrirlo, se encuentra con su mensaje y con un sobre para Gustavo, su gerente, el que entonces puede disponer del mensaje enviado por su colega Marcelo.

Si el gerente de XYZ quiere enviar una respuesta, sigue el mismo procedimiento, salvo que en este caso el sobre sigue el camino inverso.

**De este procedimiento, podemos sacar algunas conclusiones a saber:**

1. El viaje real de los mensajes sigue un camino vertical descendente en el emisor y ascendente en el

receptor, pasando por el medio de transmisión físico (el cadete). Comunicación física o vertical. (Flechas rojas en la figura anterior)

2. Cada uno de los diferentes integrantes de cada empresa dialogó con su par u homólogo, aunque obviamente no directamente, sino por el procedimiento de los mensajes dentro de cada sobre.

Comunicación lógica u horizontal, (flechas negras de puntos en la figura anterior). Desde el punto de vista conceptual, los procesos de la capa "n" conciben su comunicación como si fuera horizontal, usando el protocolo de la capa "n", aún cuando estos se comuniquen con las capas inferiores a través de la interfase n/n1, y no con el otro lado. La abstracción del proceso entre pares es vital, sin esta técnica sería imposible el diseño de la red. Dicho de otra manera, sería un problema intratable si no se divide en varios más pequeños y manejables, o sea el diseño de capas individuales.

3. El procedimiento de introducir el mensaje recibido de la capa superior, se llama ENCAPSULAMIENTO, y es fundamental en el proceso de comunicación entre ambos extremos (emisor y receptor).

4. Cada capa o nivel brinda servicios a la inferior o superior, según el sentido del mensaje (emisor o receptor) a través de una Interface entre ambos que se llama Punto de Acceso al Servicio (SAP = Service Access Point), el cual no debe variar aun cuando pueda variar el responsable de un nivel.

5. Esto último permite que se pueda cambiar el protocolo de una capa por otro más eficiente, siempre y cuando no se altere del SAP.



¿Estás listo para un desafío?

**1. Indique la opción correcta**

El propósito de la existencia de la Capa de Sesión consiste en proveer a las capas superiores un canal libre de errores, independiente de la tecnología.

- Verdadero
- Falso

**2. Indique la opción correcta**

Uno de los servicios de la capa de sesión consiste en gestionar el control de diálogo.

- Verdadero
- Falso

**3. Indique la opción correcta**

Las sesiones pueden controlar el tráfico de los mensajes en ambas direcciones.

- Verdadero
- Falso

**4. Indique la opción correcta**

En la Capa de Presentación se pueden realizar tareas de compresión de datos.

- Verdadero
- Falso

**5. Indique la opción correcta**

Los navegadores de Internet utilizan servicios correspondientes a la Capa de:

- Aplicación.
- Presentación.
- Sesión.
- Transporte.

**6. Indique la opción correcta**

La capa que se ocupa de los aspectos de sintaxis y semántica de la información que transmite es la capa de:

- Aplicación.
- Presentación.
- Sesión.
- Transporte.

#### 7. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Procedimiento de transmisión de datos a través de las capas	Aplicación
Capa que permite que los usuarios establezcan sesiones de trabajo	Presentación
Capa que se ocupa de los aspectos de sintaxis y semántica	Sesión
Capa que contiene protocolos necesarios para compatibilizar aplicaciones	Encapsulamiento

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

El propósito de la existencia de la Capa de Sesión consiste en proveer a las capas superiores un canal libre de errores, independiente de la tecnología.

- Verdadero
- Falso

## 2. Indique la opción correcta

Uno de los servicios de la capa de sesión consiste en gestionar el control de diálogo.

- Verdadero
- Falso

## 3. Indique la opción correcta

Las sesiones pueden controlar el tráfico de los mensajes en ambas direcciones.

- Verdadero
- Falso

## 4. Indique la opción correcta

En la Capa de Presentación se pueden realizar tareas de compresión de datos.

- Verdadero
- Falso

## 5. Indique la opción correcta

Los navegadores de Internet utilizan servicios correspondientes a la Capa de:

- Aplicación.
- Presentación.
- Sesión.
- Transporte.

## 6. Indique la opción correcta

La capa que se ocupa de los aspectos de sintaxis y semántica de la información que transmite es la capa de:

- Aplicación.
- Presentación.
- Sesión.
- Transporte.

## 7. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Procedimiento de transmisión de datos  
a través de las capas

Encapsulamiento

Capa que permite que los usuarios establezcan sesiones de trabajo	Sesión
Capa que se ocupa de los aspectos de sintaxis y semántica	Presentación
Capa que contiene protocolos necesarios para compatibilizar aplicaciones	Aplicación

## SP3 / Ejercicio resuelto

Ante las expectativas de un mayor crecimiento en la empresa en la que trabajamos, ante la factibilidad de incrementar las conexiones de la red a otro edificio y posiblemente a otra sucursal, una vez comprendido el modelo de referencia OSI, que sirve de base de referencia sobre la cual fue implementada nuestra red, estamos en condiciones de afirmar que los servicios que actualmente corren sin problemas en la red actual (tales como la transferencia de archivos, correo electrónico y algunas aplicaciones) podrán seguir siendo prestados en una red mas grande.

Ante el crecimiento de la red en cuanto a su extensión física, aplicaremos lo aprendido en el estudio de las capas más bajas de la red (Física y Enlace de Datos) pudiendo inclusive ampliar los medios de transmisión utilizados actualmente, sin mayores problemas, ya que el modelo de referencia utilizado nos permite agregarlos sin tener que trabajar sobre las otras capas.

Además, podemos responder con base científica que se podrán adquirir programas de administración empresarial, pues estos no son más que software que se implementa sobre la capa de aplicaciones de nuestra red instalada. La estratificación en capas nos brinda esa tranquilidad.

Lo anterior se fundamenta en lo aprendido acerca de la estructura de las redes y los principios sobre los cuales esta asentado el modelo de referencia OSI.

## SP3 / Ejercicio por resolver

Aplicando lo aprendido referente a la división en capas y al encapsulamiento resuelva la siguiente situación:

Los gerentes de dos empresas "AZUL" y "ROJA" necesitan comunicarse entre sí, pero no tienen ningún medio de comunicación disponible, ni teléfono, ni fax, ni email, solo dispone de hojas de papel, sobres y lápiz o lapicera. Cada una de estas empresas está compuesta por cuatro pisos o plantas y que están ubicadas en dos barrios distintos, lo suficientemente separados entre sí.

Supongamos también que en el último piso de cada empresa tiene sus oficinas sendos gerentes, a los que identificaremos como Enrique para la empresa AZUL y Pablo para la empresa ROJA.

En el piso tercero de la empresa AZUL tiene sus oficinas Elena, la secretaria de Enrique, y en el tercer piso de la empresa ROJA está Sofía, la secretaria de Pablo.

En el segundo piso de la empresa AZUL está el despacho de Ignacio, el jefe del Departamento Despacho y en el mismo piso de la empresa ROJA, están las oficinas del jefe del Departamento Despacho Felipe.

En el primer piso de la empresa AZUL se encuentra Pedro, el empleado administrativo encargado de la correspondencia que entra y sale de la empresa, y en el piso similar de la empresa ROJA se encuentra Antonio con tareas similares

Por último, en la planta baja de ambos edificios se encuentra el portero, que para el caso de la empresa AZUL se llama Juan y en la empresa ROJA se llama José.

Además, tenemos a Luis, que es el cadete que realiza los viajes en su motocicleta entre ambas empresas, llevando la correspondencia entre ambas.

Se pide:

1. Indique mediante un esquema cómo es el mecanismo de envío de mensajes (encapsulamiento) entre ambas empresas.
2. Indicar además qué pasaría si se enferma Felipe y debe reemplazarlo Eduardo, que decide cambiar toda la actividad de su oficina. ¿Se podrán volver a comunicar? Si la respuesta es afirmativa, ¿bajo qué condiciones?
3. Describa cuáles son las conclusiones que ha podido sacar de este procedimiento.

## SP3 / Evaluación de paso



¡Vamos a comprobar cuánto aprendiste!

**1. Indique la opción correcta**

TCP/IP no es un modelo o pila de protocolos que pueda utilizarse para configurar una red LAN.

- Verdadero
- Falso

**2. Indique la opción correcta**

Una red punto a punto implica que el canal es compartido por todos los host y los mensajes son recibidos por todas las estaciones.

- Verdadero
- Falso

**3. Indique la opción correcta**

Una red de difusión es una red en la cual el mensaje va de un extremo a otro y no es compartido por todas las estaciones.

- Verdadero
- Falso

**4. Indique la opción correcta**

Todas las comunicaciones de Internet se llevan a cabo siguiendo el modelo de protocolos:

- IPX/SPX.
- NETBEUI.
- TCP/IP.
- NETBIOS.

**5. Indique la opción correcta**

Una de las funciones típicas de los protocolos de red, que se encarga de reordenar los envíos recibidos para que sigan la misma secuencia que en el origen (esto se debe a que en ciertos entornos, como por ejemplo Internet, las tramas pueden viajar por caminos diferentes y por lo tanto no recibirse en el orden correcto) es llamada:

- Direccionamiento.
- Control de errores.
- Control de flujo.
- Envío ordenado.

**6. Indique la opción correcta**

Indicar cuál NO ES un aspecto a tener en cuenta al analizar la red.

- TOPOLOGÍA: determina la interconexión entre los usuarios.
- PROTOCOLO: sincrónico o asincrónico, formato de los mensajes, etc.
- LAS FUNCIONES DE CADA CAPA: de manera tal que no haya dos capas que cumplan la misma función.
- PROCEDIMIENTOS DE RECUPERACIÓN: Procedimientos para el manejo de problemas tales como errores, ruido, etc.

**7. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Uno de los componentes de una red es:

la difusión

Uno de los tipos de canales de comunicación utiliza:

las especificaciones eléctricas

La capa física define:

la línea de transmisión

La capa de red puede resolver:

la congestión

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

TCP/IP no es un modelo o pila de protocolos que pueda utilizarse para configurar una red LAN.

Verdadero

Falso

## 2. Indique la opción correcta

Una red punto a punto implica que el canal es compartido por todos los host y los mensajes son recibidos por todas las estaciones.

Verdadero

Falso

## 3. Indique la opción correcta

Una red de difusión es una red en la cual el mensaje va de un extremo a otro y no es compartido por todas las estaciones.

Verdadero

Falso

## 4. Indique la opción correcta

Todas las comunicaciones de Internet se llevan a cabo siguiendo el modelo de protocolos:

IPX/SPX.

NETBEUI.

TCP/IP.

NETBIOS.

## 5. Indique la opción correcta

Una de las funciones típicas de los protocolos de red, que se encarga de reordenar los envíos recibidos para que sigan la misma secuencia que en el origen (esto se debe a que en ciertos entornos, como por ejemplo Internet, las tramas pueden viajar por caminos diferentes y por lo tanto no recibirse en el orden correcto) es llamada:

Direccionamiento.

Control de errores.

Control de flujo.

Envío ordenado.

## 6. Indique la opción correcta

Indicar cuál NO ES un aspecto a tener en cuenta al analizar la red.

TOPOLOGÍA: determina la interconexión entre los usuarios.

PROTOCOLO: sincrónico o asincrónico, formato de los mensajes, etc.

LAS FUNCIONES DE CADA CAPA: de manera tal que no haya dos capas que cumplan la misma función.

PROCEDIMIENTOS DE RECUPERACIÓN: Procedimientos para el manejo de problemas tales como errores, ruido, etc.

## 7. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Uno de los componentes de una red es:

la línea de transmisión

Uno de los tipos de canales de comunicación utiliza:

la difusión

La capa física define:

las especificaciones eléctricas

La capa de red puede resolver:

la congestión

# Situación Profesional 4: ¿Qué características tendrá nuestra red?

## Las redes de área local (LAN)

La empresa para la que usted trabaja como pasante sigue muy satisfecha con su trabajo. Con el asesoramiento que usted le ha brindado se deciden ampliar entonces la red según lo previsto, para lo cual Ud. deberá poder enlazar la red actual con otra red nueva en otro edificio contiguo ubicado a 80 metros. Ante esta situación se plantea ¿cómo resolveremos la conexión con ese edificio?. Para ello vamos a profundizar los conocimientos comprendiendo bien de qué se trata la red Local (LAN) para ver si lo que hicimos hasta ahora es compatible con las nuevas necesidades, de qué manera realizar el enlace, o si hace falta pasar a otro tipo de red y en ese caso, qué acciones tomar.

Estudiaremos los métodos de acceso al medio, si son compatibles con este crecimiento y los futuros, y haremos hincapié en el más utilizado: la red Ethernet y sus variantes (Fast Ethernet y Gigabit Ethernet).

# SP4 / H1: Introducción a las Redes de Área Local (LAN)

Si bien ya vimos en la SP1 la clasificación de las redes, profundizaremos algunos conceptos sobre las redes LAN y WAN para luego centrarnos en comprender mejor algunas características propias de las redes LAN.

## Redes LAN

La red LAN es aquella que tiene cerca sus computadoras, que pueden estar en la misma oficina, en diferentes pisos o en edificios contiguos de un mismo predio. Estas redes tienen gran velocidad en las comunicaciones porque no tienen problemas de interferencias. La razón es que la interferencia es directamente proporcional a la distancia entre el emisor y el receptor, y también directamente proporcional a la velocidad de la transmisión. Por lo tanto, al aumentar la distancia o velocidad de transmisión, también aumenta la interferencia.

En las redes LAN como las distancias son cortas las interferencias serán mínimas, por eso, las LAN se pueden dar el lujo de transmitir a altas velocidades a costa de distancias cortas. Las velocidades de transmisión de este tipo de red se hallan comúnmente entre los 10 Mbps y los 1000 Mbps (Mbps = Megabits por segundo = 1 millón de bits por segundo).

En estas redes la transmisión de datos tienen una tasa de error muy baja.

El cableado que se utiliza para interconexión tiene un uso privado, por lo que no se tiene que compartir. Esto significa que es utilizado solamente por las computadoras que conforman la LAN.

Utilizan canales de difusión. Veremos en esta SP mas adelante los detalles de esto.

En la SP5 veremos las características y performances de este cableado.

Una red LAN puede tener computadoras conectadas en diferentes pisos de un mismo edificio y también puede interconectarse con otras redes del tipo WAN, de las que daremos detalles a continuación

## Redes WAN

Las redes WAN son aquellas que tienen ubicadas sus computadoras en lugares muy lejanos. Pueden encontrarse agrupadas en diferentes continentes, países, provincias, ciudades o edificios muy separados dentro de la misma zona.

Estas redes tienen menor velocidad en las comunicaciones porque tienen mayores problemas de interferencias. La razón es que las WAN pueden lograr distancias grandes a costa de velocidades de transmisión bajas.

En la actualidad las velocidades de transmisión pueden ir desde los 56 Kbps (Kbps = Kilobits por segundo = 1000 bits por segundo) hasta varios Mbps, dependiendo de la tecnología utilizada al momento de efectuar la instalación de la red.

Utilizan canales punto a punto.

Además, en las redes WAN la velocidad se ve degradada por el uso de protocolos (lenguajes de comunicación) más pesados y complejos, pues los paquetes de datos que viajan a través de ellos deben poseer la información necesaria para que se puedan enrutar a través de las diferentes subredes (y así llegar a la dirección correcta) y retransmitirlos en caso de que se pierdan en el trayecto.

El cableado que interconecta las computadoras tiene por lo general un uso compartido y es prestado por empresas de telecomunicaciones (públicas o privadas) que lo ofrecen como un servicio a un costo generalmente alto. Este servicio puede incluir tramos con enlaces de microondas y satélites, sobre todo al interconectar computadoras que están diferentes países o incluso continentes.

Las WAN utilizan por lo general las líneas de teléfono y servicios de conexión con proveedores de internet para intercomunicar las computadoras. Además, no tienen límites con respecto a la cantidad de usuarios: por ejemplo se puede considerar a Internet como una WAN con millones de computadoras interconectadas.

En la mayoría de los casos, una red WAN está compuesta de varias redes LAN interconectadas. Por ejemplo una empresa puede tener una red LAN formada por varias computadoras en las oficinas de ventas, administración, compras y producción, y sus empleados utilizan la red tanto para comunicarse entre ellos como para acceder a las bases de datos comunes. Hasta acá es una red LAN, pero ahora que esta empresa tiene sucursales en otros países con los que comparte datos de ventas y estadísticas y además los empleados intercambian experiencias mediante grupos de opinión, los gerentes participan de videoconferencias, etc. Aquí ya tenemos una red WAN, compuesta por varias LAN de cada una de las sucursales.

## Diferencia entre LAN y WAN

Las redes pueden WAN utilizar en su gran mayoría conexiones punto a punto y las redes LAN utilizan canales de acceso múltiple, que a la vez son canales de difusión.

En esta SP veremos en las siguientes herramientas las redes de difusión y sus respectivos protocolos.

Es clave determinar, en una red de difusión, quién tiene derecho a usar el medio (canal), cuando existe competencia por éste.

Cuando se dispone de un solo canal, la determinación de quién utiliza el servicio, se hace mucho más difícil.

Existen muchos protocolos para resolver este problema. Los canales de difusión también se conocen como canales de acceso múltiple o canales de acceso aleatorio.

Las LAN tienen tres características importantes:

- 1 Un campo de acción relativamente reducido, a lo sumo unos pocos kilómetros.
- 2 Una velocidad de varios **Mbps** \* 4.1.
- 3 Una pertenencia a una sola organización.

Entre las LAN y WAN, se encuentran las MAN o Redes de Área Metropolitana, que cubren una ciudad completa, pero en general utilizan la tecnología desarrollada para las LAN.

Las redes de televisión por cable (**CATV**) \* 4.2 son un ejemplo de redes MAN.

Una diferencia importante entre las WAN y LAN, es que en las primeras, por lo general, el medio físico de comunicación es arrendado; en cambio en las LAN, al ser de pequeña cobertura, el medio es propio de la organización.

Esto trae varias ventajas: la principal es que el ancho de banda ya no significa un precioso recurso como lo es las grandes redes, de tal manera que los diseñadores no deben preocuparse por el mismo.

Otra diferencia es que el cable de la LAN es muy fiable, su tasa de error es 1000 veces inferior al de una WAN.

Esto permite trabajar con protocolos más sencillos, ya que en las WAN el tratamiento de errores debe hacerse

en cada una de las capas, pudiéndose evitar esto en el caso de las redes LAN.

# REFERENCIAS 4

## 4.1 : Mbps

Mbps:

Mega bits por segundo, o millones de bits por segundo. Es una medida de velocidad que fue estudiada en la Situación Profesional 1.

---

## 4.2 : CATV

CATV:

Cable de Televisión: Se trata de la red de cable coaxil que pasa por nuestro hogar.

---



¿Te animás a medir cuánto aprendiste?

**1. Indique la opción correcta**

Las redes pueden dividirse en dos categorías: las que utilizan conexiones punto a punto y aquellas que utilizan canales de difusión.

- Verdadero
- Falso

**2. Indique la opción correcta**

Las redes de televisión por cable CATV son redes LAN.

- Verdadero
- Falso

**3. Indique la opción correcta**

En las redes LAN, por lo general, el medio físico de comunicación es:

- Propio.
- Arrendado.
- Indistinto.
- Accesorio.

**4. Indique la opción correcta**

¿Cuál de las siguientes NO ES característica de las redes LAN?

- Campo de acción relativamente reducido.
- El tratamiento de errores debe hacerse en cada una de las capas.
- Velocidad de varios Mbps con cableado muy fiable y una tasa de error muy baja.
- Pertenencia a una sola organización.

**5. Indique la opción correcta**

Entre las LAN y las WAN, existe un tipo de redes que en general utilizan la tecnología desarrollada para las redes LAN:

- PAN.
- WLAN.
- VLAN.
- MAN.

#### 6. Ordene relaciones

Unir los conceptos: las redes LAN tienen las siguientes características:

Campo de acción  
Velocidad  
Pertenencia

Pocos kilómetros  
Muchos Megabits por segundo  
Una sola organización

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Las redes pueden dividirse en dos categorías: las que utilizan conexiones punto a punto y aquellas que utilizan canales de difusión.

- Verdadero
- Falso

## 2. Indique la opción correcta

Las redes de televisión por cable CATV son redes LAN.

- Verdadero
- Falso

## 3. Indique la opción correcta

En las redes LAN, por lo general, el medio físico de comunicación es:

- Propio.
- Arrendado.
- Indistinto.
- Accesorio.

## 4. Indique la opción correcta

¿Cuál de las siguientes NO ES característica de las redes LAN?

- Campo de acción relativamente reducido.
- El tratamiento de errores debe hacerse en cada una de las capas.
- Velocidad de varios Mbps con cableado muy fiable y una tasa de error muy baja.
- Pertenencia a una sola organización.

## 5. Indique la opción correcta

Entre las LAN y las WAN, existe un tipo de redes que en general utilizan la tecnología desarrollada para las redes LAN:

- PAN.
- WLAN.
- VLAN.
- MAN.

## 6. Ordene relaciones

Unir los conceptos: las redes LAN tienen las siguientes características:

Campo de acción  
Velocidad  
Pertenencia

Pocos kilómetros  
Muchos Megabits por segundo  
Una sola organización

# SP4 / H2: Los Métodos de Acceso al Medio en las redes LAN

## SP4 / H2: Los métodos de acceso al medio en las redes LAN

Existen en la actualidad dos tipos de protocolos más utilizados en la transmisión de redes LAN. Ellos son:

**CSMA/CD** \* 5.1: desarrollado por la compañía Xerox para la red Ethernet y también usado por el estándar de IEEE conocido como 802.3.

**TOKEN PASSIGN** \* 5.2: es un protocolo determinístico que pone un límite superior al tiempo de transmisión, que la Ethernet no tiene. Existen dos versiones:

- Token Bus desarrollado por General Motors. (En desuso).
- Token Ring: desarrollado por IBM. Presenta alta fiabilidad y capacidad de servicio.

## Estándares para Redes Locales IEEE 802

La clave es la disponibilidad de un estándar que permita la interconexión de distintos dispositivos, con una interfase de bajo costo; por ello IEEE, decidió, en Febrero de 1980, crear un comité, conocido como 802 para preparar los estándares de LAN.

El estándar preliminar IEEE 802 quedó establecido en Octubre de 1981. Si bien tuvieron grandes problemas para completar cada sección, el comité decidió su lanzamiento, obteniéndose comentarios que fueron incorporados en el próximo borrador.

Las siguientes son las principales características del estándar:



Interactiva "Estándares básicos de IEEE 802"

1 Se aceptaron dos métodos de acceso: CSMA/CD y Token Passing (paso de testigo).

2 Se reconocen dos topologías, de bus y anillo. El bus con cualquiera de ambos accesos al medio (CSMA/CD o Token) y anillo para Acceso Token Passing.

3 El Nivel 2 de OSI (Enlace de Datos), se divide en dos subcapas: una inferior, llamada Subcapa de Acceso al Medio (MAC: Media Access Control) y una superior conocida como Subcapa de Control del Enlace Lógico (LLC: Logical Link Control).

4 El protocolo de la subcapa LLC es el mismo para todos los métodos de acceso y topologías, definido por el estándar 802.2.

5 Para la subcapa MAC, se definieron tres estándares, el 802.3 (CSMA/CD), el 802.4 (Token Bus) y el 802.5 (Token Ring)

6 Debajo de la subcapa de Acceso al Medio (MAC) del Nivel 2 de OSI, o sea en el Nivel 1 de OSI, existen diferentes grupos de capas físicas. Aunque pueden usar medios físicos similares. El énfasis está puesto en la optimización del medio para el método de acceso de cada caso.

7 Cada Método de Acceso (MAC) puede tener múltiples medios (por ejemplo CSMA/CD y Token Passing pueden utilizar coaxiales banda base, de banda ancha y, como en la actualidad, UTP y fibra óptica).

Fuente: IES siglo 21 elaboración propia

El cuadro anterior, sólo muestra los estándares básicos de IEEE 802. En la actualidad existen muchos otros, que pueden ser comprobados en [www.ieee.org](http://www.ieee.org) [www.ieee.org](http://www.ieee.org) <http://www.ieee.org>

La aceptación de los estándares 802 fue rápida y ampliamente difundida. Han sido aceptados por ANSI y por la Organización Internacional de Estandarización (OSI) como un estándar internacional y por la Oficina Nacional de Estandarización de Estados Unidos.

## Los Estándares IEEE 802, una visión de conjunto

La tarea del IEEE 802 fue la de especificar el medio por el cual los dispositivos pueden comunicarse sobre una LAN. El comité ha caracterizado este trabajo en lo siguiente:

**"Una Red Local es un sistema de comunicación de datos que permite a un número de dispositivos independientes comunicarse con cualquier otro. Este estándar define un grupo de interfaces y protocolos para las Redes Locales".**

Una Red Local se distingue de otro tipo de redes en que la comunicación es confinada a un área geográfica de tamaño moderado, como un único edificio de oficinas, un almacén o depósitos, o un campus. La red generalmente depende de un canal de comunicaciones de alta velocidad y una tasa muy baja de errores. En casi todos los casos, la red propia y usada por una única organización. Esto en contraste a las redes que cubren grandes distancias (WAN), las que interconectan equipos en diferentes partes de un país o territorio. El objetivo del estándar es asegurar la compatibilidad entre equipamientos de manera de determinar que la comunicación se establezca con un mínimo de esfuerzo por parte de los usuarios. Para realizar esto, el estándar debe proveer especificaciones con las cuales establecer interfaces y protocolos comunes.

De todo esto obtenemos dos conclusiones inmediatas:

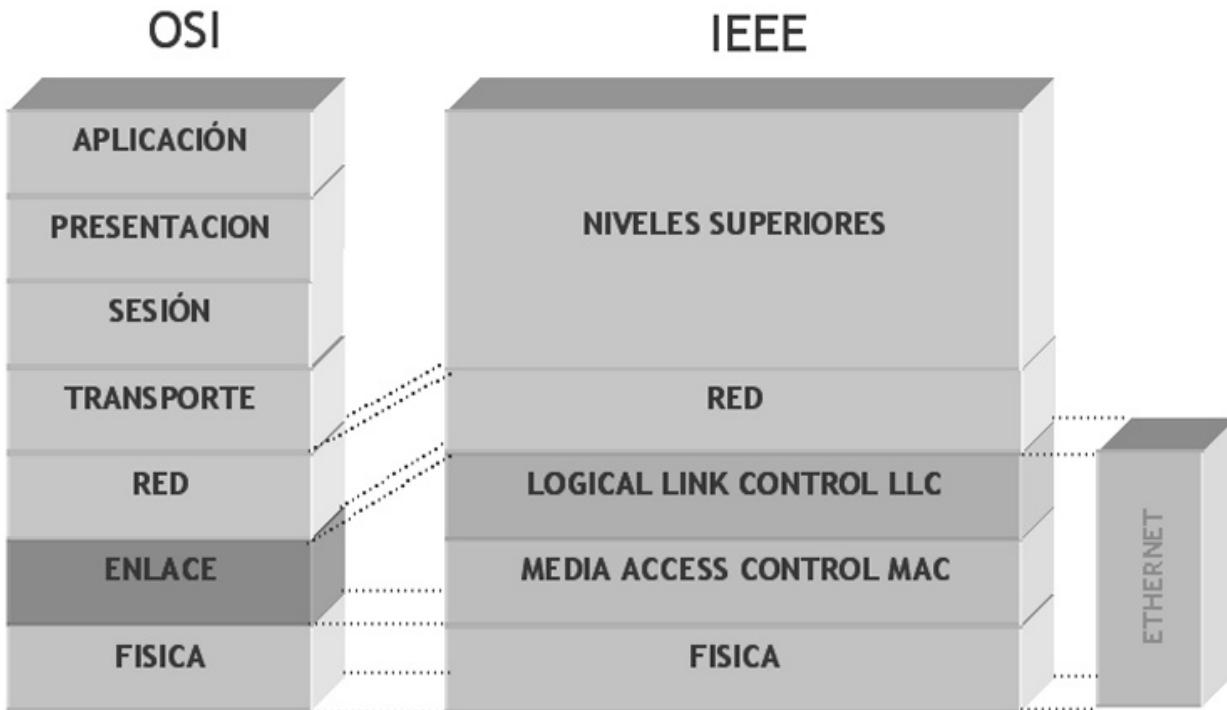
- 1- La tarea de comunicación sobre una red local es suficientemente compleja; por esta causa necesita ser descompuesta en subareas más manejables.
- 2- Un único método técnico no puede satisfacer todos los requerimientos.

La primera conclusión está reflejada en un "modelo de referencia de red local" adoptado por el comité. El modelo tiene tres capas:

- Física: esta capa está relacionada con la naturaleza del medio de transmisión y los detalles de los dispositivos conectados y las señales eléctricas.
- Control de Acceso al Medio (MAC = *Medium Access Control*): una red local está caracterizada por un conjunto de dispositivos compartiendo un único medio de transmisión. Es necesario, entonces, un mecanismo para controlar el acceso, de modo que un solo dispositivo intente trasmisir a la vez.
- Control Lógico del Enlace (LLC = *Logical Link Control*): esta capa está relacionada con el establecimiento, mantenimiento y liberación de un enlace lógico entre dispositivos, como así también la de establecer la negociación con la Capa de Red.

El resultado puede verse en la figura siguiente, en la cual se compara el Modelo de Referencia OSI, con el

Modelo de red Local de IEEE y con Ethernet.



La segunda conclusión fue alcanzada con mucho esfuerzo cuando aparentemente se concluyó que un único estándar no podía satisfacer a todos los participantes del comité. Existiendo entonces soporte para topologías bus y anillo.

### Estructura de los Estándares IEEE 802 para Redes Locales

El trabajo del comité IEEE 802 estaba originalmente organizado dentro de los siguientes subcomités:

- IEEE 802.1: Estándares de Interfaces de Capas Superiores (HILI = *High Layer Interface*). Da una introducción al conjunto de normas y define las primitivas de la interfase.
- IEEE 802.2: Estándares de Control Lógico del Enlace (LLC = *Logical Link Control*). Describe la parte superior de la capa de enlace, utiliza el protocolo LLC.
- IEEE 802.3: CSMA/CD. En ésta y en las siguientes, se describen las tres normas para las redes LAN, cubriendo los protocolos de la capa física y la subcapa MAC.
- IEEE 802.4: Token Bus. (Paso de testigo en bus).
- IEEE 802.5: Token Ring. (Paso de testigo en anillo).
- IEEE 802.6: Redes de Área Metropolitana (MAN = *Metropolitan Area Network*).

Estas normas difieren en la capa física y en la subcapa **MAC**, pero resultan compatibles en la capa de enlace.

El subcomité **HILI** (IEEE 802.1) ha publicado normas relacionadas con las interfaces de capas superiores, interconexión, direccionamiento y administración de redes.

El trabajo sobre redes de área metropolitana (IEEE 802.6) produjo la normalización de **FDDI** (Fiber Distribution

Data Interface).

Cada uno de estos grupos de trabajo o subcomités lograron estandarizar. Si bien cada uno de estos "estándares" tenía niveles físicos diferentes y subnivel de accesos al medio distintos, confluyeron en algún rasgo común (espacio de direcciones y comprobación de errores) y en algo muy importante: un nivel de enlace lógico único para todos.

## Estructura de los Estándares IEEE 802 completa

Con el desarrollo tecnológico los campos de trabajo se fueron ampliando y se constituyeron otros grupos de trabajo:

IEEE 802.7 – Banda ancha utilizando cable coaxial.

IEEE 802.8 – Grupo de Asesoramiento en Fibras Ópticas.

IEEE 802.9 – Servicios integrados de voz y datos en redes LAN.

IEEE 802.10 – Seguridad en redes LAN interoperables.

IEEE 802.11 – a/b/g/n- Redes LAN inalámbricas (WLAN Wi-Fi)

IEEE 802.12 – Prioridad por demanda (*Demand Priority*) (100 base VG)

IEEE 802.13 – No utilizado

IEEE 802.14 – Modems por cable.

IEEE 802.15 – 1 al 6 – Redes inalámbricas PAN (WPAN)

IEEE 802.16 - Redes de acceso metropolitanas de banda ancha inalámbricas (WIMAX)

IEEE 802.17 – Anillo de paquete resistente.

IEEE 802.18 – Grupo de Asesoría Técnica sobre Normativas de Radio.

IEEE 802.19 – Grupo de Asesoría Técnica sobre Coexistencia.

IEEE 802.20 – Acceso Wireless de banda ancha móvil.

IEEE 802.21 – Traspaso de medios independientes.

IEEE 802.22 – Red inalámbrica de Área Regional.

IEEE 802.23 – Grupo de trabajo en servicios de emergencia

IEEE 802.24 – Grupo de Asesoramiento Técnico en redes inteligentes (Noviembre de 2012)

IEEE 802.25 – Redes de Área de gran alcance (No ratificado aún)

# REFERENCIAS 5

## 5.1 : CSMA/CD

CSMA/CD:

Carrier Sense Múltiple Access with Collision Detection. Es el protocolo utilizado por las redes Ethernet. Y lo veremos en detalles más adelante.

---

## 5.2 : Token Passing:

Token Passing:

Paso de testigo, es un protocolo que usa una trama testigo, y la estación que la posee es la que puede usar el canal para transmitir.

---



¿Estás listo para un desafío?

**1. Indique la opción correcta**

Los métodos de acceso al medio más utilizados son: CSMA/CD (Ethernet) y TOKEN PASSING (Token Ring).

- Verdadero
- Falso

**2. Indique la opción correcta**

Una Red Local es un sistema de comunicación de datos que permite a un número de dispositivos independientes comunicarse con cualquier otro. Este estándar define un grupo de interfaces y protocolos para las Redes Locales.

- Verdadero
- Falso

**3. Indique la opción correcta**

Los estándares IEEE 802.3 describen las normas para las redes LAN, cubriendo los protocolos de la capa física y la subcapa MAC redes LAN.

- Verdadero
- Falso

**4. Indique la opción correcta**

¿A qué capas del Modelo de Referencia OSI corresponden la estructura de Ethernet y de los estándares 802 para redes locales?

- Física y Enlace.
- Enlace y Red.
- Red y Transporte.
- Transporte y Sesión.

**5. Indique la opción correcta**

El "modelo de referencia de red local" adoptado por el comité 802 hablaba de tres capas:

- Física, Enlace y Red.
- Enlace, Red y Transporte.
- Red, Transporte y Sesión.
- Física, Control de Acceso al Medio y Control Lógico del Enlace.

#### 6. Ordene relaciones

El trabajo del comité 802 estaba organizado dentro de subcomités que se dedicaba cada uno a estudiar los siguientes temas:

802.1 Estándares de interfaz de capas superiores	CSMA/CD
802.2 Estándares de control lógico del enlace	MAN
802.3 Método de Acceso al Medio	LLC
802.6 Redes de área metropolitana	HILI

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Los métodos de acceso al medio más utilizados son: CSMA/CD (Ethernet) y TOKEN PASSING (Token Ring).

- Verdadero
- Falso

## 2. Indique la opción correcta

Una Red Local es un sistema de comunicación de datos que permite a un número de dispositivos independientes comunicarse con cualquier otro. Este estándar define un grupo de interfaces y protocolos para las Redes Locales.

- Verdadero
- Falso

## 3. Indique la opción correcta

Los estándares IEEE 802.3 describen las normas para las redes LAN, cubriendo los protocolos de la capa física y la subcapa MAC redes LAN.

- Verdadero
- Falso

## 4. Indique la opción correcta

¿A qué capas del Modelo de Referencia OSI corresponden la estructura de Ethernet y de los estándares 802 para redes locales?

- Física y Enlace.
- Enlace y Red.
- Red y Transporte.
- Transporte y Sesión.

## 5. Indique la opción correcta

El "modelo de referencia de red local" adoptado por el comité 802 hablaba de tres capas:

- Física, Enlace y Red.
- Enlace, Red y Transporte.
- Red, Transporte y Sesión.

X Física, Control de Acceso al Medio y Control Lógico del Enlace.

## 6. Ordene relaciones

El trabajo del comité 802 estaba organizado dentro de subcomités que se dedicaba cada uno a estudiar los siguientes temas:

- |  |         |
|--|---------|
| 802.1 Estándares de interfaz de capas superiores | HILI    |
| 802.2 Estándares de control lógico del enlace    | LLC     |
| 802.3 Método de Acceso al Medio                  | CSMA/CD |
| 802.6 Redes de área metropolitana                | MAN     |



## SP4 / H3: La red Ethernet

Ethernet es una tecnología para redes de área local (*LAN* = Local Area Network) que permite la conexión de un conjunto de ordenadores (*host*) a través de un sistema flexible y de bajo costo. En la actualidad, la mayoría de los computadores soportan Ethernet, lo que junto al bajo costo y la alta flexibilidad constituyen las razones por las cuales es tan popular.

El término "Ethernet" se refiere a la familia de productos de red de área local (LAN) comprendidos por el estándar IEEE 802.3. Definido como protocolo CSMA/CD.

En la actualidad, encontramos tres velocidades de operación a través de cables de cobre (UTP, categorías 5, 5e 6 y 7) y de fibra óptica:

- 10 Mbps - Ethernet - 10Base-T
- 100 Mbps - Fast Ethernet - 100Base-T
- 1000 Mbps - Gigabit Ethernet - 1000Base-T

Trataremos de abarcar todos los temas relacionados con *Ethernet* a la vez de hacer esta lectura fácil y sencilla. Por ello incluiremos todo el rango de las tecnologías, como son la tradicional Ethernet de 10 Mbps, *Fast Ethernet* o Ethernet de 100 Mbps y *Giga Ethernet* o Ethernet de 1000 Mbps. Se describirán los distintos medios de comunicación con sus respectivos estándares, cómo el cableado estructurado, sus mediciones y los dispositivos de conectividad como Repetidores Hub y Switch.

Es importante entender cómo se pueden combinar los distintos componentes Ethernet para crear LAN, y a pesar de ver algunos ejemplos, podrá apreciar la infinita variación de diseños de red posibles.

Por sobre todo enfocaremos, en forma integral, el diseño del sistema de red que usa Ethernet para el transporte de datos entre los computadores miembros.

El sistema Ethernet ha crecido a lo largo de los años, haciéndose cada vez más complejo, incluyendo una gran variedad de medios y dispositivos, cada uno basado en su propio conjunto de hardware y su respectiva configuración. Trataremos de cubrir todos los sistemas utilizados, desde el coaxial original con que fue construida la primera red, al cableado estructurado y la fibra óptica utilizada en la actualidad.

Sabemos que existen, dentro del "Folklore de Ethernet", una serie de conceptos equivocados, y otros que no son comprendidos en su totalidad, lo que hace que muchas veces los sistemas sean mal configurados, cuando no mal instalados. Por ello vamos a recurrir siempre a los estándares oficiales, de manera que no queden dudas de la exactitud de los conceptos aquí vertidos.

### Breve historia y evolución de Ethernet

En el año 1973, Bob Metcalfe \* 6.1, en ese entonces experto del Centro de Investigación de Xerox en Palo Alto de California, (PARC = Palo Alto Research Center) redactó un documento describiendo el sistema de red Ethernet que él había inventado para interconectar estaciones de trabajo (computadoras avanzadas), haciendo posible el envío de datos entre ellas e impresoras láser de alta velocidad. Probablemente el primer gran invento de Xerox PARC fue la primera computadora personal con interfase gráfica de usuario y con dispositivo mouse de señalamiento, llamada la "Xerox Alto". Esta invención permitió incluir la primera impresora láser para computadoras personales, y con la creación de Ethernet, la primera tecnología LAN de alta velocidad interconectando todo el conjunto.

La red operaba a 2,94 Mbps usando el protocolo CSMA/CD A partir del ALOHA Network.

Metcalfe mejora el sistema Aloha, desarrollando un nuevo sistema que incluía:

- Un mecanismo que consiste en escuchar antes de transmitir (*Carrier Sense - CS*)
- Soporte de acceso múltiple en un canal compartido por muchas estaciones (*Multiple Access - MA*)
- Un mecanismo para detectar las colisiones (*Collision Detect - CD*)

De esta forma nace el protocolo CSMA/CD. El éxito del proyecto llevó al desarrollo de la especificación Ethernet de 10 Mbps Versión 2.0 por parte del consorcio formado por:

- Digital Equipment Corporation
- Intel Corporation
- Xerox Corporation

Ethernet es la tecnología de red LAN más ampliamente usada en el mundo entero. Cientos de millones de tarjetas adaptadoras de red (NIC = *Network Interface Card*), Hub y Switch han sido instalados y las expectativas son de un sostenido crecimiento.

En sus treinta años de vida, Ethernet ha sufrido varios cambios que le permitieron adaptarse a las crecientes demandas de ancho de banda y necesidades de distintos usuarios, que van desde las pequeñas redes hogareñas o de pequeños negocios hasta grandes corporaciones.

Ethernet ha estado permanentemente en estado de desarrollo y "reinvención" de los estándares por distintas organizaciones, principalmente el IEEE (*Institute of Electrical and Electronics Engineers*).

## Razones por las cuales Ethernet es la red de área local más difundida

**Ventajas de Ethernet**

Interacción

Las razones por las cuales Ethernet es la red LAN más extendida debemos encontrarlas en los siguientes ítems.

Bajo costo

Escalabilidad Una de las primeras críticas a Ethernet era la degradación de la performance a medida que aumentaba el tráfico, como consecuencia de las colisiones. Pero con el avance de la tecnología y sobre todo la posibilidad de la división de los "dominios de colisiones", constituye un simple y robusto mecanismo de transmisión que permite la entrega confiable de los datos.

Confiabilidad

Estandarización de los medios físicos

Amplia disponibilidad de herramientas de administración

Interactiva "Ventajas de Ethernet"

Las razones por las cuales Ethernet es la red LAN más extendida debemos encontrarlas en el siguiente ítem:

1 Bajo Costo: debido a que Ethernet utiliza un concepto muy sencillo de protocolo de acceso al medio (CSMA/CD), que estudiaremos en detalle más adelante, el hardware asociado a este protocolo es de muy bajo costo, lo que no sucede con otras LAN que, si bien cuentan con un acceso al medio más elaborado y más eficiente, sobre todo en alto tráfico, justamente esa eficiencia es a costa de un hardware más elaborado y obviamente más caro.

2 Escalabilidad: el primer estándar de la industria de Ethernet fue publicado en 1980. Este estándar definía una tasa de transferencia de 10 millones de bit por segundo (10 Mbps), el cual era muy rápido para la época, (la primera versión de Token

Ring era de 4 Mbps, y otras redes locales propietarias tenían una velocidad de 1 Mbps). Esto se mantuvo hasta mediados de los años '90. El desarrollo de Fast Ethernet a 100 Mbps en 1995, permitió un incremento de la velocidad diez veces mayor. Fast Ethernet constituyó uno de los mayores logros, ya que las interfaces de red actuales pueden soportar tanto 10 como 100 Mbps, sobre el mismo sistema de cableado estructurado; esta operación es totalmente automática a través de un sistema de autonegociación. Obviamente, este crecimiento pone un gran ancho de banda a disposición del usuario en su escritorio. Pero esto no quedó aquí: anticipándose a la creciente demanda, fue desarrollada en 1998 Gigabit Ethernet, proveyendo otro crecimiento de diez veces. Todo esto le da la posibilidad al administrador de la red de proveer conexiones de muy alta performance, ya sea como backbone [②](#) de la red, o en el escritorio del usuario.

3 Confiabilidad: una de las primeras críticas a Ethernet era la degradación de la performance a medida que aumentaba el tráfico, como consecuencia de las colisiones. Pero con el avance de la tecnología y sobre todo la posibilidad de la división de los "dominios de colisiones" [③](#), constituye un simple y robusto mecanismo de transmisión que permite la entrega confiable de los datos.

4 Estandarización de los medios físicos: uno de los medios más utilizados para la comunicación entre los equipos es el cableado estructurado, lo que permite a partir de un estándar de la industria, pasar de 10 Mbps a 1000 Mbps sin necesidad de cambiar la instalación de la estructura física del cableado. Esto posibilita que por el mismo medio se puedan transmitir voz y datos sin necesidad de cambiar absolutamente nada de la instalación. El cable UTP (Unshielded Twisted Pair) fue introducido en 1987, permitiendo la transmisión de la señal Ethernet sobre cableado estructurado, similar al usado en el sistema telefónico.

5 Amplia disponibilidad de herramientas de administración: la gran aceptación de Ethernet brinda otra ventaja, que consiste en una gran variedad de herramientas de administración, como así también de detección y reparación de fallas. Las herramientas de administración están basadas en estándares tales como SNMP (Single Network Management Protocol) que es un estándar ampliamente usado en TC-P/IP [④](#). Esto permite que el administrador de red cuente con una herramienta común para visualizar el funcionamiento de toda la red desde una ubicación central, abarcando los distintos dispositivos, tanto de las LAN como las WAN. Este monitoreo le permite saber el estado de los dispositivos conectados.

IES siglo 21 elaboración propia

## Los 4 Elementos Básicos de Ethernet

- **Medio Físico:** cables y dispositivos usados para transportar la señal digital
- **Trama:** conjunto ordenado de bit usados para transportar datos sobre el sistema
- **Protocolo de Control de Acceso al Medio:** las reglas que permiten que múltiples estaciones accedan al medio compartido (canal Ethernet)
- **Componentes de Señalización:** dispositivos electrónicos que permiten enviar y recibir señales sobre Ethernet

## Ethernet, IEEE 802.3 y los Sistemas Operativos

Tanto Ethernet como las Normas IEEE 802.3 son soportados por los sistemas operativos de redes más utilizados, tanto de Microsoft como de Apple, Linux, IBM y Novell en todas sus versiones.

## REFERENCIAS 6

### 6.1 : Robert Metcalfe

### Robert Metcalfe

0



Fundador de 3com

<b>Nombre</b>	Robert Metcalfe
<b>Nacimiento</b>	7 de abril de 1946 Brooklyn, Nueva York, Estados Unidos
<b>Alma mater</b>	Universidad de Harvard
<b>Ocupación</b>	Ingeniero

[https://www.ecured.cu/Robert\\_Metcalfe](https://www.ecured.cu/Robert_Metcalfe)



¡Vamos a comprobar cuánto aprendiste!

**1. Indique la opción correcta**

Ethernet se refiere a la familia de productos de red de área local comprendidos por el estándar 802.3 y define como protocolo CSMA/CD.

- Verdadero
- Falso

**2. Indique la opción correcta**

¿Cuál es la razón por la cual el cableado estructurado permite, a partir de un estándar de la industria, pasar de 10 Mbps a 1000 Mbps sin necesidad de cambiar la instalación de la estructura física del cableado?

- Bajo costo.
- Confiabilidad.
- Estandarización de los medios físicos.
- Amplia disponibilidad de herramientas de administración.

**3. Indique la opción correcta**

El mejoramiento realizado por Metcalfe del sistema ALOHA incluía un mecanismo que consistía en escuchar antes de transmitir, a este se lo denominó:

- Carrier Sense.
- Multiple Access.
- Collision Detection.
- Todas las anteriores.

**4. Indique la opción correcta**

Ethernet es una tecnología que se desarrolló para redes del tipo:

- PAN.
- LAN.
- CAN.

- MAN.

**5. Indique la opción correcta**

Indicar cuáles de las siguientes NO es una razón por las cuales Ethernet es la red LAN más extendida.

- Bajo Costo.
- Escalabilidad.
- Confiabilidad
- Poca disponibilidad de herramientas de administración.

**6. Ordene relaciones**

Indicar que velocidad corresponde a cada tipo de red:

Ethernet	4 Mbps
Fast Ethernet	100 Mbps
Gigabit Ethernet	1000 Mbps
Token Ring (primera versión)	10 Mbps

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Ethernet se refiere a la familia de productos de red de área local comprendidos por el estándar 802.3 y define como protocolo CSMA/CD.

- Verdadero
- Falso

## 2. Indique la opción correcta

¿Cuál es la razón por la cual el cableado estructurado permite, a partir de un estándar de la industria, pasar de 10 Mbps a 1000 Mbps sin necesidad de cambiar la instalación de la estructura física del cableado?

- Bajo costo.
- Confiabilidad.
- Estandarización de los medios físicos.
- Amplia disponibilidad de herramientas de administración.

## 3. Indique la opción correcta

El mejoramiento realizado por Metcalfe del sistema ALOHA incluía un mecanismo que consistía en escuchar antes de transmitir, a este se lo denominó:

- Carrier Sense.
- Multiple Access.
- Collision Detection.
- Todas las anteriores.

## 4. Indique la opción correcta

Ethernet es una tecnología que se desarrolló para redes del tipo:

- PAN.
- LAN.
- CAN.
- MAN.

## 5. Indique la opción correcta

Indicar cuáles de las siguientes NO es una razón por las cuales Ethernet es la red LAN más extendida.

- Bajo Costo.
- Escalabilidad.
- Confiabilidad
- Poca disponibilidad de herramientas de administración.

## 6. Ordene relaciones

Indicar que velocidad corresponde a cada tipo de red:

Ethernet	100 Mbps
Fast Ethernet	1000 Mbps
Gigabit Ethernet	10 Mbps
Token Ring (primera versión)	4 Mbps



# SP4 / H4: El control de acceso al medio utilizado por Ethernet (CSMA/CD)

Vamos a investigar cómo utiliza Ethernet el medio de transmisión. Este proceso se conoce como Método de Acceso al Medio.

En el caso de las redes Ethernet y las IEEE 802.3, el método utilizado es CSMA/CD (en inglés: *Carrier Sense Multiple Access with Collision Detection*, que traducido al castellano es Acceso Múltiple por Detección de Portadora con Detección de Colisiones). Éste es el método de acceso al medio que utilizan en común la Ethernet original y las derivadas de la norma IEEE 802.3, lo que ha hecho que en forma habitual a ambos tipos de redes se las designe como "Ethernet".

Es importante tener en cuenta que CSMA/CD se implementa tanto en la topología de Bus Lineal como en las de Estrella basada en concentradores, que pueden ser Hubs (o actualmente Switches) (Mas adelante verá claramente la diferencia entre Hub y Switch).

La necesidad de establecer un mecanismo para acceder al medio (es decir, usar el cable) se deriva del simple hecho de que el medio de transmisión es el mismo para todos los hosts conectados, lo cual significa que hay que diseñar alguna forma de compartirlo (*Multiple Access*); en este sentido los métodos de acceso al medio son algo así como las "reglas de convivencia de una familia".

La regla principal dice que:

En una red CSMA/CD, cualquier computadora puede acceder al medio de transmisión en cualquier momento, excepto en el caso de que otro host lo esté utilizando en ese momento.

La pregunta es, ¿cómo sabe una computadora si el cable está libre, es decir, que otra no lo está utilizando para transmitir? Continuamente cada computadora está "escuchando" la línea, o mejor dicho, detectando la portadora (Carrier Sense). De esta forma es muy sencillo para cada computadora saber si el medio está ocupado o libre.

Si está libre, inicia la transmisión de la trama de datos; en el caso que estuviera ocupado, simplemente sigue censando (escuchando) la línea a la espera de que se desocupe.

El problema puede darse en el caso de que estando libre la línea, dos o más computadoras intenten transmitir justo al mismo tiempo. En ese caso, como ambas escuchan que el medio está libre, ambas iniciarán la transmisión, pero las tramas enviadas por cada una de ellas "colisionarán" en la línea, haciendo que se pierda la información.

Para solucionar este inconveniente, cada computadora está atenta y en escucha de la línea para determinar si se produce una colisión. En el caso de que al transmitir, se produzca una colisión, entonces detendrá la transmisión, generará una señal para el barrido del canal y luego repetirá el procedimiento de escucha hasta que pueda reenviar la trama.

La pregunta central es ¿cuándo reenviará la trama?

Veámoslo así: la línea está libre, dos computadoras desean transmitir y lo hacen al mismo tiempo, las tramas colisionan, ambas computadoras detectan la colisión y deciden retransmitir la trama enviada. Si ambas esperaran el mismo lapso entre el instante en que detectan la colisión y reenvían la trama, entonces, volvería a producirse otra colisión, lo cual, repitiendo el proceso, originaría otra colisión, y luego otra... hasta el infinito.

Para evitar esta desagradable situación, el tiempo que media entre que la computadora detecta la colisión y el

momento en el cual reenvía la trama es un lapso aleatorio de tiempo (en realidad utilizan un algoritmo que calcula un valor de tiempo aleatorio). De esta forma disminuye la probabilidad de que las tramas retransmitidas vuelvan a colisionar.

Sin embargo, puede darse el caso que vuelva a ocurrir una colisión. En ese caso, las estaciones incrementan en tiempo de espera para volver a escuchar el medio. Por ejemplo, supongamos que se produce la primera colisión, entonces cada computadora "saca un retardo al azar" entre, 0 segundos y 1 segundo. Existe una cierta probabilidad (no nula) de que ocurra una nueva colisión. Entonces vuelven a "sacar" otro retardo al azar, pero esta vez un valor entre 0 segundos y 10 segundos (un intervalo más grande de tiempo). Esto hace que la probabilidad de que se produzca una segunda colisión disminuya drásticamente. En el caso que se produjera una segunda colisión, el tercer retardo aleatorio se elegiría de un intervalo aún mayor. Así hasta diecisésis veces; si en esa cantidad de intentos no pudo completar la transmisión, descarta todo intento de comunicación. Por esta razón, puede suceder que una estación no pueda enviar sus tramas (sobre todo, si la estación es muy lenta respecto de sus competidoras).

Obsérvese que en realidad es imposible saber de antemano en qué momento un host conseguirá establecer una comunicación, ya que el medio puede estar ocupado por otras transmisiones, sobre todo por máquinas más rápidas. Aun en el caso de que detecte que el mismo no esté en uso, puede ocurrir una colisión y tener que esperar un lapso indeterminado.

De allí el nombre de Redes No Determinísticas para las redes Ethernet, o todas las que usan este Control de Acceso al Medio.

Es por esto que las redes IEEE 802.3 no pueden garantizar una velocidad de transmisión estable, y lo que es más importante, la cantidad de colisiones se incrementa con la cantidad de host conectados (lo que multiplica los tiempos de espera de retransmisión), lo cual hace que el rendimiento no sea estable y decrezca sensiblemente con la cantidad de computadoras conectadas.

Es por este procedimiento que también suele decirse que las redes CSMA/CD "*compiten*" por el uso del medio, y que es una forma de acceso basada en la contención.

## La difusión de la trama

Las redes IEEE 802 (es decir tanto IEEE 802.3 como IEEE 802.4 y 802.5) son redes de difusión (también llamadas de broadcast), ya que una vez que la transmisión de la trama se realiza con éxito, es difundida a todos los host conectados a la red. Cada computadora escucha la trama y lee la dirección de destino.

En el caso que la dirección de destino no coincida con la propia, simplemente la descarta; en el caso de coincidencia de la dirección destino, entonces inicia el procesamiento completo de la misma, pasándola a las capas superiores.

## Una aclaración con respecto al término difusión

Existe cierta confusión en cuanto al uso de términos como difusión y multidifusión. En los párrafos anteriores hemos hecho referencia al proceso de difusión inherente a cualquier sistema de comunicación con medio compartido, en el sentido de que el host emisor deposita la trama en la línea con la dirección que identifica a la computadora destino; esta trama es difundida a lo largo de todo el cable mientras cada host compara la dirección destino con la propia; y sólo en el caso de que ambas coincidan, se procesa por completo el mensaje.

Existe otro procedimiento, también denominado de difusión, en el cual el objetivo de la computadora emisora es enviar un mensaje a todos los demás host de la red. Como en ese caso deberíamos enviar una trama a cada

host, lo que se realiza es enviar una sola trama con una dirección destino especial. Esta dirección especial, significa "este mensaje es para todas las computadoras", de tal forma que todos los host, luego de leer la dirección de destino, procesarán por completo el mensaje. Este mecanismo se denomina "*Broadcast*", si el mensaje se envía a todas las PC de la red, y "*Multicast*" si se envía a un grupo de host de la red. Como extensión de esta denominación, se llama "*Unicast*" cuando la dirección está dirigida a un solo host.

Como se puede observar, en este caso la difusión no se debe a una característica inherente al medio de transmisión, sino a la necesidad de un host de enviar un mensaje a todos los demás en la red; es un proceso "*voluntario*".

En Ethernet, se observa que aunque sólo las computadoras destino procesarán por completo el mensaje (*Unicast* y *Multicast*), todos los host de la red lo recibirán y compararán las direcciones, ya que la red es inherentemente de difusión.

Por último una aclaración. Las redes de difusión inherente como Ethernet y las basadas en IEEE 802 presentan por definición un riesgo de seguridad ante penetraciones a la seguridad física del edificio donde residen o por donde circula el cableado; ya que si bien es cierto que las placas de red diseñadas por los fabricantes "legales" tienen la obligación de cumplir la norma, en el sentido de que una placa de red debe eliminar toda trama que no vaya dirigida a ella y sólo procesar por completo las que tengan su propia dirección MAC, no se necesita una tecnología distinta para olvidar esta regla y diseñar una placa que escuche y procese todas las tramas transmitidas en la red; de hecho, estos dispositivos existen, y son conocidos como placas de red (NIC) promiscuas, o que trabajan en modo promiscuo y son utilizadas por los analizadores de protocolos, ya que deben capturar todo el tráfico, aun las tramas con errores para luego procesarlas y definir, de esta forma, el funcionamiento de la red.

**En este aspecto, podemos aclarar que los cables de fibra óptica son más difíciles de violar que los de UTP o coaxial, ya que es más complicado realizar una derivación clandestina. Es por esto que los cables de fibra óptica se recomiendan para instalaciones de seguridad.**

## Las Direcciones MAC

Obviamente para que la difusión funcione, cada host debe tener asignada una dirección (o nombre que la identifique), es la llamada Dirección MAC (MAC Address) (MAC: Media Access Control – Control de Acceso al Medio) o también dirección física o de hardware.

Las direcciones MAC son comunes a todas las normas basadas en IEEE 802 y constan de 48 bits (6 Bytes), que habitualmente se describen con caracteres hexadecimales.

Dado que para codificar cada carácter hexadecimal se necesitan 4 bits, una dirección MAC consta de 12 dígitos hexadecimales. (Es habitual que, al representar un dato en hexadecimal, se utilice alguna de las dos siguientes nomenclaturas.

Por ejemplo, para indicar que 3BF6 representa un valor en hexadecimal se lo puede escribir como:

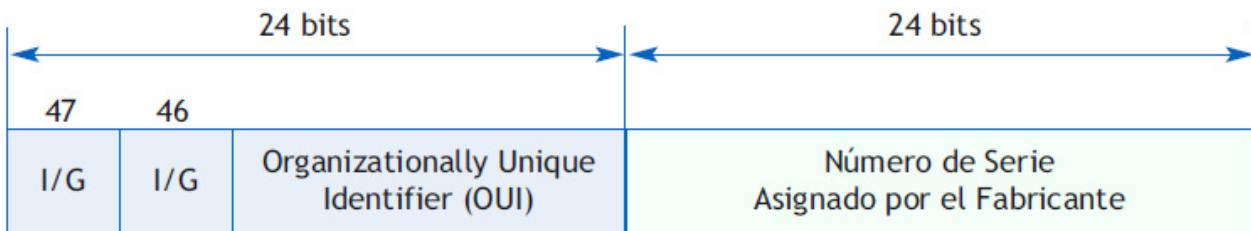
- (3BF6)H
- 0x3BF6

En el caso de Ethernet, las direcciones MAC residen físicamente en las NIC y es imposible cambiarlas, por cuanto se graban en el proceso de fabricación. Estas direcciones están compuestas de dos partes:

- Los 24 bits (3 bytes) más significativos (los que se encuentran hacia la izquierda) se conocen como

el Organizational Unique Identifier (OUI).

- Los 24 bits (3 bytes) menos significativos indican el Número de Serie consignado por el fabricante ver figura.



Notar que el bit 46 indica lo siguiente, según sea su valor:

- 0 (cero) asignado globalmente por el fabricante.
- 1 (uno) asignado localmente por el administrador de red.

Observe que se ha elegido una cantidad grande de bits (48) para codificar las direcciones MAC de estos 48 bits., obteniéndose un valor teórico de:

$$2^{48} = 281.474.976.710.656$$

Como dos bit quedan a criterio del administrador de red, los 46 bits restantes proporcionan:

$$2^{46} = 7,03\,1013$$

Es decir, unos 70 billones de direcciones MAC distintas.

Esta cantidad es tan grande porque ha debido procurarse que no existan dos placas de red con la misma dirección MAC, ya que si existieran dos placas de red con la misma dirección MAC y ambas residieran en la misma red... imagine las consecuencias.

Para garantizar que los fabricantes no den la misma dirección MAC a dos placas, existe una organización centralizada que asigna a cada fabricante un lote de direcciones válidas.

$$2^{48} = 281.474.976.710.656$$

## OUI (Organizationally Unique Identifiers)

A continuación puede verse un resumen (extraído de Internet) de algunos fabricantes de NIC. Como se observa, los dos primeros dígitos hexadecimales son par.

## OUI (Organizationally Unique Identifiers)

Asignación	Organización	Asignación	Organización	Asignación	Organización
00000C	Cisco	0000AA	Xerox	080020	Sun
00000E	Fujitsu	0000C8	Altos	08002B	DEC
00000F	NeXT	0000E2	Acer	080037	Fujitsu-Xerox
00001D	Cabletron	0020AF	3COM	080039	Spider Systems
00005E	IANA	0080C2	IEEE 802.1	080046	Sony
00006B	MIPS	00AA00	Intel	08005A	IBM
000077	MIPS	02608C	3Com-IBM	080069	Silicon Graphics
000093	Proteon	080002	3Com	08008B	Pyramid
0000A2	Wellfleet	08000B	Unisys	800010	AT&T

*Los 3 primeros bytes son siempre distintos  
Si el bit menos significativo es 0 (cero), la dirección es global*

## Forma de presentar las direcciones MAC

Las direcciones MAC son expresadas como 12 dígitos hexadecimales (0 - 9, más A - F en mayúsculas), pueden ser escritos como:

Sin separar con guiones:	123456789ABC
Separados con un guión:	123456-789ABC
Separados por puntos:	1234.5678.9ABC
Separados por dos puntos:	2:34:56:78:9A:BC
Separados por guiones:	12-34-56-78-9A-BC

"direcciones MAC" | IES siglo 21 elaboración propia

Las puede visualizar en su PC (siempre que tenga una placa de red Ethernet), con los siguientes comandos:

Desde WINDOWS: ejecutando CMD para abrir la ventana de comandos. Una vez allí ejecutar IPCONFIG/ALL y observar el parámetro Physical Address

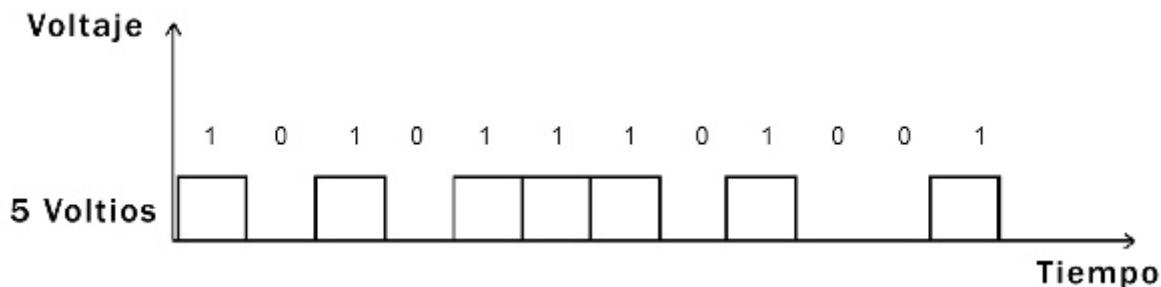
## La codificación Manchester

Como se ha comentado anteriormente, todas las transmisiones de datos basadas en Ethernet o en las normas IEEE 802 son de Banda Base, lo cual significa que los datos se transmiten en forma digital, es decir, en secuencias de 0 y 1 lógicos.

Habitualmente uno tiende a pensar que los 1 y 0 lógicos se codifican (o traducen) a sus equivalentes eléctricos como un nivel alto de tensión (digamos, 5 voltios) para un 1 lógico y un nivel bajo (digamos 0 voltios) para un 0 lógico, como se muestra en la siguiente figura.

En realidad esto no es así y en casi ningún caso se utiliza una codificación tan directa.

La razón principal es que realmente induce a error porque se hace difícil distinguir un 0 lógico (0 voltios), de un período de inactividad o no transmisión. Suponga una secuencia lógica como 0000001101 codificada de esta manera (0 voltios para el 0 lógico y 5 voltios para el 1 lógico), ¿cómo hace el receptor para saber que la secuencia comienza con 6 ceros y no que ese tiempo es un período de inactividad?

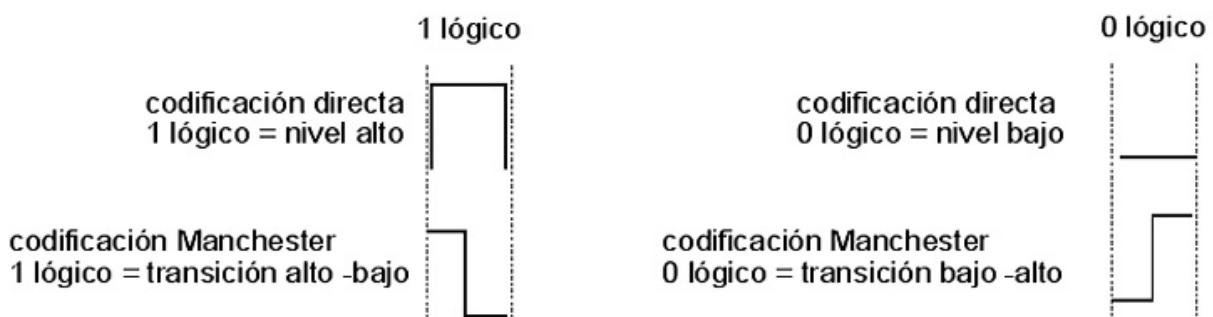


"Transmisión digital codificada en forma "directa". | Transmisión digital codificada en forma "directa". 1 lógico= 5 volts; 0 lógico= 0 volts

En respuesta a esto, la IEEE 802 adoptó la codificación Manchester, en cuyo caso, justo en la mitad del período correspondiente a un bit, se introduce una transición, ya sea de nivel alto a bajo o viceversa.

Según la Codificación Manchester será:

- una transición de nivel alto a nivel bajo codifica un 1 lógico.
- una transición de nivel bajo a nivel alto codifica un 0 lógico



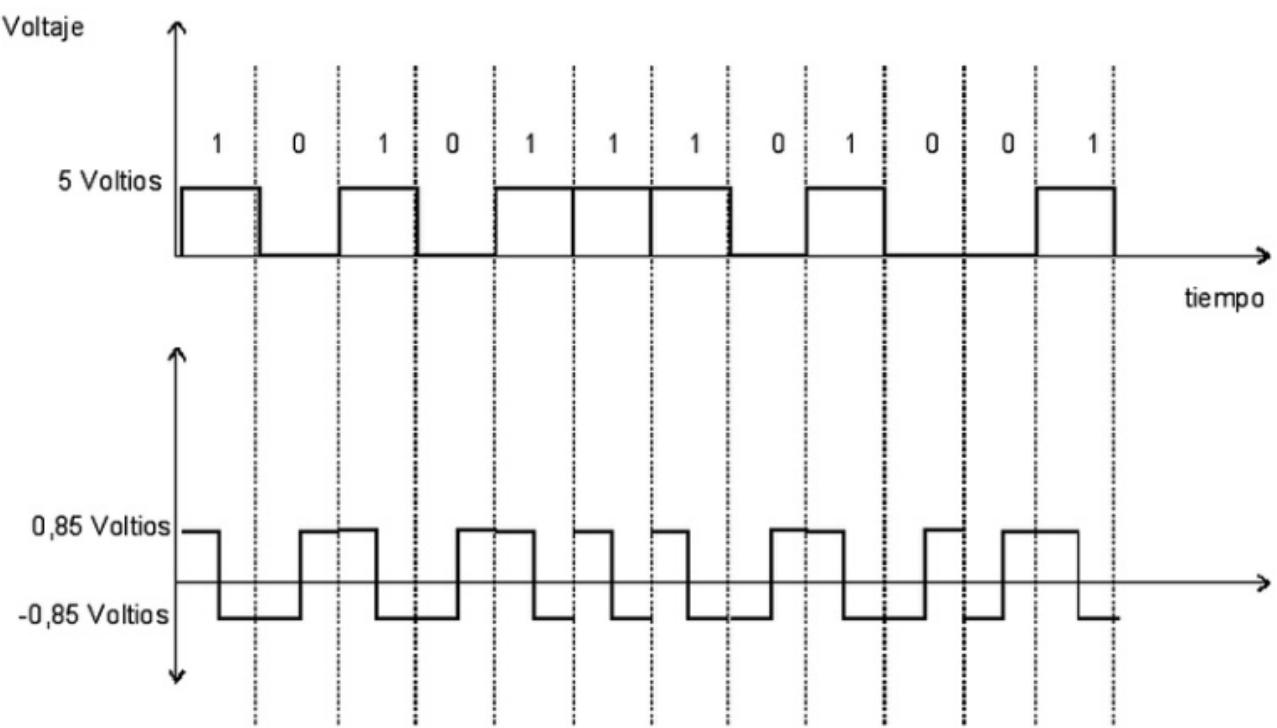
Relación entre la codificación directa y la Manchester

De esta forma es imposible confundir un 0 lógico con un período de inactividad, ya que un período de no transmisión es un período sin transiciones de nivel.

Para eliminar ambigüedades, el nivel alto se sitúa en 0.85 voltios y el nivel bajo en un valor negativo de tensión - 0.85 voltios. (En realidad existe otra razón de gran peso para establecer los niveles altos y bajos en dos valores de tensión iguales pero de distinto signo: analizando el espectro en frecuencia (Fourier) del tren de

pulsos transmitido con esta codificación, encontrará que la componente de continua (frecuencia = 0) es nula o despreciable. La ausencia de la componente de continua es una ventaja a la hora de transmitir.

La siguiente figura muestra las codificaciones "directa" y Manchester para la misma secuencia de unos y ceros lógicos.



Una dificultad emergente de la codificación Manchester es que necesita el doble del ancho de banda para transmitir la misma secuencia de bits que la codificación directa.

Existen otros métodos de codificación; el comité IEEE 802 adoptó el Manchester por una cuestión de confiabilidad y sencillez.

## Otros controles de acceso al medio (CSMA/CA)

Este método de acceso es muy similar a CSMA/CD y se utiliza para redes inalámbricas.

Las dos primeras siglas CS y MA significan lo mismo que lo explicado para CSMA/CD.

La última sigla CA significa *Collision Avoidance* (Evasión de Colisiones) consiste en enviar una señal muy corta que indica el anuncio de la intención de transmitir antes de hacerlo con la finalidad de **evitar** que se produzcan las colisiones.

De esta forma, el resto de los equipos sabrán cuando hay alguno que va a trasmisitir y se reduce la probabilidad de colisiones en el canal.



¿Te animás a medir cuánto aprendiste?

**1. Indique la opción correcta**

La regla principal del protocolo de acceso al medio CSMA/CD dice que en una red CSMA/CD cualquier computadora puede acceder al medio de transmisión en cualquier momento, excepto en el caso de que otro host lo esté utilizando en ese momento.

- Verdadero
- Falso

**2. Indique la opción correcta**

Ethernet es una red NO DETERMINÍSTICA.

- Verdadero
- Falso

**3. Indique la opción correcta**

Una dirección MAC esta compuesta por dos partes: 24 bits (3 bytes) para la Organizational Unique Identifier (OUI) y 24 bits (3 bytes) para el Número de Serie.

- Verdadero
- Falso

**4. Indique la opción correcta**

¿En que tipo de redes se utiliza el protocolo CSMA/CD?

- 802.3.
- Ethernet.
- Bus lineal.
- Estrella basada en concentrador HUB o SWITCH.
- Todas son correctas.

**5. Indique la opción correcta**

Por confiabilidad y sencillez, el comité 802 adoptó, para codificar la transmisión de datos:

- La Ley de Shannon.
- El modelo OSI.
- La ley de la Entropía.
- La codificación Manchester.

**6. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

El método de acceso al medio	Define como se codifican los datos en la transmisión
La codificación Manchester	Define como se utiliza el medio de transmisión
La dirección MAC	Determina la identificación única a nivel físico

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

La regla principal del protocolo de acceso al medio CSMA/CD dice que en una red CSMA/CD cualquier computadora puede acceder al medio de transmisión en cualquier momento, excepto en el caso de que otro host lo esté utilizando en ese momento.

Verdadero

Falso

## 2. Indique la opción correcta

Ethernet es una red NO DETERMINÍSTICA.

Verdadero

Falso

## 3. Indique la opción correcta

Una dirección MAC esta compuesta por dos partes: 24 bits (3 bytes) para la Organizational Unique Identifier (OUI) y 24 bits (3 bytes) para el Número de Serie.

Verdadero

Falso

## 4. Indique la opción correcta

¿En que tipo de redes se utiliza el protocolo CSMA/CD?

802.3.

Ethernet.

Bus lineal.

Estrella basada en concentrador HUB o SWITCH.

Todas son correctas.

## 5. Indique la opción correcta

Por confiabilidad y sencillez, el comité 802 adoptó, para codificar la transmisión de datos:

La Ley de Shannon.

El modelo OSI.

La ley de la Entropía.

La codificación Manchester.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

El método de acceso  
al medio

Define como se codifican los  
datos en la transmisión

La codificación  
Manchester

Determina la identificación única  
a nivel físico

La dirección MAC

Define como se utiliza el medio  
de transmisión

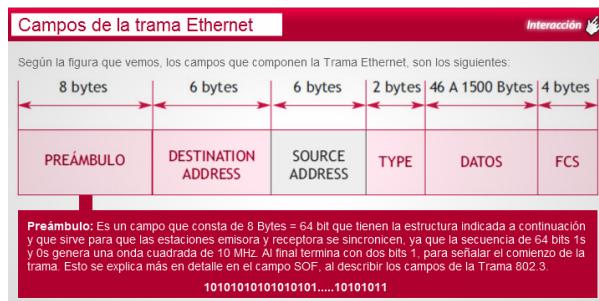


# SP4 / H5: Definiciones de tramas. Los estándares IEEE 802.x

Veremos con un poco más de detalle cómo interaccionan las subcapas LLC y MAC.

¿Recuerda que en la situación profesional anterior habíamos indicado que los mensajes enviados por las capas superiores se encapsulaban agregando una cabecera y, a menudo, una cola, a medida que descendía a través de la pila de protocolos?

## Campos de la trama Ethernet



Interactiva "Campos de la trama Ethernet"

Según la figura que vemos, los campos que componen la Trama Ethernet, son los siguientes:

Preámbulo: es un campo que consta de 8 Bytes = 64 bit que tienen la estructura indicada a continuación y que sirve para que las estaciones emisora y receptora se sincronicen, ya que la secuencia de 64 bits 1s y 0s genera una onda cuadrada de 10 MHz. Al final termina con dos bits 1, para señalar el comienzo de la trama. Esto se explica más en detalle en el campo SOF, al describir los campos de la Trama 802.3.

101010101010101....10101011

MAC Address: Destination y Source (Destino y Origen): Estos campos están formados por 6 Bytes = 48 bit, como ya hemos visto anteriormente, cuando se trató de las direcciones MAC origen y destino.

Type (Tipo): Este campo indica el Tipo de protocolo de Capa de Red; de esta forma Ethernet permite dar servicios a "múltiples" protocolos de Capa de Red, haciéndola muy versátil.

Datos: Este campo define al "paquete", o sea la Unidad de Datos generada en la capa de red. Debe tener un tamaño mínimo de 46 Bytes = 512 bits, para que la estación emisora pueda detectar las colisiones (CD: Collision Detection). En caso de que no alcance esa cantidad, deberá agregarse un "relleno" (PAD), para completar el tamaño mínimo. El máximo del campo Datos es de 1500 Bytes.

FCS (Frame Check Sequence): Es un mecanismo para la detección de errores. Está formado por 4 Bytes = 16 bits, y utiliza una operación de división de polinomios de toda la trama (excepto el Preámbulo y el SOF), por un polinomio fijo. Se envía el resto de esa división como FCS.

IES siglo 21 elaboración propia

## La trama IEEE 802.3

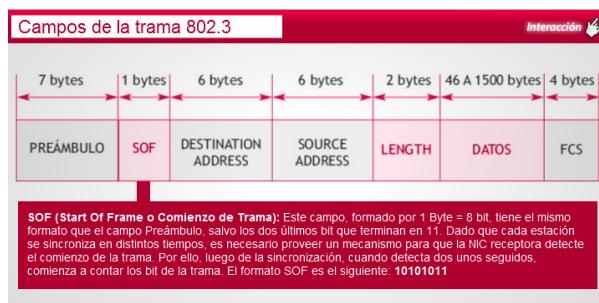
A nivel de la capa de enlace, considerando las dos subcapas introducidas por IEEE, la situación es la que se muestra en la siguiente figura:

La subcapa de Control Lógico del Enlace (LLC: Logical Link Logical) agrega un encabezado LLC, donde figuran los números de secuencia del paquete y acuse. Lo cual (de ser utilizado) permite que la capa de enlace ofrezca a las capas superiores (capa de red) un servicio confiable, porque permitirá que la subcapa LLC del receptor reorganice los paquetes en el mismo orden en que fueron enviados.

Luego, este nuevo paquete se encapsula en la subcapa MAC donde se agrega una cabecera y una cola, lo cual incluye, entre otra cosas las direcciones MAC de la computadora emisora y la de destino (de 48 bits o 6 Bytes c/u). Finalmente, éste es el paquete que es enviado por el medio de transmisión.

## Campos de la trama 802.3

La Trama 802.3, según la figura que vemos a continuación, es similar a la Trama Ethernet, salvo que el campo Preámbulo está compuesto por 7 Bytes = 56 bits y tiene el mismo formato que en Ethernet. Se agrega un campo Comienzo de Trama (SOF) que, en realidad, completa el campo preámbulo y de esta forma es similar a la trama Ethernet. También se reemplaza el campo Tipo por campo Length (Longitud de Trama).



Interactiva "Campos de la trama 802.3"

SOF (Start Of Frame o Comienzo de Trama): Este campo, formado por 1 Byte = 8 bit, tiene el mismo formato que el campo Preámbulo, salvo los dos últimos bit que terminan en 11. Dado que cada estación se sincroniza en distintos tiempos, es necesario proveer un mecanismo para que la NIC receptora detecte el comienzo de la trama. Por ello, luego de la sincronización, cuando detecta dos unos seguidos, comienza a contar los bit de la trama. El formato SOF es el siguiente:

10101011

Length (Longitud de Trama): Este campo indica la longitud de la Trama, ya que en este caso, la Trama MAC, no tiene contacto con la Capa de Red, sino con la Subcapa LLC, siendo ésta la que negocia con la Capa superior el Tipo de protocolo de Capa de Red, y actúa de esta forma en forma similar a Ethernet.

Datos: Este campo ahora no define al "paquete", sino la Unidad de Datos de la Capa LLC, conocida como Trama LLC, o también como DSAP (Destination Service Access Point), SSAP (Source Service Access Point), Destino y Origen respectivamente, y que tienen que ver con el Punto de Acceso al Servicio que provee la Subcapa LLC.

IES siglo 21 elaboración propia

## Diferencias entre las tramas Ethernet y 802.3

Existen 2 diferencias entre una trama IEEE 802.3 y una Ethernet:

- **La primera** es que la trama Ethernet no tiene el Byte de Inicio de Trama (SOF), pero en su lugar el Preámbulo es de 8 Bytes en vez de 7, como ocurre en la IEEE 802.3. En realidad esto no cambia en nada, ya que en un caso (Ethernet) se trata de 64 bits terminando en 11, y en el otro son 56 bits con la secuencia 101010... y otros bits con el formato 10101011. O sea, que en definitiva es lo mismo.
- **La segunda** diferencia es que la trama Ethernet no posee los 2 Bytes de Longitud, pero en su lugar incorpora 2 Bytes de Tipo, que indican a qué protocolo de la capa de red van dirigidos los datos. Esto hace que la Trama Ethernet sea incompatible con la Trama 802.3.



¿Estás listo para un desafío?

**1. Indique la opción correcta**

En la trama 802.3 el Preámbulo consta de 7 Bytes que sirve para que las estaciones emisora y receptora se sincronicen, y luego viene un campo Comienzo de Trama de 1 Byte, cuyos dos últimos bits terminan en 11.

- Verdadero
- Falso

**2. Indique la opción correcta**

En la trama 802.3 el campo Length indica la longitud de la trama ya que en este caso, la trama Mac no tiene contacto con la Capa de Red, sino con la Subcapa LLC, siendo esta la que negocia con la capa superior el Tipo de protocolo de la Capa de Red, y actúa de esta forma en forma similar a Ethernet.

- Verdadero
- Falso

**3. Indique la opción correcta**

En la trama 802.3 el campo que provee un mecanismo para que la NIC receptora detecte el comienzo de trama es el campo:

- Preámbulo.
- SOF.
- Length.
- FCS.

**4. Indique la opción correcta**

En las tramas Ethernet y 802.3 el campo que provee un mecanismo para detección de errores es el campo:

- Preámbulo.
- SOF.
- Length.

- FCS.

**5. Indique la opción correcta**

En las tramas Ethernet y 802.3 el campo Destination Address (Dirección de Destino) consta de:

- 16 bits.
- 32 bits.
- 48 bits.
- 64 bits.

**6. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

En la trama Ethernet

Existe el campo Type

En la trama 802.3

Existe el campo FCS

En las tramas Ethernet y 802.3

Existe el campo Length

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

En la trama 802.3 el Preámbulo consta de 7 Bytes que sirve para que las estaciones emisora y receptora se sincronicen, y luego viene un campo Comienzo de Trama de 1 Byte, cuyos dos últimos bits terminan en 11.

Verdadero

Falso

## 2. Indique la opción correcta

En la trama 802.3 el campo Length indica la longitud de la trama ya que en este caso, la trama Mac no tiene contacto con la Capa de Red, sino con la Subcapa LLC, siendo esta la que negocia con la capa superior el Tipo de protocolo de la Capa de Red, y actúa de esta forma en forma similar a Ethernet.

Verdadero

Falso

## 3. Indique la opción correcta

En la trama 802.3 el campo que provee un mecanismo para que la NIC receptora detecte el comienzo de trama es el campo:

Preámbulo.

SOF.

Length.

FCS.

## 4. Indique la opción correcta

En las tramas Ethernet y 802.3 el campo que provee un mecanismo para detección de errores es el campo:

Preámbulo.

SOF.

Length.

FCS.

## 5. Indique la opción correcta

En las tramas Ethernet y 802.3 el campo Destination Address (Dirección de Destino) consta de:

16 bits.

32 bits.

48 bits.

64 bits.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

En la trama Ethernet

Existe el campo FCS

En la trama 802.3

Existe el campo Length

En las tramas Ethernet y 802.3

Existe el campo Type

## SP4 / Ejercicio resuelto

Podremos realizar la conexión de nuestra red actual con el edificio contiguo con toda tranquilidad, ya que, según lo aprendido, teniendo en cuenta la estratificación por capas sobre la que implementamos nuestra red, sabemos que por sobre las características físicas de los medios utilizados (en nuestro caso par trenzado UTP), la capa de enlace de datos nos permite asegurar que por encima del control de acceso al medio (en nuestro caso CSMA/CD) la subcapa control de enlace lógico (LLC) tiene la capacidad de ser compatible tanto con una ampliación de la actual como con cualquier otra topología, ya sea LAN o MAN.

Resolvemos la conexión con el edificio contiguo que se encuentra a 80 metros entonces, con una extensión de nuestra red local (LAN) sobre una red Ethernet.

No nos hace falta entonces pasar a otro tipo de red (cuyas características físicas estudiaremos en profundidad en las situaciones profesionales siguientes)

## SP4 / Ejercicio por resolver

Ud. deberá resolver la siguiente situación. La empresa para la que usted trabaja como pasante deciden ampliar más la red, para lo cual Ud. deberá poder enlazar la red actual con otra red nueva en otro edificio ubicado a 800 metros. Ante esta situación se plantea ¿Qué enlace implementar?. Lo que hicimos hasta ahora será compatible con las nuevas necesidades? de qué manera realizaremos el enlace? hace falta pasar a otro tipo de red? Funcionará todo? En base a que podremos realizar tal afirmación?



¡Vamos a comprobar cuánto aprendiste!

**1. Indique la opción correcta**

Ethernet es una red DETERMINÍSTICA.

- Verdadero
- Falso

**2. Indique la opción correcta**

Las redes CSMA/CD "compiten" por el uso del medio y la forma de acceso es basada en la contención.

- Verdadero
- Falso

**3. Indique la opción correcta**

La capa relacionada con la naturaleza del medio de transmisión, los detalles de los dispositivos conectados y las señales eléctricas es la capa:

- Física.
- Enlace.
- Red.
- Transporte.

**4. Indique la opción correcta**

El Control Lógico del Enlace y el Control de Acceso al Medio operan en el nivel de referencia OSI:

- Física.
- Enlace.
- Red.
- Transporte.

**5. Indique la opción correcta**

Una dirección MAC está compuesta por:

- 16 bits.

- 24 bits.
- 32 bits.
- 48 bits.

**6. Indique la opción correcta**

El método de acceso al medio más utilizado en redes LAN actualmente es:

- CSMA/CD.
- CSMA/CA.
- TOKEN BUS.
- TOKEN RING.

**7. Indique la opción correcta**

¿Cuál es la razón por la cual, sobre el mismo sistema de cableado estructurado se permite incrementar la tasa de transferencia y proveer conexiones de muy alta performance, ya sea como backbone de la red, o en el escritorio del usuario?

- Bajo costo.
- Escalabilidad.
- Confiabilidad.
- Amplia disponibilidad de herramientas de administración.

**8. Ordene relaciones**

El trabajo del comité 802 estaba organizado dentro de subcomités, que se dedicaba cada uno a estudiar los siguientes temas:

- |   |            |
|---|------------|
| 802.4 Paso de testigo en bus                  | Token Bus  |
| 802.2 Estándares de control lógico del enlace | Token Ring |
| 802.3 Método de Acceso al Medio               | LLC        |
| 802.5 Paso de testigo en anillo               | CSMA/CD    |

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Ethernet es una red DETERMINÍSTICA.

Verdadero

Falso

## 2. Indique la opción correcta

Las redes CSMA/CD "compiten" por el uso del medio y la forma de acceso es basada en la contención.

Verdadero

Falso

## 3. Indique la opción correcta

La capa relacionada con la naturaleza del medio de transmisión, los detalles de los dispositivos conectados y las señales eléctricas es la capa:

Física.

Enlace.

Red.

Transporte.

## 4. Indique la opción correcta

El Control Lógico del Enlace y el Control de Acceso al Medio operan en el nivel de referencia OSI:

Física.

Enlace.

Red.

Transporte.

## 5. Indique la opción correcta

Una dirección MAC está compuesta por:

16 bits.

24 bits.

32 bits.

48 bits.

## 6. Indique la opción correcta

El método de acceso al medio más utilizado en redes LAN actualmente es:

CSMA/CD.

CSMA/CA.

TOKEN BUS.

TOKEN RING.

## 7. Indique la opción correcta

¿Cuál es la razón por la cual, sobre el mismo sistema de cableado estructurado se permite incrementar la tasa de transferencia y proveer conexiones de muy alta performance, ya sea como backbone de la red, o en el escritorio del usuario?

- Bajo costo.
- Escalabilidad.
- Confiabilidad.
- Amplia disponibilidad de herramientas de administración.

#### 8. Ordene relaciones

El trabajo del comité 802 estaba organizado dentro de subcomités, que se dedicaba cada uno a estudiar los siguientes temas:

802.4 Paso de testigo en bus	LLC
802.2 Estándares de control lógico del enlace	CSMA/CD
802.3 Método de Acceso al Medio	Token Bus
802.5 Paso de testigo en anillo	Token Ring

# Situación profesional 5: ¿Que topologías, dispositivos y cables utilizar?

## La capa Física de las redes

Ya ha comprendido cómo es una red local (LAN) y los parámetros que la rigen. Ahora determinaremos el tipo de medio físico (cableado) y los estándares por utilizar para conformar esa red local. De acuerdo con las necesidades de la empresa, deberá decidir que dispositivos utilizará y cómo será la distribución y orden de conexión de los mismos. Para ello es necesario que comprenda las normas de instalación para comunicar los distintos armarios de conexión. El cableado debe respetar ciertos requisitos indispensables para cumplir con su cometido.

# SP5 / H1: Topologías básicas de redes LAN

## La Capa Física en las redes LAN

A nivel técnico es habitual referirse al tipo de cableado con que se diseñan las redes como la Capa Física de la Red. Esta terminología surge a partir de las especificaciones de las normas para los modelos multicapa de las redes, tema que estudiaremos más adelante.

Aclaremos también que mejor que decir cableado sería decir canal de comunicación o medio de comunicación, ya que de esta forma incluiríamos también a las redes que no están basadas en cables, como las redes infrarrojas o las que utilizan satélites. En este contexto, a los cables suele denominárselos medios de transmisión guiados, y a las comunicaciones infrarrojas o por medio de ondas electromagnéticas que se propagan por el espacio o la atmósfera como medios de transmisión no guiados. Para los primeros, veremos las topologías básicas de redes LAN y para los segundos veremos las topologías básicas de redes wireless o WLAN.

Además, estudiaremos los diversos tipos de cable que se utilizan como elemento de conexión física de las redes LAN.

## Topologías Básicas de Redes LAN

La forma en la cual se interconectan las computadoras en una red, se denomina "topología de la red". Es importante notar que se hace referencia a una topología lógica y no necesariamente física; es decir, es altamente posible que nunca vea un tendido de cable que a simple vista se asemeje a los que se presentarán en los gráficos que ejemplifican los casos siguientes.

Las tres topologías lógicas básicas de las redes de computadoras son las siguientes:

### Topología de Bus

En la topología bus, también conocida como bus lineal, todas las computadoras se conectan a un mismo medio físico de transmisión, a través de sus correspondientes placas de red.

Dichas placas de red están diseñadas de acuerdo al modo en que van a conectarse (por ejemplo, la topología bus); es decir, existen placas de red específicas para cada tipo. De aquí la respuesta a por qué es posible correr "cualquier sistema operativo en cualquier topología de red": quien maneja los pormenores de la topología es el dispositivo de interconexión; la placa de red y sus drivers o controladores.

Los drivers o controladores son pequeños programas (software) que permiten al sistema operativo interactuar con la placa de red. En general, los fabricantes de placas de red se ven obligados a crear drivers específicos para cada sistema operativo de red; es decir que deben proveer los controladores para Windows 9x, Windows NT, Unix, Linux etc.

Como puede deducir, en el sustrato más físico de una red, las comunicaciones no se producen "entre computadoras", sino entre placas de red, las cuales envían y reciben la información proporcionada por el sistema operativo. Dado que también es posible conectar al medio físico otros dispositivos, como por ejemplo impresoras (siempre que soporten la correspondiente placa de red), suele denominarse a cada dispositivo conectado como nodo y, en el contexto más amplio, como host.

Al medio físico también suele denominárselo backbone (columna vertebral) o segmento.

Es muy importante hacer notar que no es necesario (y de hecho pocas veces ocurre) que los dispositivos conectados se encuentren sobre una línea recta; en general, éstos adoptan físicamente la disposición adecuada a la oficina o ambiente de trabajo y esto es posible ya que el cable ofrece la flexibilidad necesaria.

Observe también que los extremos del cable no se unen, sino que se encuentran conectados a los **terminadores** \*7.1. La función de los terminadores es evitar que "se pierda" la señal eléctrica; sin ellos la red se ve imposibilitada de transmitir.

Lo que realmente distingue a la topología lógica de bus es que:

- todos los dispositivos se conectan directamente al medio,
- que el mismo es compartido y,
- que los extremos del cable o backbone no se unen entre sí, sino que sus extremos están conectados a los terminadores.

En general, la topología de bus lineal se basa en tecnologías pasivas, en el sentido de que cuando uno de los host desea transmitir, deposita la señal en el bus con su correspondiente dirección de destino; la cual se difunde a lo largo de todo el medio. Todos los nodos "leen" la señal y comparan la dirección de destino con la propia, si ésta no coincide, se desecha el mensaje, pero en el caso de coincidir, continúa su procesamiento. Se dice que es una tecnología pasiva, porque ningún nodo hace un esfuerzo por retransmitir la señal o mensaje, simplemente se limitan a tomarlo del medio para inspeccionarlo. Esto le brinda una característica especial a las redes de bus: si una de las computadoras (o nodos) conectados deja de funcionar, la red sigue funcionando ya que los nodos no participan activamente en la transmisión.

Por otro lado, se debe ser sumamente cauto en cuanto a dos aspectos: los terminadores deben estar correctamente conectados y las conexiones de cada nodo al bus deben estar perfectamente realizadas, porque si cualquiera de estas conexiones no está perfectamente hecha, el bus literalmente se corta y es incapaz de transmitir. La mayor cantidad de fallas en esta topología se produce, justamente, en esos dos puntos y es bastante engorroso aislar la falla (es decir, encontrarla) ya que no existe un método sencillo que nos indique cuál de los nodos está mal conectado o en qué lugar del cable está el problema, lo cual obliga a revisar todo el cableado.

Generalmente esta topología es la que demanda menor cantidad de metros de cable.

## Topología de Estrella

En esta topología, los nodos no se conectan directamente al medio de transmisión, sino que lo hacen (a través de sus respectivas placas de red) con un dispositivo concentrador o hub, siendo éste quien se encarga de difundir los mensajes entre los nodos.

En general, los hub no tienen capacidad de direccionamiento, es decir que de la misma forma que en la topología de bus cuando un nodo emite un mensaje, todos los demás lo toman y leen la dirección de destino, y sólo en el caso que ésta sea la propia, lo siguen procesando.

De la misma forma que en la topología bus, la caída o desconexión de cualquiera de los nodos no afecta el resto del funcionamiento de la red; pero a diferencia de aquella, aun si el cableado sufriera desperfectos, la red seguiría funcionando, ya que el hub permite aislar muy fácilmente la computadora cuya conexión es defectuosa. Por otro lado, los hub suelen proveer información sobre el funcionamiento de la red, indicando con luces de diferentes colores (led) qué nodos están funcionando correctamente y cuáles no, y cuál está transmitiendo en cada momento. Por supuesto que si el concentrador o hub falla, la red no funciona.

## Topología de Anillo o Ring

En el caso de la topología de anillo o ring, un cableado vincula a todos los nodos, de tal forma que cada nodo se encuentra conectado a otros dos, razón por la cual no hay extremos de línea ni terminadores. Las señales volcadas al medio de transmisión se desplazan en un único sentido de circulación, de nodo en nodo.

A diferencia de la topología de bus, que es pasiva (las placas de red de cada nodo sólo escuchan los mensajes puestos en la línea, pero no participan en la propagación de la señal), en la topología de anillo cada una de las computadoras participa en la retransmisión de la señal. El proceso habitual se basa en que un nodo recibe una señal "por un lado"; si la dirección no coincide con la propia, entonces, "lo pasa" al siguiente nodo. En este caso, la placa de red de cada nodo participa activamente en la retransmisión de las señales, lo cual trae como consecuencia que si una de las computadoras falla, o existen problemas en el cableado de la misma, la red no funcionará. Este tipo de problema se minimiza utilizando un MAU, que actúa como un HUB para la topología anillo; en este caso es el MAU el que se encarga de retransmitir la señal.

A diferencia de las otras topologías, el anillo provee un orden en las comunicaciones, lo cual minimiza la merma de rendimiento ante el incremento de nodos conectados a la red, ofreciendo un rendimiento más estable.

## Un problema de seguridad...

Si ha leído atentamente las descripciones de las tres topologías básicas, podrá deducir que en la esencia misma de las comunicaciones de red existe un grave problema de seguridad. Observe que en el caso del bus lineal y en de la topología de estrella, todos los mensajes pasan en definitiva por un mismo elemento, el cual es compartido por todas las computadoras que forman la red: el cable backbone, en el caso del bus lineal y el hub, en el caso de la topología en estrella. También habrá notado que las normas establecen que cuando una placa de red recibe un mensaje que no tiene su propia dirección como destino, debe desecharlo...y ahí es justamente donde radica el problema. ¿Qué pasaría si cuando una placa de red recibe un mensaje que no la tiene como destino, infringe la norma y no desecha el mensaje?...De esta forma, si un ladrón puede acceder físicamente a su red, podrá "ver" todas las comunicaciones que se producen en la misma.

Esta debilidad, cuyo origen radica en que inherentemente las redes LAN utilizan el mecanismo de difusión, ha dado lugar a la creación de medidas de seguridad, como por ejemplo la encriptación de los mensajes, de tal forma que, aunque pueden ser interceptados por extraños, les resultarán ilegibles si no conocen el código mediante el cual se descifra el mismo. En instalaciones de alta seguridad, además del encriptado de los mensajes, se agregan medidas que impiden físicamente el acceso de extraños al cableado de la red. Por ejemplo, en el Pentágono todos los cables de red se disponen dentro de una "vaina" en la cual se introduce un gas a alta presión; de esta forma, si alguien pretende acceder al cable producirá una fuga de gas y una baja de presión dentro de la mencionada vaina. Al detectarse una baja de presión se dispara una alarma que permite determinar con precisión el lugar exacto de la fuga.

## Comparación de las topologías básicas

En el siguiente cuadro se resumen algunas de las características que distinguen a las tres topologías básicas.

	Bus lineal	Estrella	Anillo
Falla de una computadora Cableado defectuoso	No afecta la red Falla la red Difícil de aislar la falla	No afecta la red No afecta la red. La falla es fácil de aislar	Falla la red Falla la red Falla difícil de aislar
Longitud del cableado	Menor cantidad de metros de cable	Máxima cantidad de metros de cable	Intermedia cantidad de metros de cable
Nodos: Activos / Pasivos Estabilidad del rendimiento	Pasivos Diminuye al aumentar el número de nodos	Pasivos Diminuye al aumentar el número de nodos	Activos Relativamente estable al aumentar el número de nodos
Dificultad al agregar nodos Terminadores Fallas en el punto central	Intermedia Sí usa. No tiene	Muy fácil No usa. Si falla el Hub, falla la red.	Intermedia No usa. No usa / falla la red (en el caso que use MAU)
Costo	Muy bajo	Bajo (los hub han bajado de precio)	Medio - Alto

"Comparación de topologías básicas" | Elaboración DEPROE, IES siglo21

## Topologías básicas de redes wireless o WLAN

En las redes Wireless existen dos tipos de topologías básicas: topología AD-HOC y topología de Infraestructura.

### Topología AD-HOC

En esta topología, los dispositivos inalámbricos (sus tarjetas de red) son los que crean la red LAN. Cada host o nodo de la red se comunica en forma **peer to peer** con los otros dispositivos que se quieren conectar, todo esto sin necesidad de pasar por un equipo concentrador o Acces Point.

Las redes Ad-Hoc sólo pueden ser inalámbricas, por lo que deberá tener una tarjeta de red de este tipo en cada equipo que desee conectar.



"Red AdHoc" | [http://3.bp.blogspot.com/\\_4RDZ7e94K78/TPaDLAjUb2I/AAAAAAAAC/2aD0MyeYDaY/s1600/Inalambrica.JPG](http://3.bp.blogspot.com/_4RDZ7e94K78/TPaDLAjUb2I/AAAAAAAAC/2aD0MyeYDaY/s1600/Inalambrica.JPG)

Para poder armar una red de esta topología, solo necesitamos utilizar el mismo SSID \* 7.2 para todo los nodos y no sobrepasar una cantidad razonable de dispositivos (Windows 7 recomienda máximo 9 equipos), lo cual reduce significativamente el rendimiento de la red.

Para configurar una red así en Windows7:

Vaya a Panel de control\Redes e Internet\Centro de redes y recursos compartidos

Haga clic en Administrar redes inalámbricas, en el menú elija Agregar

## ¿Cómo desea agregar una red?



### Crear un perfil de red manualmente

Esta acción crea un perfil de red nuevo o ubica una red existente y guarda un perfil de red en el equipo. Necesita saber el nombre de red (SSID) y la clave de seguridad (si fuera necesaria).



### Crear una red ad hoc

Esta acción crea una red temporal para compartir archivos o una conexión a Internet

"Crear una red Ad Hoc" | Sistema Operativo Microsoft Windows 7

Haga clic en Crear una red ad hoc, haga clic en Siguiente y, a continuación, siga los pasos del asistente.

Deberemos darle nombre a la red, elegir una opción de seguridad colocando una clave de seguridad para nuestra red y ya estará configurada para que otros usuarios puedan conectarse a nuestra red Ad-Hoc.

Si desea seguir un tutorial para aprender a configurar una red Ad Hoc y compartir internet a través de ella, le recomiendo este video:

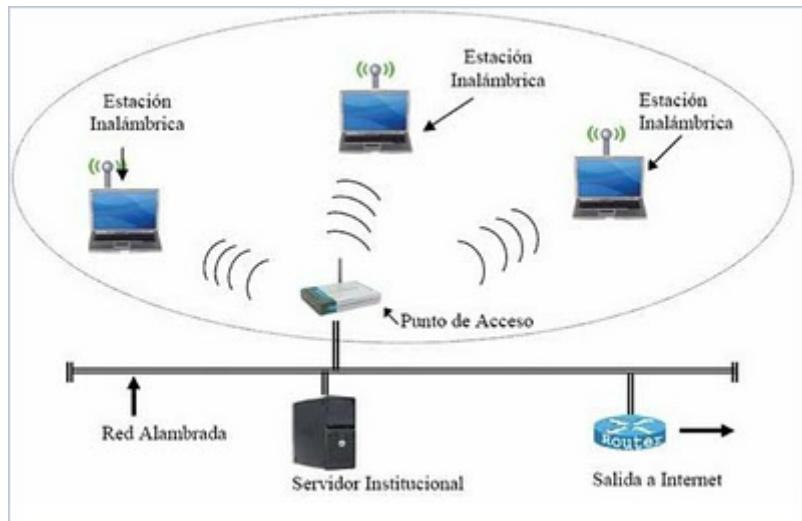
Si desea seguir un tutorial para aprender a configurar una red Ad Hoc y compartir internet a través de ella, le recomiendo el siguiente: <http://www.youtube.com/watch?v=KIW-7MHyf90>

Esta topología es muy útil en entornos de trabajo de pocas computadoras, sobre todo si no necesitan conectarse a otra red. Si bien se puede configurar de alguna de ellas para acceder a otras redes, como por ejemplo a internet, esto no se recomienda para usarlo frecuentemente como sería el trabajo en una oficina. Si se puede utilizar por ejemplo para compartir archivos entre los nodos disponibles en un determinado momento.

Por su naturaleza descentralizada, se hace más adecuada en aquellas situaciones en las que no puede confiarse en un nodo central. Son también útiles en situaciones de emergencia, como desastres naturales al requerir muy poca configuración y permitir armar una red muy rápido.

## Topología de infraestructura

En esta topología, se utiliza un concentrador denominado Punto de Acceso o Access Point para enlazar al resto de las estaciones inalámbricas o nodos. Si lo comparamos con las redes cableadas, funciona en forma similar a un switch o a un router.



"Topología de Infraestructura" |

<http://3.bp.blogspot.com/-bWFg11cCvQ4/TWNZqJzAWI/AAAAAAAABI/1UC8Qw8zEnY/s400/infraa.JPG>

El Access Point funciona encaminando las tramas hacia una red convencional o hacia otras redes distintas. En el primer caso actúa como Switch y en el segundo como Router (verá en detalle estos las características y diferencias en estos equipos en la SP11).

En este tipo de redes, para poder establecer la comunicación, todas las computadoras deben estar dentro del radio de cobertura del Acces Point.

Si no dispone de un equipo Acces Point puede utilizar alguna máquina antigua como por ejemplo una 586, Pentium o Pentium II corriendo alguna versión de Linux como Linuxap, Openap u otras.

## Otro problema de seguridad...

Muchas redes wireless o WLAN son instaladas en forma muy rápida, y suele suceder que los instaladores novicios en su afán de hacerlo rápidamente suelen omitir la seguridad convirtiendo así a estas redes en redes abiertas.

Si a esto le agregamos que todos los Acces Point del mercado vienen de fábrica con la misma configuración predeterminada para cada modelo y esta es fácilmente encontrada en internet, tenemos muchas redes abiertas a merced de potenciales administradores que pueden "adueñarse" de la administración del Acces Point. Es importante conocer que si este intruso cambia las claves de acceso, todos los equipos poseen un botón de "reset" al cual se puede recurrir en caso de tener que recuperar su administración.

Suponiendo que Ud. tenga controlado lo anterior, además existen muchas alternativas para mejorar la seguridad de las redes de este tipo. Las más usuales son la utilización de protocolos de cifrado como WEP, WPA o WPA2 que codifican la información transmitida para proteger su confidencialidad. WPA2 es el protocolo más seguro para redes Wireless en este momento, ya que realiza un proceso llamado handshake de cuatro vías (veremos en detalle el Handshake en la SP10), pero requiere que el hardware y el software de cada nodo sea compatible.

Además los equipos Acces Point nos permiten hacer un filtrado MAC, cosa que es muy recomendable estableciendo permiso de acceso solamente a aquellos dispositivos autorizados.

También se puede ocultar el punto de acceso, para que sea invisible para usuarios no deseados.

# REFERENCIAS 7

## 7.1 : Terminador



## 7.2 : SSID

SSID: Service Set Identifier es un código de 32 bits que se incluye en todos los paquetes de la red inalámbrica para identificar los paquetes como pertenecientes a esa red y no a otra. Más comúnmente conocido como "el nombre de la red wireless".



¿Te animás a medir cuánto aprendiste?

**1. Indique la opción correcta**

En la topología bus, todas las computadoras se conectan a un mismo medio físico de transmisión a través de sus correspondientes placas de red.

- Verdadero
- Falso

**2. Indique la opción correcta**

Los Hubs tienen capacidad de direccionamiento.

- Verdadero
- Falso

**3. Indique la opción correcta**

En la topología anillo, el cableado vincula a todos los nodos, de tal forma que cada nodo se encuentra conectado a otros dos, razón por la cual no hay extremos de línea ni terminadores.

- Verdadero
- Falso

**4. Indique la opción correcta**

¿Cuál de las siguientes NO es un tipo de topología básica de las redes?

- Topología de Bus.
- Topología de Estrella.
- Topología de Anillo o Ring.
- Topología de Estrella en Bus.

**5. Indique la opción correcta**

¿En qué topología los extremos del cable o backbone no se unen entre sí, y sus extremos están conectados a terminadores?

- Topología de Bus.

- Topología de Estrella.
- Topología de Anillo o Ring.
- Topología de Estrella en Bus.

**6. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

En la topología de Bus se utilizan  
En la topología de Estrella se utilizan  
En la topología de Anillo se utilizan

Terminadores  
Concentradores del tipo MAU  
Concentradores del tipo Hub o Switch

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

En la topología bus, todas las computadoras se conectan a un mismo medio físico de transmisión a través de sus correspondientes placas de red.

- Verdadero
- Falso

## 2. Indique la opción correcta

Los Hubs tienen capacidad de direccionamiento.

- Verdadero
- Falso

## 3. Indique la opción correcta

En la topología anillo, el cableado vincula a todos los nodos, de tal forma que cada nodo se encuentra conectado a otros dos, razón por la cual no hay extremos de línea ni terminadores.

- Verdadero
- Falso

## 4. Indique la opción correcta

¿Cuál de las siguientes NO es un tipo de topología básica de las redes?

- Topología de Bus.
- Topología de Estrella.
- Topología de Anillo o Ring.
- Topología de Estrella en Bus.

## 5. Indique la opción correcta

¿En qué topología los extremos del cable o backbone no se unen entre sí, y sus extremos están conectados a terminadores?

- Topología de Bus.
- Topología de Estrella.
- Topología de Anillo o Ring.
- Topología de Estrella en Bus.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

En la topología de Bus se utilizan  
En la topología de Estrella se utilizan  
En la topología de Anillo se utilizan

Concentradores del tipo Hub o Switch  
Concentradores del tipo MAU  
Terminadores

# SP5 / H2: Nivel físico Ethernet

Al nivel físico se lo subdividió en dos subniveles:

- El de señalización física
- El de acoplamiento al medio

Puede estar montado sobre coaxial, par trenzado, fibra óptica, o microondas. Permite trabajar en banda ancha o banda base.

La longitud del bus, llamado Segmento, está limitada por el tipo de medio físico utilizado, y por las características del protocolo CSMA/CD. Es importante recordar que, de acuerdo con este protocolo, se producen "colisiones", las que deben ser detectadas, y para ello es necesario que la estación pueda escuchar su propia trama (Collision Detection).

Pueden conectarse más de un segmento a través de repetidores (los Hub y Switch hacen de repetidores). Estos repetidores regeneran la señal y la retransmiten a través de los segmentos conectados a ellos.

Existe una regla práctica, conocida como la "Regla 5 – 4 – 3 – 2 – 1". Ésta es una regla de uso práctico, pero no siempre tiene validez. La misma dice:

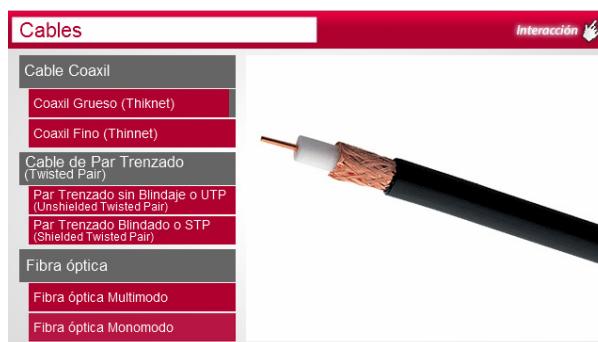
5. Segmentos
4. Repetidores
3. Segmentos con host
2. Segmentos de enlace (sin host)
1. Dominio de colisión

Para mantener una adecuada calidad de señal a 10 Mbps, y para permitir que el protocolo detecte colisiones, la máxima longitud de un segmento está limitada según el medio físico, como veremos más adelante.

Un repetidor está formado, en esencia, por dos tranceptores (*transceiver*) unidos consecutivamente y conectados a dos segmentos diferentes de cable. El repetidor pasa señal digital en ambas direcciones, amplificando y regenerando dicha señal, cuando pasa a través de ellos.

El máximo camino de transmisión entre dos estaciones cualesquiera consiste de cinco segmentos uni-dos por repetidores.

Los tipos de cable principales son:



Interactiva "Calbes"

Cable Coaxial

Coaxial Grueso (Thiknet)  
Coaxial Fino (Thinnet)  
Cable de Par Trenzado (Twisted Pair)  
Par Trenzado sin Blindaje o UTP (Unshielded Twisted Pair)  
Par Trenzado Blindado o STP (Shielded Twisted Pair)  
Fibra óptica  
Fibra óptica Multimodo  
Fibra óptica Monomodo

IES siglo 21 elaboración propia

Si bien, en principio podría utilizarse cualquier tipo de cable para establecer las topologías básicas, la industria y el criterio de las autoridades normativas han establecido ciertos estándares basados en parámetros tales como velocidad de transferencia, seguridad, longitud de los cables, facilidad de instalación, etc.

Los **estándares de Red** (*Network Standards*) definidos son normativas que tratan acerca de la performance y requerimientos de **todos los elementos de una red**, por ejemplo: IEEE 802, ATM Forum u otros.

A continuación, veremos con detalle las características de cada tipo de cable definidos por IEEE 802.3, los más utilizados en las redes LAN actuales.

## IEEE 802.3 10Base5 (Thicknet) Original de Ethernet

El primer medio utilizado por Ethernet fue un coaxial rígido, conocido como coaxial grueso o "thicknet". Este cable se amuraba en las paredes y, a través conectores especiales, llamados vampiros (vampire taps), por su característica de "morder" la cubierta aislante del cable y traspasar la malla de protección del coaxial y hacer contacto con el conductor central de cobre. De este conector se accedía, por medio de un cable flexible de pares de cobre, y se conectaba a la estación a través de un conector AUI (Adapter Universal Interface), que consiste de un conector DB15, como puede verse en la figura siguiente.



### Características del Coaxil Grueso (Thicknet)

- Longitud del cable limitada a 2,5 km, no más de 4 repetidores entre estaciones.
- Menos de 500 metros por segmento.
- Cada segmento puede contener un máximo de 100 nodos (*transceivers*).
- Los Taps deben ser ubicados en múltiplos de 2.5 metros (mínimo).

## Nomenclatura del cable Thicknet – 10Base5:

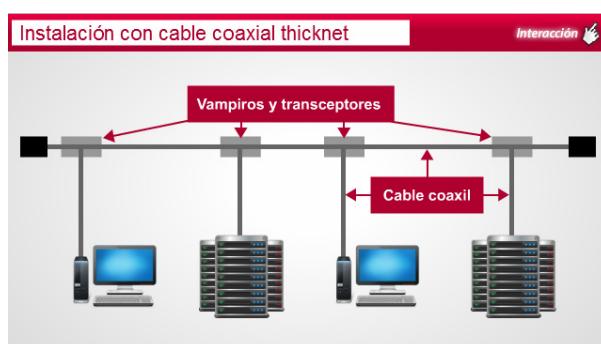
10 Megabits por segundo.

Baseband transmission (Transmisión Banda Base).

500 Metros. Longitud máxima del segmento.



En la figura que viene, se puede ver una instalación realizada con cable coaxial thicknet, en la misma pueden visualizarse los segmentos de cable 10Base5, los conectores Vampiros con los respectivos transceptores y los cables de bajada hasta la estación.



Interactiva "Instalación con cable coaxial thicknet"

IES siglo 21 elaboración propia

## IEEE 802.3 10Base2 (Thinnet o Cheapernet)

El comité 802.3 elaboró luego un suplemento económico al estándar, conocido como "Cheapernet". Este suplemento definió una interfase menos costosa para un cable coaxial delgado. La velocidad de datos se mantiene a 10 Mbps, pero debido a esta interfase barata y al cable delgado, cada segmento está limitado a 185 metros.

Cable especial de 50 ohm fue desarrollado para usar exclusivamente en redes Ethernet.

A continuación damos algunas de las características de este cable:

- Alta velocidad de propagación: aproximadamente "0,77C", donde "C" es la velocidad de la luz en el vacío.
- Baja impedancia de transferencia: ésta es necesaria tanto para prevenir señales no deseadas (por ejemplo, interferencias de estaciones de radio, etc) y para mantener las señales de radiación fuera del cable.
- Flexibilidad: este cable permite una fácil instalación.
- Marca e impedancia: la envoltura más externa es despojada de marcas de conexión para prevenir desigualdades del cable en esos puntos. La conexión dentro del cable no es igual, pero produce un puente de alta impedancia.

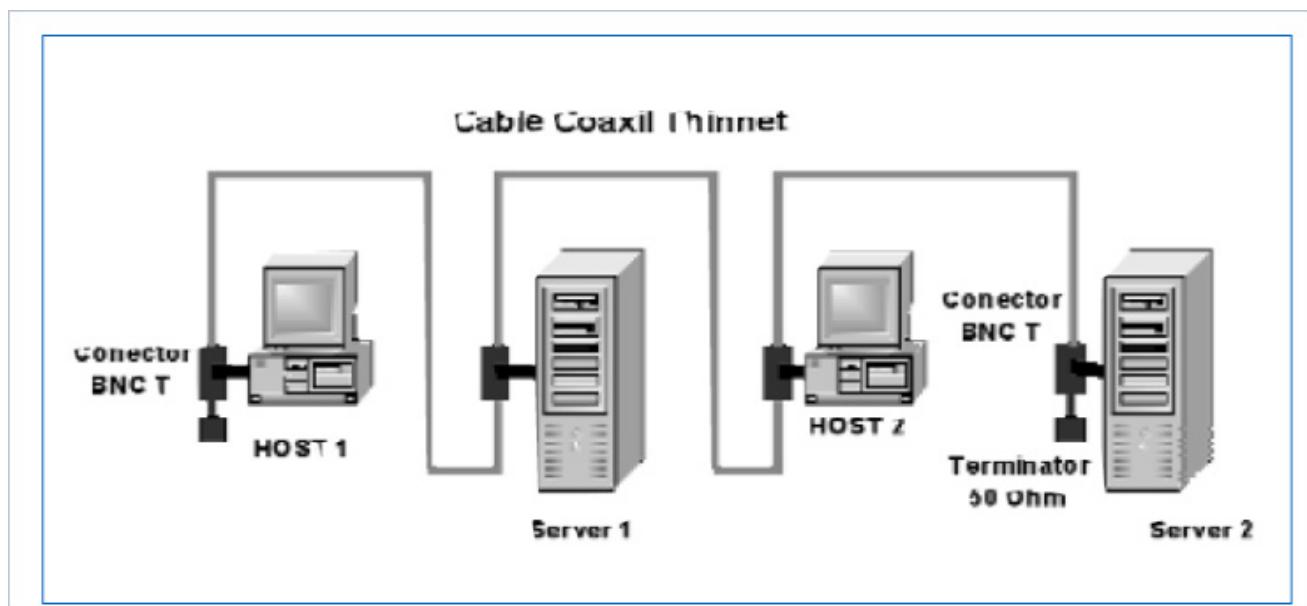
## Características del Coaxial Fino (Thinnet)

El cable Coaxil fino (Thinnet coax) se puede implementar bajo la normas RG58/U (núcleo sólido de cobre) o RG58 A/U (núcleo trenzado de cobre), ambas con una impedancia de 50 ohms.

- Conectores BNC y BNC "T".
- Segmento de 185 metros (606 pies).
- Máximo 30 estaciones por segmento.
- Los segmentos llevan un terminador de 50 Ohms en cada extremo.
- Mínima distancia entre nodos: 0,5 metros.
- Puesta a tierra en un único punto.
- 10 Megabits por segundo.
- *Baseband transmission* (Transmisión Banda Base).
- 185 Metros Longitud máxima del segmento.
- Adecuado para pequeñas áreas, con poca cantidad de usuarios

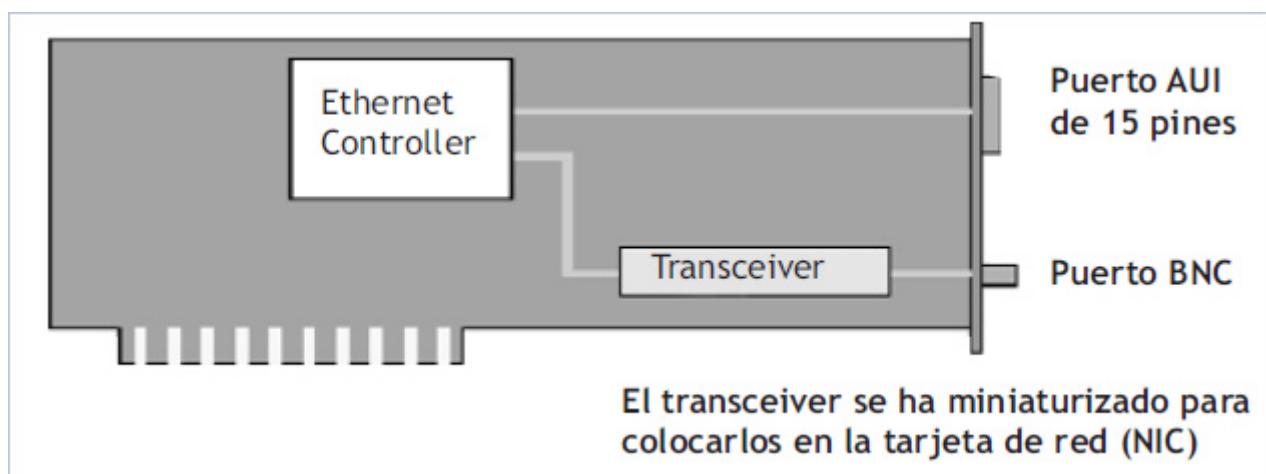
En general, el cable coaxial se utiliza en la topología de Bus Lineal y como elemento de interconexión entre hub. En la actualidad, los hub con puertos BNC para cable coaxial han dejado de utilizarse, pero todavía puede encontrar algunos instalados y funcionando, sobre todo en lugares grandes como las fábricas, donde las distancias son grandes la instalación de este tipo de cables fue ventajoso debido a las distancias, los costos y la protección que posee su malla contra efectos electromagnéticos.

En la figura que sigue, se puede ver una instalación realizada con cable coaxial thinnet de 50 ohm y conectores BNC tipo T. Pueden visualizarse también los terminadores de 50 Ohm para eliminar el "eco" de la señal.



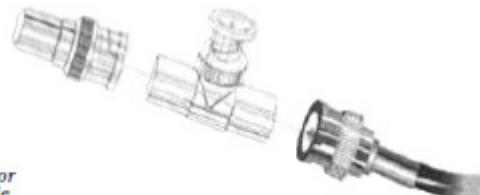
## Componentes Thinnet (10Base2)

En la figura, pueden verse las características de una tarjeta de red para 10Base2. Como se observa es muy simple en cuanto a los componentes, y de allí su bajo costo.

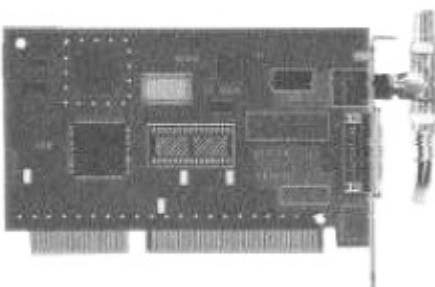




Cable coaxial 10Base2 de 50 Ohm



En este dibujo, vemos el terminador, el conector T y el conector BNC con más detalle.



Observar cómo se conecta el cable coaxil a la placa de red. Puede verse el terminador, el conector T y el BNC.



Conjunto de elementos BNC para utilizar con cable coaxil

Como usted observa en las imágenes anteriores, la placa de red se conecta al cable del bus mediante un conector T. Si la computadora en cuestión se encuentra en el extremo del bus, una de las patas de la T deberá tener conectado un terminador. La otra salida se conecta al cable mediante un conector BNC. Si no estuviera en el extremo, ambas salidas la conectarían al cable del bus.

## IEEE 802.3 10BaseT

### Cable de Par Trenzado (Twisted Pair)

A fin de compatibilizar los cableados de edificios, dos organizaciones (TIA/EIA), dieron comienzo al estudio para implementar estándares que permitieran transmitir voz y datos por el mismo tipo de cable. Por esta causa, cuando estudiemos el cableado, veremos que a simple vista, los cables UTP y sus conectores son similares a los "cables comunes de teléfono", salvo algunas diferencias que parecen mínimas, pero que no lo son.

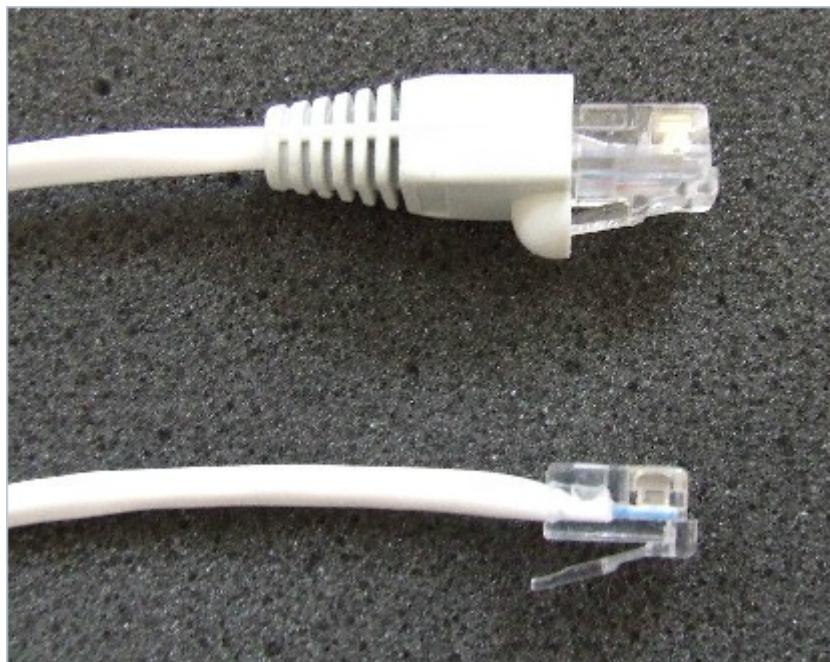
Los cables UTP se utilizan en la topología de estrella con hub o switch, con bocas o puertos de conexión tipo RJ45 hembra en los cuales se introduce el extremo del cable que es RJ45 macho (como puede observar en las figuras siguientes). El cable de conexión consta de dos extremos RJ45 macho. La placa de red posee un extremo RJ45 hembra. En un esquema muy sencillo, el cable UTP se extiende desde la placa de red hasta el puerto del hub. A continuación se describen las características más importantes del cableado estructurado.

## Cable UTP – Pares trenzados sin protección

El conector más grande es el RJ45 adecuado para UTP. El más chico, RJ11, es el conector de telefonía que se utiliza normalmente (es el que tiene en su casa). A estos conectores, por ser los que se insertan se los denomina RJ45 macho o también RJ45 Plug.



"RJ11 RJ45" | [http://meteo.milliflora.com/images/met\\_img\\_rj11rj45.jpg](http://meteo.milliflora.com/images/met_img_rj11rj45.jpg)



"RJ45 11" | <http://www.run-it-direct.co.uk/images/RJ45toRJ11.JPG>

El siguiente es el conector RJ45 que está diseñado para recibir la inserción de los anteriores, se los denomina RJ45 hembra o Jack RJ45. Notará que tiene la indicación de como conectar los cables según se quiera respetar la norma EIA/TIA 568 A o B.



"RJ45" | [http://www.morrisproducts.com/images/88020\\_l.jpg](http://www.morrisproducts.com/images/88020_l.jpg)

- Aprobado por IEEE 9/90.
- Protocolo CSMA/CD.
- Compatible con 10BASE5 y 10BASE2.
- Emula la topología bus mediante Hub/Switch.
- El cableado en Estrella simplifica la instalación y la localización de averías.
- Mejora la tolerancia a fallas.
- 10/100/1000 Megabits por segundo.
- Baseband transmission (Transmisión Banda Base).
- Twisted Pair.

En la siguiente imagen puede observar el cable UTP



"UTP" |

[http://www.szmaizhong.com/uploadfile/k4/ktcable2834/product/cat6-cable-\(utp-ftp-stp-sftp\)/305M-UTP-Cat6-Communication-Cable-1332744172-0.jpg](http://www.szmaizhong.com/uploadfile/k4/ktcable2834/product/cat6-cable-(utp-ftp-stp-sftp)/305M-UTP-Cat6-Communication-Cable-1332744172-0.jpg)

## Las categorías de UTP

Las [especificaciones 568 de la Asociación de Industrias Electrónicas e Industria de las Telecomunicaciones \(EIA/TIA\)](#) especifican el tipo de cable UTP que se utilizará en cada situación. Para esto se clasificó en categorías, de las cuales a continuación resumimos las características principales:

- Categoría 1

Funciona a 0,4 MHz, puede transportar voz pero no datos. Cable utilizado para telefonía. No se recomienda utilizarlo en la actualidad.

- Categoría 2

Funciona a 4 MHz, consiste en 4 pares trenzados. Es capaz de transmitir datos hasta 4 Mbps. No se

recomienda utilizarlo en la actualidad. Hasta esta categoría no están descriptas en la norma 568.

- Categoría 3

Funciona a 16 MHz, consiste en 4 pares trenzados a razón de 1 giro cada 10 cm. Es capaz de transmitir datos hasta 16 Mbps. No se recomienda utilizarlo si se necesita transmitir datos a más de 16 Mbps. A partir de esta categoría, están descriptas en la norma 568

- Categoría 4

Funciona a 20 MHz, consiste en 4 pares trenzados. Es capaz de transmitir datos hasta 16 Mbps. No se recomienda utilizarlo si se necesita transmitir datos a más de 16 Mbps. Utilizado en la topología Token Ring.

- Categoría 5

Funciona a 100 MHz, consiste en 4 pares trenzados a razón de 1 a 2 giros por cada 1cm. Es capaz de transmitir datos hasta 100 Mbps. Desarrollado para Fast Ethernet

- Categoría 5e

Funciona a 100 MHz, es capaz de transmitir datos hasta 1000 Mbps. El cable es como el de la categoría 5 pero con mejores controles de calidad que lo hacen apto para Gigabit Ethernet.

- Categoría 6

Especificado para redes de alta velocidad de hasta 1000 Mbps (1 Gbit/s) Gigabit Ethernet. [No es un estándar TIA](#).

También esta especificada la categoría 6e propuesta para ser incluida en las especificaciones ISO/IEC 11801 y la categoría 6STP (protegida) que puede ser utilizada tanto en redes Ethernet como también en Token Ring

- Categoría 7

Similar a la categoría 6, [no es un estándar TIA](#). Supera en velocidad a la categoría 6 pero requerirá probablemente nuevos conectores en vez del RJ-45. La versión 7f está propuesta para ser incluida en las especificaciones ISO/IEC 11801

## Más información sobre el Sistema de Cableado UTP

Existen diversas normas de aplicación al cableado en UTP, cronológicamente tenemos:

- IEEE 803.5j: Referida a la utilización de UTP para redes Token Ring.
- IEEE 802.3i: Denominada usualmente Ethernet 10BaseT, para uso de UTP para redes Ethernet
- EIA/TIA 568: Estándar para cableado de telecomunicaciones en edificios comerciales.

El objetivo de la norma fue el de definir un cableado que soporte un entorno multiprotocolo y multiproveedor, como así también, el de ofrecer una guía para el diseño de equipos y nuevos productos ofrecidos, los que deberían funcionar adecuadamente.

La norma define una estructura general, comenzando desde el puesto de trabajo. Para ello establece que el mismo debe tener dos conexiones, llamado cableado horizontal, con un armario de telecomunicaciones en donde se encuentran los equipos de telecomunicaciones.

En cualquiera de los casos, el cable debe tener un solo tramo.

Las dos conexiones son:

1. Una, para telefonía, debe utilizar el mismo cable UTP de cuatro pares.

2. La otra, para datos, está compuesta por tres tipos de cables distintos:

- a. UTP de cuatro pares. Ésta es la única usada actualmente.
- b. STP que es un cable de pares blindados, también conocido como cable Tipo I.
- c. Coaxial de 50 ohms.

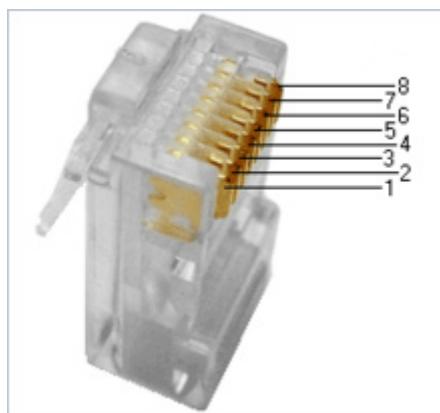
La instalación de fibra óptica es opcional y adicional a los vínculos anteriores.

## El conector RJ45

En la figura que sigue, puede verse la estructura del conector RJ45, tanto el macho (lado del cable), como la hembra o Jack que se inserta en la caja de la pared (roseta).

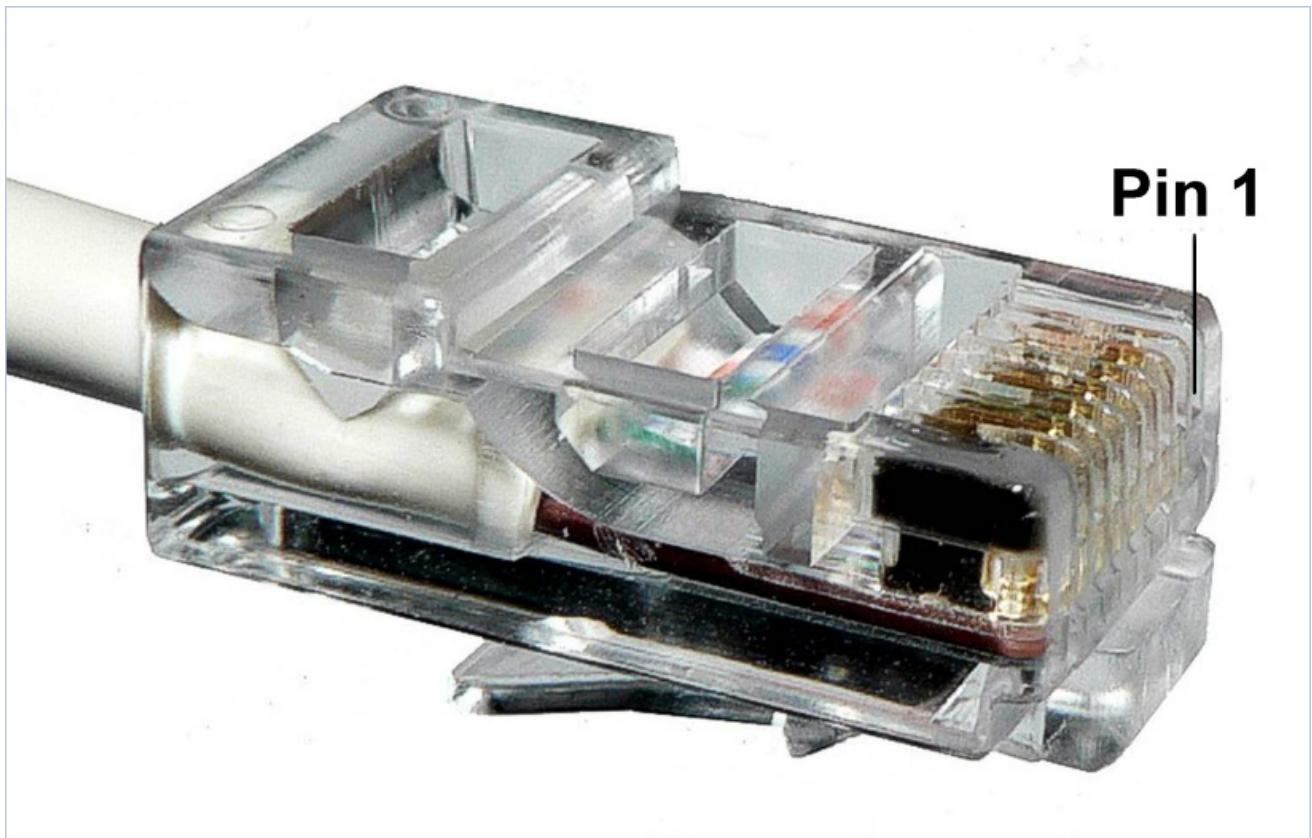
El conector está formado por una serie de pines o contactos (8, en total), numerados de izquierda a derecha, como se indica en la figura. Según la norma TIA/EIA 568, esos pines tienen una forma de conexión, conocido como *pinups*. El detalle se verá más adelante.

Para el conector RJ45 macho o RJ45 Plug los pines de conexión se numeran del 1 al 8 como muestran las imágenes:

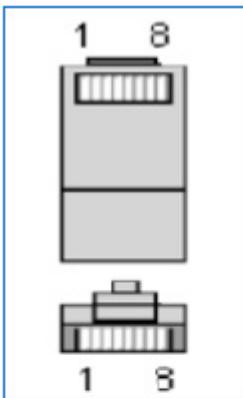


"Posicion de los pines" |

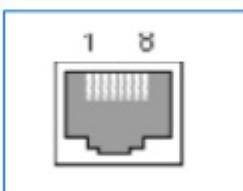
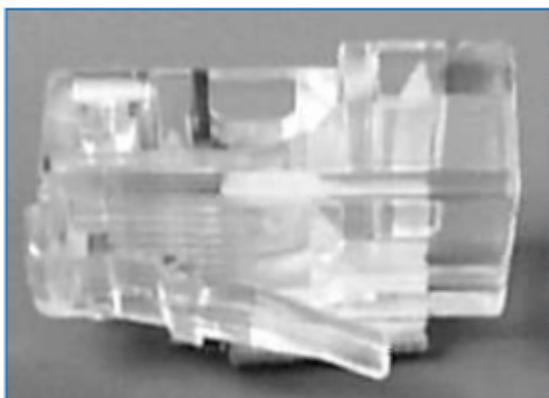
<http://upload.wikimedia.org/wikipedia/commons/thumb/3/36/Rj45plug-8p8c.png/220px-Rj45plug-8p8c.png>



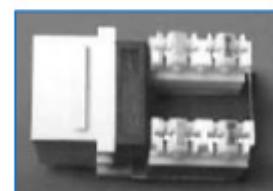
"RJ 45 Plug" | [http://4.bp.blogspot.com/-Kou5MV5IJTk/T-SMpBAJUwl/AAAAAAAAGc/x3cykyIFyA4/s1600/RJ-45\\_connector.jpg](http://4.bp.blogspot.com/-Kou5MV5IJTk/T-SMpBAJUwl/AAAAAAAAGc/x3cykyIFyA4/s1600/RJ-45_connector.jpg)



Conecotor RJ45 Macho  
(Lado del cable)

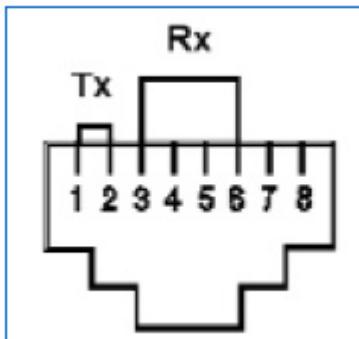


Conecotor RJ45 hembra  
correspondiente a Placas de Red (NIC) y Hub



Vista superior del Jack

Vista frontal del Jack



10BaseT usa los pines 1-2 / 3-6  
Compatible con los patrones de  
cableado  
TIA568A y TIA 568B

## Recomendaciones

Se recomienda especificar las instalaciones nuevas de cableado para cumplir con los requisitos mínimos de:

ANSI/TIA/EIA-568-A-5 Transmission Performance Specification for 4 pair 100 Ohm category 5e y sus grupos y trabajos asociados.

EIA/TIA-568-B Commercial Building Telecommunication Cabling Standard y sus grupos y trabajos asociados.

EIA/TIA-606-A Administration Standard for telecommunication Infrastructure of Commercial Building.

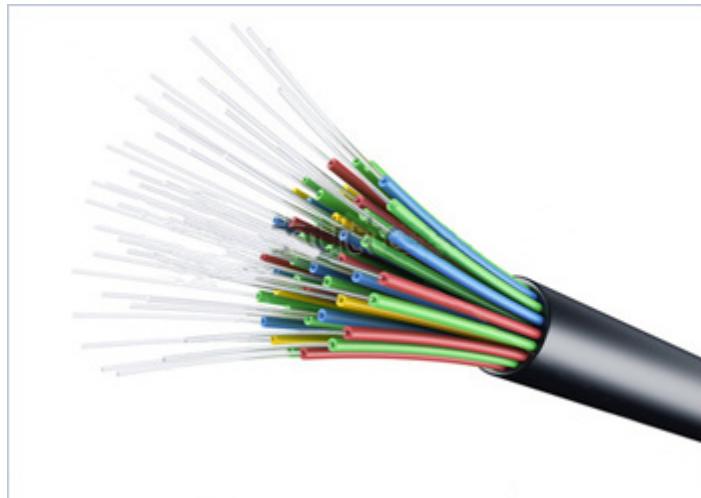
ISO/IEC 11801 "Generic cable form customer premises".

Se recomienda especificar 5e pues es capaz de transmitir de forma estandarizada a 100 Mbps (velocidad que hoy en día aún se considera más que suficiente) y en caso de requerirse puede lograr 1000 Mbps respetando ciertos requisitos adicionales.

El estándar EIA/TIA 568A define al cableado estructurado para edificios comerciales y fue actualizado por el estándar EIA/TIA 568B, debido a las altas prestaciones exigidas últimamente a los cables de pares cruzados y a la popularización del uso de los cables de fibra óptica, que han conllevado cambios en el estándar gracias a la contribución de más de 60 organizaciones incluyendo fabricantes, usuarios finales y consultoras.

## Fibra Óptica

Es un medio de transmisión utilizado en redes por el que se envían pulsos de luz que representan los datos. La fuente de luz puede ser laser o LED y esta se propaga por el interior de una fibra de vidrio (o también materiales plásticos con las mismas propiedades).



"Fibra-optica" | <http://teltelecom.com/images/fibra-optica.png>



"Hilos fibra óptica" |

<http://4.bp.blogspot.com/-dJujZhTrNAQ/T2oMhl2e7YI/AAAAAAAAB3A/2bol21NNY-s/s1600/Cable+Fibra+Optica.jpg>

Eso permite enviar gran cantidad de datos a grandes distancias con velocidades superiores a las del cableado convencional. Además son un excelente medio de transmisión pues son inmunes a las interferencias electromagnéticas que producen efectos indeseados (ruido) sobre los cables convencionales.

La utilización que particularmente nos interesa es sobre las redes locales (LAN) donde aprovecharemos las ventajas que brinda frente a los otros medios de transmisión.

## Tipos

El haz de luz en el interior de una fibra puede seguir diferentes trayectorias. Estas se denominan modos de propagación.

Según el modo de propagación podemos clasificarlas en dos tipos:

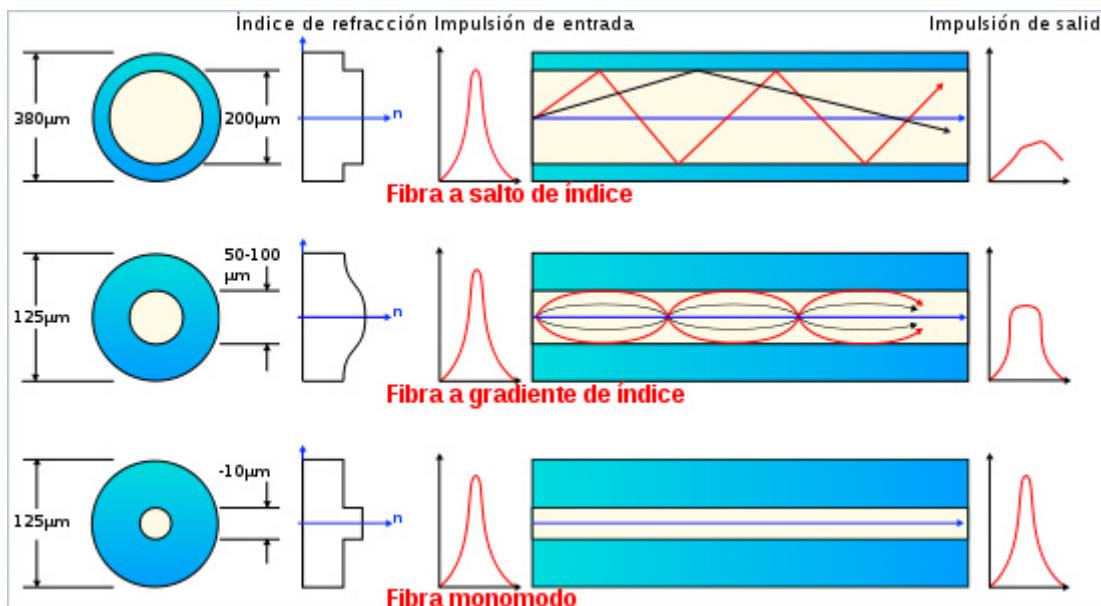
- **Fibra Óptica Multimodo**

Es una fibra óptica en la que los haces de luz pueden propagarse por más de un modo o trayectoria. Estas se utilizan en aplicaciones de corta distancia porque es económica y simple de instalar. Debido a que está fabricada con un núcleo relativamente grande (en comparación con la monomodo) su instalación y conectación es sencilla.

Según el índice de refracción del núcleo, tenemos **dos subtipos**:

**Índice escalonado o a saltos:** en este tipo de fibra el núcleo, al tener el mismo índice de refracción en toda su longitud genera saltos o escalones de refracción que producen a la salida una señal con alta dispersión.

**Índice gradual o gradiente:** en este tipo de fibra el núcleo está construido con distintos materiales de distinto índice de refracción en toda su longitud que producen a la salida una señal con menor dispersión.



"Fibra óptica multimodo y monomodo" |

[http://3.bp.blogspot.com/-H\\_6sjw6UbWA/UFa49X-TuLI/AAAAAAAFAw/TSNyefiWXOo/s1600/550px-Fibra\\_optica.svg.png](http://3.bp.blogspot.com/-H_6sjw6UbWA/UFa49X-TuLI/AAAAAAAFAw/TSNyefiWXOo/s1600/550px-Fibra_optica.svg.png)

#### • Fibra Óptica Monomodo

Es una fibra óptica en la que sólo es posible que se propague un modo de luz (sólo una trayectoria). Esto se obtiene reduciendo el tamaño del núcleo para que sólo permita un modo de propagación. De esta forma produce a la salida una señal con muy baja dispersión, lo cual permite alcanzar grandes distancias y transmitir a gran velocidad.

Si bien con la fibra óptica se pueden alcanzar hasta 400 km de distancia y decenas de Gbps en velocidad de transmisión, en estas condiciones ya no estamos hablando de una LAN, por lo tanto los protocolos a utilizar serán los adecuados para otro tipo de redes (WAN)

En las redes LAN los estándares aplicados son los que se definen a continuación (IEEE 802.3 10Base FL, IEEE 802.3 100Base FX y IEEE 802.3 1000BaseX) cada uno con sus características principales.

## IEEE 802.3 10BaseF

10 Base F es el nombre que le ha dado el IEEE a una familia de implementaciones a nivel físico de la arquitectura 802.3 (popularmente conocido como Ethernet)

El número 10 hace referencia a la velocidad de transmisión (10 Mbps), Base se refiere a que transmite la señal en la banda base (una sola frecuencia) y F se refiere al medio de transmisión (Fibra Óptica)

De la familia 10 Base F la más utilizada fue la 10 Base FL

## 802.3 10BaseFL

Sus características principales son:

- El medio de transmisión es una Fibra Óptica del tipo multimodo
- La Velocidad de transmisión máxima es de 10 Mbps

- La longitud máxima del segmento es de 2000 m
- La topología física sobre la que se implementa normalmente es del tipo Estrella

Como notará al leer las características, la utilización de esta tecnología permite el uso de la fibra óptica como medio de transmisión de 10 Mbps hasta 2 kilómetros por segmento, lo cual permite alcanzar a una LAN distancias que no serían posibles con la utilización de UTP ni coaxial.

### **IEEE 802.3 100BaseFX**

100 Base FX es el nombre que le ha dado el IEEE a la versión de Fast Ethernet sobre Fibra Óptica

El número 100 hace referencia a la velocidad de transmisión (100 Mbps), Base se refiere a que transmite la señal en la banda base (no hay múltiples de frecuencias), FX se refiere a que permite correr Fast Ethernet sobre Fibra Óptica

Sus características principales son:

- El medio de transmisión es una Fibra Óptica del tipo multimodo. Utiliza dos hebras de fibra por enlace.
- La Velocidad de transmisión máxima es de 100 Mbps
- La longitud máxima del segmento es de 2000 m transmitiendo Full Duplex.
- La topología física sobre la que se implementa normalmente es del tipo Estrella

Al leer las características, notamos que la utilización de esta tecnología permite el uso de la fibra óptica como medio de transmisión de 100 Mbps hasta 2 kilómetros por segmento, lo cual permite mantener las distancias alcanzadas en una LAN que alcanza 10 Base FL pero superando su velocidad de transmisión hasta 10 veces.

### **IEEE 802.3 1000BaseX**

Es una ampliación del estándar Ethernet (802.3ab y 802.3z del IEEE) que consigue una velocidad de transmisión de 1000 Mbps sobre Fibra Óptica.

Sus características principales son:

- El medio de transmisión es una Fibra Óptica. Utiliza dos hebras de fibra por enlace.
- La Velocidad de transmisión máxima es de 1000 Mbps
- La longitud máxima del segmento es de hasta 550 m transmitiendo en Fibra Óptica Multimodo (estándar denominado 1000BaseSX).
- La longitud máxima del segmento es de hasta 5000m transmitiendo en Fibra Óptica Monomodo (estándar denominado 1000BaseLX).

Esta tecnología permite el uso de la fibra óptica como medio de transmisión de 1000 Mbps o 1 Gbps, superando la velocidad de transmisión de 100BaseFX hasta 10 veces. Hay que tener en cuenta las distancias y el tipo de fibra óptica a utilizar, cuyas características se resumieron cuando vimos Fibra Ópticas Multimodo y Monomodo.



¿Estás listo para un desafío?

**1. Indique la opción correcta**

Los pinos utilizados en el conector RJ45 cuando se conectan cables UTP para las redes Ethernet son: 1-2 para Transmisión y 3-6 para Recepción.

- Verdadero
- Falso

**2. Indique la opción correcta**

La "Regla 5 – 4 – 3 – 2 – 1" indica: 5 Segmentos, 4 Repetidores, 3 Segmentos con host, 2 Segmentos de enlace (sin host) y 1 Dominio de colisión.

- Verdadero
- Falso

**3. Indique la opción correcta**

¿Cuál es la longitud máxima del segmento de cable UTP?

- 90 m.
- 185 m.
- 500 m.
- 2000 m.

**4. Indique la opción correcta**

¿Cuál es la máxima velocidad de transmisión de datos que soporta el cable Thinnet?

- 8 Mbps.
- 10 Mbps.
- 100 Mbps.
- 1024 Mbps.

**5. Indique la opción correcta**

¿Cuál es la longitud máxima de segmento del cableado Thicknet?

- 100 m.
- 185 m.
- 500 m.
- 2000 m.

**6. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

IEEE 802.3 10 Base 5  
IEEE 802.3 10 Base 2  
IEEE 802.3 10 Base T  
IEEE 802.3 10 Base F

Coaxil Thinnet  
Cable UTP  
Coaxil Thicknet  
Fibra Óptica

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Los pinos utilizados en el conector RJ45 cuando se conectan cables UTP para las redes Ethernet son: 1-2 para Transmisión y 3-6 para Recepción.

- Verdadero  
 Falso

## 2. Indique la opción correcta

La "Regla 5 - 4 - 3 - 2 - 1" indica: 5 Segmentos, 4 Repetidores, 3 Segmentos con host, 2 Segmentos de enlace (sin host) y 1 Dominio de colisión.

- Verdadero  
 Falso

## 3. Indique la opción correcta

¿Cuál es la longitud máxima del segmento de cable UTP?

- 90 m.  
 185 m.  
 500 m.  
 2000 m.

## 4. Indique la opción correcta

¿Cuál es la máxima velocidad de transmisión de datos que soporta el cable Thinnet?

- 8 Mbps.  
 10 Mbps.  
 100 Mbps.  
 1024 Mbps.

## 5. Indique la opción correcta

¿Cuál es la longitud máxima de segmento del cableado Thicknet?

- 100 m.  
 185 m.  
 500 m.  
 2000 m.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

- IEEE 802.3 10 Base 5  
IEEE 802.3 10 Base 2  
IEEE 802.3 10 Base T  
IEEE 802.3 10 Base F

- Coaxil Thinnet  
Cable UTP  
Coaxil Thicknet  
Fibra Óptica

## SP5 / H3: Estándares para el cableado

Un problema común a todo aquel que comience a planificar una instalación de una red es: qué tipo de cableado voy a utilizar?

¿Cuándo debo utilizar cada tipo de cable? ¿Puedo utilizar varios tipos distintos en una misma instalación?

Responderemos estas preguntas a continuación.

Los **estándares de cableado** definen en forma genérica la performance y calidad de los **cables, conectores y hardware** por ejemplo: ANSI/TIA/EIA 568-A, ISO IEC 11801.

Resumiremos en el cuadro siguiente los estándares TIA/EIA

### Estándares TIA/EIA

Estándar	Descripción
TIA/EIA - 568A	Estándar de cableado para telecomunicaciones en edificios comerciales.
TIA/EIA - 569A	Estándar de cableado para edificios comerciales, para recorridos y espacios de telecomunicaciones.
TIA/EIA - 570A	Estándar de cableado para telecomunicaciones residenciales y comerciales menores.
TIA/EIA - 606	Estándar de administración para la infraestructura de telecomunicaciones de edificios comerciales.
TIA/EIA - 607	Requisitos de conexión a tierra y conexión de telecomunicaciones para edificios comerciales.

"Estándares TIA/EIA" | Elaboración DEPROE, IES siglo21

## Armado del cable con UTP – Estándar TIA/EIA 568 A-B.

### Guía para cableado 10BaseT con UTP (Unshielded Twisted Pair)

Veremos a continuación como realizar el armado de un cable UTP:

#### Selección de la Categoría de Cable

En la actualidad, todas las redes utilizan Cableado Estructurado con Pares Trenzado sin Protección (*Unshielded Twisted Pair - UTP*), y eso es lo que nosotros discutiremos.

El proceso empieza con la selección de la categoría apropiada. Hoy básicamente se instala como mínimo UTP Categoría 5 y de ser posible Categoría 5e.

Nos aseguramos de este modo correr 100 Mbps y con factibilidad de 1000 Mbps de velocidad, ya que los requisitos de ensamblado de cables físicos son los mismos. A lo largo de este texto, nos referiremos a ambos como CAT5.

Cuando pide UTP CAT5 recibirá un cable que contiene 4 pares trenzado de cobre, un total de 8 alambres. Los cables pueden estar constituidos por un solo hilo o varios.

Normalmente se los conoce como sólidos o flexibles. Típicamente el sólido se usa para atravesar paredes y techos y el flexible para los cordones (patchcord) que va de la roseta de la pared a la computadora o los cables del patchpanel al Hub o Switch.

Es muy importante saber si la cubierta exterior del cable que contiene los 4 pares trenzados, es de calidad Plena o No Plena (*Plenum grade* o *Non-plenum grade*), ya que se refiere a los "códigos antiflama" o contra fuego, pero eso está fuera del alcance de esta guía.

## Los Pares

Los pares en el cable UTP están coloreados para que pueda identificar los distintos alambres. Estos colores están codificados para cada fin. En UTP CAT5 cada par de cables está compuesto de un alambre de color y el otro, de fondo blanco y una raya del mismo color.

El esquema de color utilizado en la actualidad es el Standard 568 (EIA/TIA 568).

La siguiente tabla muestra el esquema de colores de los distintos pares:

PAR	COLORES
Par N° 1	Blanco/Azul Azul
Par N° 2	Blanco/ Naranja Naranja
Par N° 3	Blanco/Verde Verde
Par N° 4	Blanco/Marrón Marrón



## Los conectores

Con UTP CAT 5 se usan normalmente conectores plug y jacks RJ45.

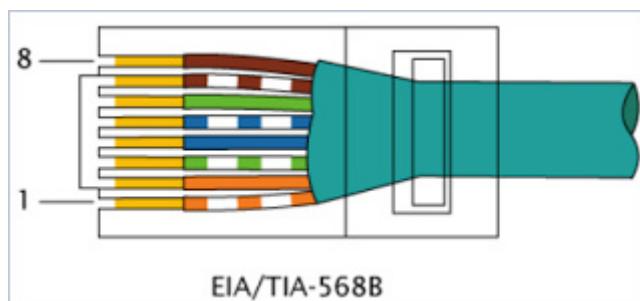
El plug se sujeta al cable y el jack es el dispositivo donde se inserta el conector en la roseta de la pared, la tarjeta de red NIC (Network Interface Card), el Hub o Switch.

Para los cables UTP, el conector en el puesto de trabajo debe ser un RJ45, efectuando el cableado según dos variantes funcionalmente idénticas, denominadas T568A y T568B, según la siguiente tabla.

EIA/TIA T568A (colores de los cables)	PIN	Función	EIA/TIA T568B (colores de los cables)
Blanco/Verde	1	TX+	Blanco/Naranja
Verde	2	TX-	Naranja
Blanco/Naranja	3	RX+	Blanco/Verde
Azul	4	Telefonía	Azul
Blanco/Azul	5	Telefonía	Blanco/Azul
Naranja	6	RX-	Verde
Blanco/Marrón	7		Blanco/Marrón
Marrón	8		Marrón

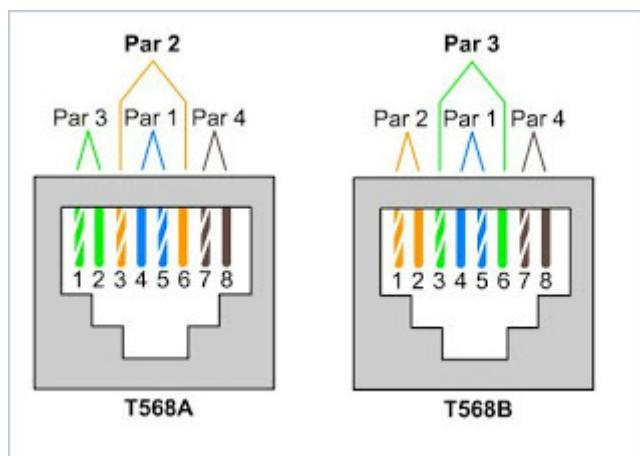
"Tabla indicadora de conectores" | Elaboración DEPROE, IES siglo21

Si bien ambas normas pueden usarse indistintamente, la más comúnmente usada fue la T568A. Hoy en día se utiliza más la T568B.



"EIA/TIA 568B" | [http://2.bp.blogspot.com/\\_QpIXYhOYRg/Sr5kqp\\_8UI/AAAAAAAFA4/hPeYhzsTaYg/s320/RJ-45\\_TIA-568B.png](http://2.bp.blogspot.com/_QpIXYhOYRg/Sr5kqp_8UI/AAAAAAAFA4/hPeYhzsTaYg/s320/RJ-45_TIA-568B.png)

Una instalación debe estar realizada completamente con una norma. Si se elige la Norma T568A, luego no puede cambiarse a la T568B, o hacer una parte de la instalación con una norma y la otra parte con otra.



"T568A y T568B" |

## Cable cruzado (Crossover)

Normalmente, los pares de Transmisión (TX) y de Recepción (RX) son intercambiados en el concentrador. Si no se un concentrador y se quieren conectar dos Host (Computadoras) por sus NIC (Network Interface Card), es necesario cruzar los pares, de manera que lo que es "transmisión" en un lado, sea "recepción" en el otro y viceversa.

En este caso deberá armarse un cable cruzado o "crossover". Este cable debe realizarse haciendo en un extremo el conexionado, según el estándar 568A y en el otro extremo, según 568B.

En la siguiente tabla puede verse cómo se cruzan los cables.

Nombre 568 A	NIC1	NIC2	Nombre 568 B
TX+	1	3	RX+
TX-	2	6	RX-
RX+	3	1	TX+
RX-	6	2	TX-

"Cables cruzados" | EIA/TIA 568B

Dentro de los casos contemplados en esta norma, cuando se utiliza UTP, los host se conectan a un concentrador. En la actualidad, cuando se habla de una LAN de UTP se piensa inmediatamente en un concentrador del tipo Switch, ya que los del tipo Hub ya han quedado en desuso.

Es importante hacer notar que en la actualidad tiende a confundirse a la Norma IEEE 802.3 con Ethernet, y escuchar frases (o verlas escritas en las cajas de las placas de red) como "Ethernet 10BaseT"; más allá de la confusión, esto no causa ningún problema.

## Armado de conector plug RJ45

A continuación, veremos los distintos pasos para el armado del Cable de Conexión. Esto es válido tanto para el cable directo como para el cable cruzado. La única diferencia es que en el cable directo ambos extremos se construyen con la misma norma, 568 A o 568 B, mientras que en el cruzado, un extremo se construye con 568 A y el otro con 568 B.

### Pasos para armar el conector plug RJ45

- Paso 1: cortar un trozo de cable del tamaño adecuado.
- Paso 2: cortar el revestimiento.
- Paso 3: separar y destrenzar los pares de cables.
- Paso 4: organizar y aplanar los hilos, según TIA/EIA 568 A o B.

- Paso 5: cortar los hilos a la distancia adecuada (1/2 pulgada ó 13 mm).
- Paso 6: insertar el cable en la ficha RJ45. Deben reunirse los alambres que forman los pares para que puedan insertarse en el Plug RJ45.
- Paso 7: empujar los hilos hacia adentro hasta que hagan tope en la ficha.
- Paso 8: inspeccionar el código de colores.
- Paso 9: engarzar (crimpear) con la herramienta adecuada (pinza de crimpear).
- Paso 10: inspeccionar ambos extremos.
- Paso 11: probar la calidad del cable con el analizador de cables (Tester LAN).



## Armado del JACK RJ-45 y del Patch Pannel

La inserción de los cables dentro de las ranuras especiales que tienen, tanto los Jacks como los patch pannel en su parte trasera, se realiza con una herramienta de impacto como puede apreciarse en la figura siguiente.



Esta herramienta introduce por impacto los cables dentro de la cavidad, que posee unas cuchillas que cortan el

aislante y hacen contacto con el conductor de cobre central. Esta herramienta, además, posee una cuchilla para cortar el remanente de cable; de esta manera, con una sola operación se inserta el cable y se corta el sobrante.

## Conexión de los cables en los Jacks

Para conectar los cables a los jacks, siga los siguientes pasos:

- **Paso 1.** Retire sólo la cantidad de revestimiento de cable que se necesita para terminar los alambres. Cuanto más expuestos queden los hilos, peor será la conexión y mayor será la pérdida de señal.
- **Paso 2.** Asegúrese de mantener el trenzado en cada par de hilos, en la medida que sea posible, hasta el punto de terminación. Es el trenzado de los hilos lo que produce la cancelación necesaria para evitar la interferencia electromagnética. Para UTP CAT 5, la cantidad máxima de alambre no trenzado que se permite es 13 mm.
- **Paso 3.** Si es necesario doblar el cable para poder dirigirlo, asegúrese de mantener un radio de curvatura que sea igual a cuatro veces el diámetro del cable. El cable jamás se debe doblar hasta un punto que exceda un ángulo de 90°.
- **Paso 4.** Evite estirar el cable mientras lo manipula. Si el estiramiento es superior a los 11,3 kg. de tracción, los hilos ubicados dentro del cable se pueden destrenzar y, como usted ya ha aprendido, esto puede provocar interferencias y diafonía.

## Mapeo del cableado

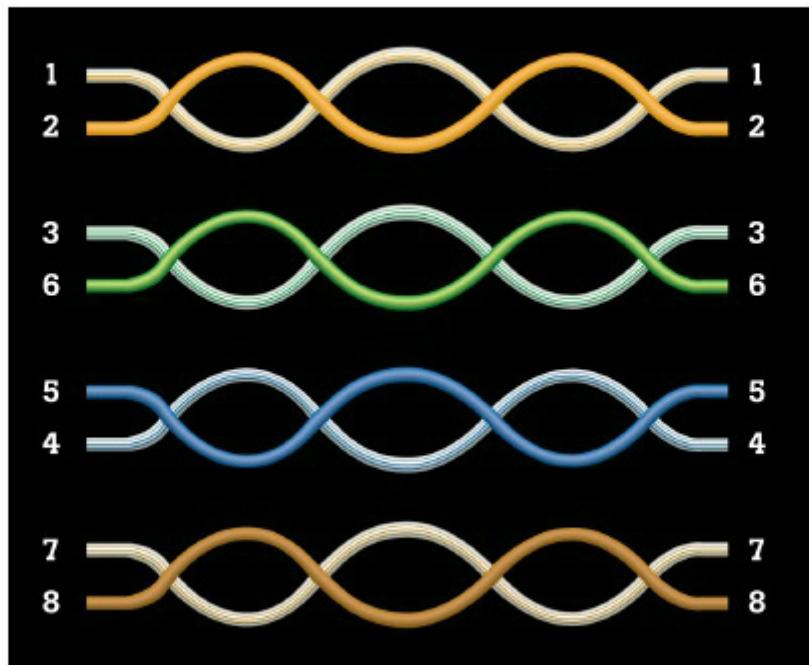
Los estándares de prueba y medidas definen la **metodología de medición, herramientas y procedimientos**, por ejemplo: ASTM D 4566.

Es muy importante verificar el funcionamiento correcto de los cables UTP e identificar cuáles son los incorrectos.

Para realizar una CERTIFICACIÓN del cableado se utiliza un equipo llamado CERTIFICADOR, que es capaz de realizar una serie de testeos a fin de verificar la performance de la infraestructura bajo una determinada categoría o estándar predefinida.

Una de las pruebas más importantes que realiza el equipo Certificador es la Prueba de Mapeado de Cables. Esta prueba se realiza sobre los cables de la instalación (no sobre los patch cords), es decir que lo que se certifica es la instalación de los cables, o más concretamente los cables instalados que van, desde la roseta o boca de conexión jack RJ-45 fijada a la pared (toma de telecomunicaciones), hasta la boca de conexión jack RJ-45 del patch panel.

# Mapa de cableado correcto



Métodos de prueba

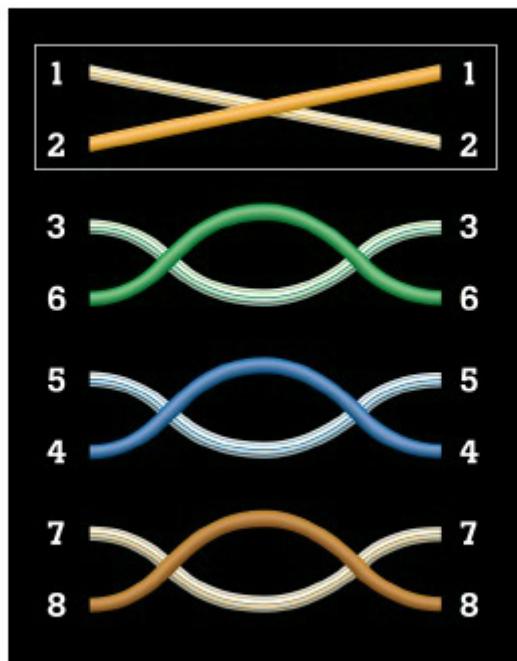
"Mapa de cableado correcto" | <http://www.slideshare.net/hvelarde/mtodos-de-prueba>

A los errores encontrados en esta prueba se los denomina mapeados incorrectos.

A los mapeados incorrectos los podemos clasificar en:

- Pares Invertidos: ésta es una falla común cuando se arman cables, a veces por accidente, cuando se insertan los pares dentro de plug o ficha RJ45. Evidentemente que este cable no va a funcionar, por cuanto la corriente que sale por un pin y que circula por un hilo, no cierra el circuito en el otro extremo.

# Pares invertidos

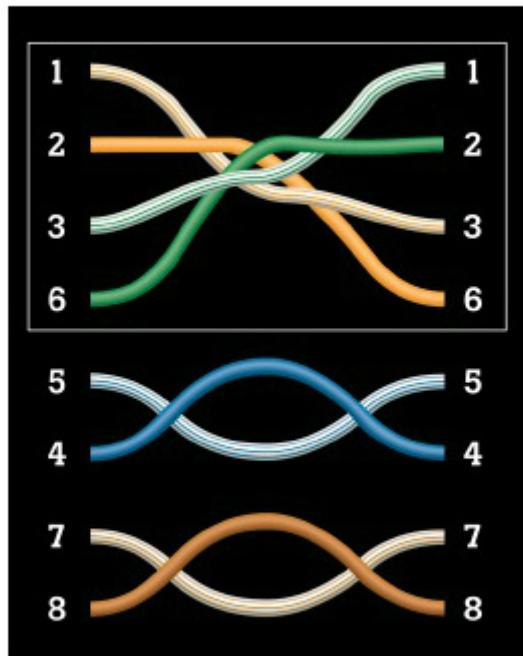


Métodos de prueba

"Par invertido" | <http://www.slideshare.net/hvelarde/mtodos-de-prueba>

- Pares Cruzados: los pares cruzados son un tremendo problema, ya que los alambres pertenecen a circuitos eléctricos distintos, con lo cual la composición de las señales no tiene nada que ver en cada extremo.

# Pares cruzados

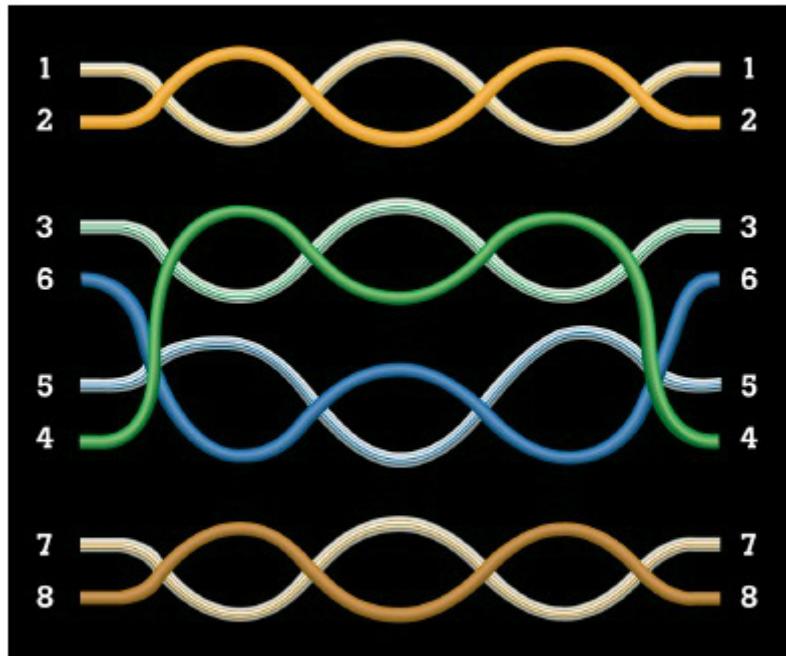


Métodos de prueba

"Pares cruzados" | <http://www.slideshare.net/hvelarde/mtodos-de-prueba>

- Pares Divididos: el problema de pares divididos, suele ser a veces bastante difícil de identificar, ya que el circuito funciona, pero los alambres de cada par (por ejemplo, el verde y el azul) pertenecen a circuitos distintos. Esto provoca muchos ruidos que no se compensan entre sí, minimizando la **paradifonía** \* 8.1 .

# Pares divididos



Métodos de prueba

"Pares Divididos" | <http://www.slideshare.net/hvelarde/mtodos-de-prueba>

También existe otra serie de testeos que el certificador puede realizar que simplemente mencionamos, tales como pruebas de longitud de cable, resistencia, next, elfext, powersum, atenuación, pérdida de retorno, impedancia, retardo y desfase, capacitancia, ACR, prueba del margen, permanent link y channel link. La explicación de cada una de ellas excede el contenido de esta materia.

Además los equipos certificadores suelen tener un set de elementos opcionales para trabajar con fibra óptica, con el cual se pueden realizar, por lo general, una serie de mediciones tales como Atenuación Óptica, Longitud y Diagnóstico de Fallas.

También para facilitar la tarea y el registro de las actividades, estos equipos suelen permitir imprimir en el momento un "ticket" con todas las mediciones efectuadas.

# REFERENCIAS 8

## 8.1 : Paradiafonía

Paradiafonía o Crosstalk: es la inducción de corrientes de un cable sobre el otro debido a su cercanía.

---



¡Vamos a comprobar cuánto aprendiste!

**1. Indique la opción correcta**

Según EIA/TIA-568-A, el color del par Tx es el Verde (par 3) y el color del par Rx es el Naranja (par 2).

- Verdadero
- Falso

**2. Indique la opción correcta**

Según EIA/TIA-568-B, el color del par Tx es el Naranja (par 2) y el color del par Rx es el Verde (par 3).

- Verdadero
- Falso

**3. Indique la opción correcta**

Un cable de pares cruzados (crossover), se construye haciendo un extremo como EIA/TIA-568-A y el otro como EIA/TIA-568-B.

- Verdadero
- Falso

**4. Indique la opción correcta**

Según EIA/TIA, para telefonía se debe utilizar:

- El par azul.
- El par naranja.
- El par verde.
- El par marrón.

**5. Indique la opción correcta**

Indicar: ¿cuáles de los siguientes errores NO es un error que se pueda encontrar en una prueba de mapeado?

- Pares Invertidos.
- Pares Cruzados.

- Pares Divididos.
- Atenuación.

#### 6. Ordene relaciones

Unir conceptos: Según EIA/TIA 568

El par 1	es el par blanco marrón - marrón
El par 2	es el par blanco azul - azul
El par 3	es el par blanco naranja - naranja
El par 4	es el par blanco verde - verde

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Según EIA/TIA-568-A, el color del par Tx es el Verde (par 3) y el color del par Rx es el Naranja (par 2).

Verdadero

Falso

## 2. Indique la opción correcta

Según EIA/TIA-568-B, el color del par Tx es el Naranja (par 2) y el color del par Rx es el Verde (par 3).

Verdadero

Falso

## 3. Indique la opción correcta

Un cable de pares cruzados (crossover), se construye haciendo un extremo como EIA/TIA-568-A y el otro como EIA/TIA-568-B.

Verdadero

Falso

## 4. Indique la opción correcta

Según EIA/TIA, para telefonía se debe utilizar:

El par azul.

El par naranja.

El par verde.

El par marrón.

## 5. Indique la opción correcta

Indicar: ¿cuáles de los siguientes errores NO es un error que se pueda encontrar en una prueba de mapeado?

Pares Invertidos.

Pares Cruzados.

Pares Divididos.

Atenuación.

## 6. Ordene relaciones

Unir conceptos: Según EIA/TIA 568

El par 1

es el par blanco naranja - naranja

El par 2

es el par blanco verde - verde

El par 3

es el par blanco azul - azul

El par 4

es el par blanco marrón - marrón

## SP5 / H4: Estándares inalámbricos y distintos tipos de dispositivos de conexión

### Estándares inalámbricos

Incrementando enormemente la capacidad de ampliación de una red LAN, veremos que el comité IEEE 802.11 define la utilización de los dos niveles inferiores del modelo OSI (Capas Física y Enlace de Datos) especificando las normas de funcionamiento en una LAN inalámbrica.

La versión básica de este estándar fue creada en 1997 y a partir de allí fue actualizándose hasta nuestros días. Estas normas constituyen la base de los productos de red inalámbricos que utilizan la marca Wi-Fi.



"Switch wifi" | [http://img1.mlstatic.com/router-wi-fi-d-link-dir-600-150mbps-3-veces-mas-veloz\\_MEC-O-9669639\\_4423.jpg](http://img1.mlstatic.com/router-wi-fi-d-link-dir-600-150mbps-3-veces-mas-veloz_MEC-O-9669639_4423.jpg)

La familia 802.11 tiene una serie de protocolos que utilizan el mismo principio básico de funcionamiento: técnicas de modulación sobre radiofrecuencias.

El estándar origina definió como método de acceso al protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) cuyo principio de funcionamiento ya fue descripto en la Situación Profesional 4 (Otros controles de acceso al medio - CSMA/CA).

Los más utilizados están definidas en los protocolos 802.11b y 802.11g. Ambos utilizan 2.4 GHz y raramente

pueden sufrir interferencias en un hogar relacionadas con la utilización del microondas, teléfonos inalámbricos y señales Bluetooth. Debido a esto, en la versión 1.2 del estándar Bluetooth por ejemplo se actualizó su especificación para que no existieran interferencias.

En la actualidad ya se encuentran disponibles en el mercado equipamiento definido en el protocolo 802.11n, que puede trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz. Con este equipamiento se obtienen las más altas prestaciones.

El segmento de operación de los equipos que operan dentro de la familia 802.11 (entre los 2,4 y los 5 GHZ) es de permitida utilización por la legislación vigente sin necesidad de licencias. Esto constituye una ventaja frente a otras tecnologías como por ejemplo Wi-Max, que son accesibles mediante una autorización para el uso del espectro electromagnético.

## 802.11a

En 1999 IEEE ratificó las normas 802.11a y 802.11b. La primera tuvo una velocidad máxima de transmisión teórica de 54 Mbps, funcionando en 5 GHz. La velocidad teórica siempre se verá reducida por la codificación de los protocolos por lo cual la velocidad real de transmisión de datos con este estándar alcanza aproximadamente los 25 Mbps. El problema surgió porque los equipamientos salieron al mercado después que los de versión 802.11b, que ya habían sido adquiridos por un gran número de consumidores y no era compatible con esta. Tenía mejor velocidad y trabajaba a una frecuencia hasta ese momento no usada, pero no era compatible con la versión b y era de elevado precio con respecto a esta. Alcance aproximado entre 8 y 25m en interiores.

## 802.11b

Tiene una velocidad máxima de transmisión teórica de 11 Mbps, funcionando en 2.4 GHz. La velocidad real de transmisión de datos con este estándar es de aproximadamente 5,9 Mbps sobre TCP y 7,1 Mbps sobre UDP. (En la SP10 se explicarán en detalle los protocolos TCP y UDP). No es compatible con 802.11a. Alcance aproximado entre 30 y 50m en interiores.

## 802.11g

Utiliza también de 2.4 Ghz pero trabaja a una velocidad teórica máxima de 54 Mbps, que se traduce en hasta 25 Mbps de velocidad real de transferencia. Es compatible con el estándar b, sin embargo, en redes bajo el estándar g la presencia de nodos operando en el estándar b reduce significativamente la velocidad de transmisión. No es compatible con 802.11a. A 11 Mbps es compatible con redes 802.11b. Alcance aproximado entre 30 y 50m en interiores.

## 802.11n

Este estándar se viene implantando desde 2008. Gracias a que puede trabajar en distintas frecuencias es compatible con todas las versiones anteriores de Wi-Fi. Fue ratificado en setiembre de 2009 por el IEEE y permite alcanzar una velocidad de transmisión teórica de 600 Mbps. En la actualidad ya existen varios productos en nuestro mercado que cumplen el estándar "n" con un máximo teórico de 450 Mbps, que se traduce en una velocidad de transmisión de datos de entre 100-150 Mbps estables, con picos de hasta 200 Mbps.

La velocidad y la transmisión máxima de datos se alcanzan cuando se utilizan todos los equipos con la misma tecnología en el modo de transmisión mejor. La velocidad de datos real, las características y el rendimiento

pueden variar dependiendo de la presencia de otros equipos con velocidades más lentas, del entorno y otros factores.

Los fabricantes de equipamiento ya tienen en sus líneas de producción productos estandarizados 802.11n, incluso los proveedores de internet ya lo ofrecen a sus clientes.



"802.11n router" |

<http://www.tecnouupdate.com.ar/2011/01/20/linksys-e4200-router-80211n-de-doble-banda-con-tecnologia-mimo-450-mbps/>

El estándar en el que se está trabajando **a futuro** es el **802.11ac** con velocidades de transferencia teóricas superiores a 1 Gbps.

## La Tarjeta de Red (Network Interface Card – NIC)

La tarjeta de red (NIC) se conecta a la placa madre de la computadora (motherboard) y provee los puertos para la conexión, ya sea con cables o de forma inalámbrica. El tipo de tarjeta dependerá de la red o del acceso al medio (capa de Enlace de Datos). Así tenemos tarjetas Ethernet, Token Ring, para FDDI (Fiber Distributed Data Interface) o Inalámbricas.

Las tarjetas de red se comunican con la red a través de conexiones seriales, y con el computador, a través de conexiones en paralelo. Son las conexiones físicas entre las estaciones de trabajo y la red. Las tarjetas de red requieren una IRQ (nivel de Interrupción), una dirección E/S y direcciones de memoria superior.

Al seleccionar una tarjeta de red, debe tener en cuenta los tres siguientes factores:

1. Tipo de red (por ej. Ethernet, Token Ring, FDDI, etc.)
2. Tipo de medios (por ej. cable UTP, coaxial, fibra óptica o wireless)
3. Tipo de bus del sistema (por ej. PCI o PCIE pudiendo encontrar en algunas computadoras viejas tarjetas con conexión ISA)

## Operaciones de las NIC de Capa 2

Las NIC ejecutan funciones importantes de la capa de enlace de datos (Capa 2) como, por ejemplo, las siguientes:

- Control del enlace lógico: se comunica con las capas superiores del computador.
- Denominación: proporciona un identificador exclusivo a través de la dirección MAC.
- Creación de tramas: forma parte del proceso de encapsulamiento, agrupando los bits para su transporte.
- Control de acceso al medio (MAC): proporciona un procedimiento estructurado para el acceso al medio compartido.

A continuación pueden verse varios ejemplos de NIC de distintos tipos (aquí repasaremos lo aprendido en la materia Hardware en lo que se refiere a distintos tipos de conectores y buses):



\* 9.1 Imágenes

Imágenes "Ejemplos de NIC"

Elaboración DEPROE, IES siglo21

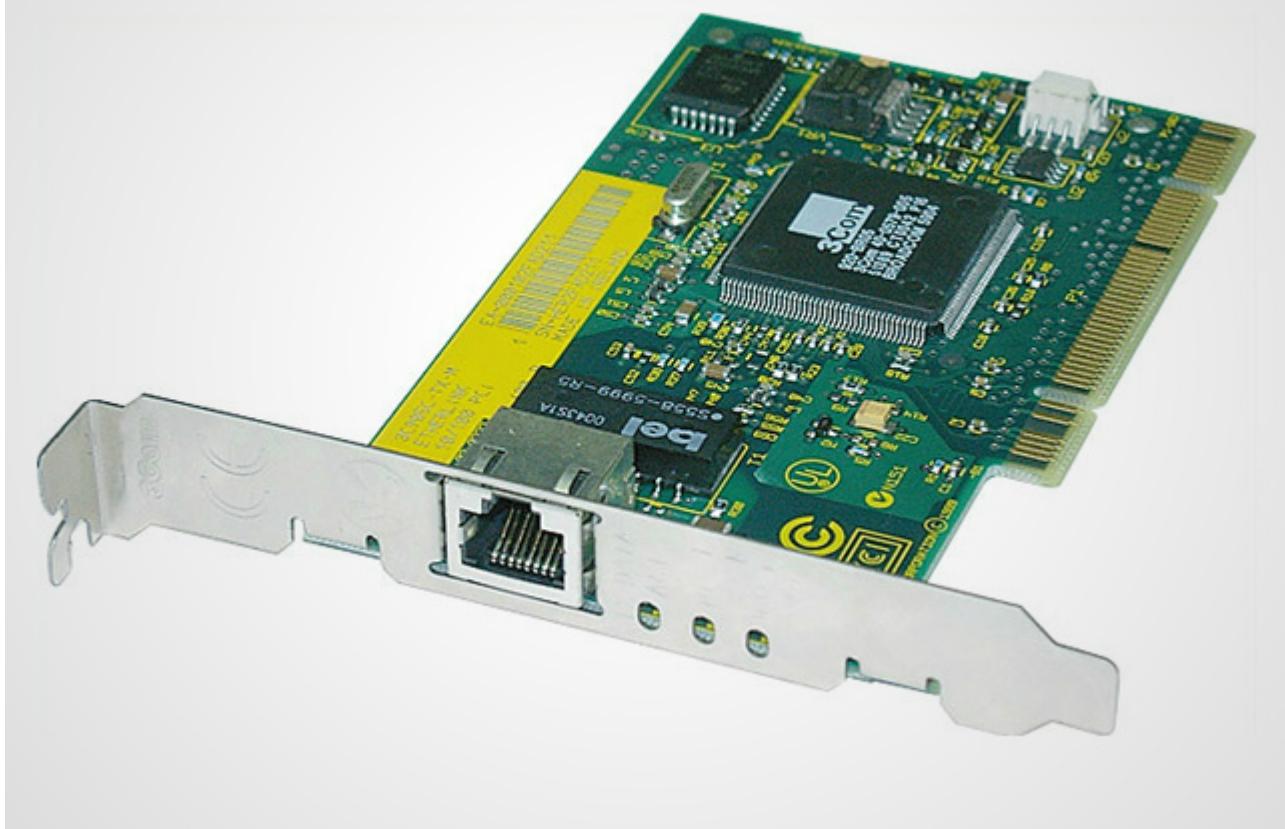
# REFERENCIAS 9

## 9.1 Imágenes: Ejemplos de NIC



A

qui tenemos una NIC con conectores BNC y RJ-45 para un bus ISA



N

IC con conector RJ-45 para un bus PCI



N

IC con conector RJ-45 para un bus PCIE



IC inalambrica para un bus PCI

N



E

xisten soluciones en USB de este tipo (que se pueden aplicar a cualquier computadora o notebook que posea puertos USB)

[http://3.bp.blogspot.com/\\_BnxoldxpKSc/S\\_QQAIU08cI/AAAAAAAUAU/S3vwJ8z9TcY/s1600/Tarjeta+de+interfaz+de+Red.jpg](http://3.bp.blogspot.com/_BnxoldxpKSc/S_QQAIU08cI/AAAAAAAUAU/S3vwJ8z9TcY/s1600/Tarjeta+de+interfaz+de+Red.jpg) <http://rpc.yoreparo.com/foros/files/plared.jpg> [http://bimg2.mlstatic.com/placa-de-red-tp-link-tg-3468-pci-express-gigabit-101001000\\_MLA-F-3117467590\\_092012.jpg](http://bimg2.mlstatic.com/placa-de-red-tp-link-tg-3468-pci-express-gigabit-101001000_MLA-F-3117467590_092012.jpg)

[http://bimg2.mlstatic.com/placa-red-adapt-usb-wireless-tp-link-tl-wn722n-150-mbps-wifi\\_MLA-F-2915516266\\_072012.jpg](http://bimg2.mlstatic.com/placa-red-adapt-usb-wireless-tp-link-tl-wn722n-150-mbps-wifi_MLA-F-2915516266_072012.jpg)



¿Te animás a medir cuánto aprendiste?

**1. Indique la opción correcta**

IEEE 802.11 define la utilización de los dos niveles inferiores del modelo OSI (Capas Física y Enlace de Datos) especificando las normas de funcionamiento en una LAN inalámbrica.

- Verdadero
- Falso

**2. Indique la opción correcta**

La velocidad teórica siempre se verá reducida por la codificación de los protocolos y la velocidad del equipamiento compatible con los anteriores se verá reducida también si el modo de operación tiene que adaptarse a otros nodos presentes en la red con los cuales son compatibles pero a frecuencias más bajas.

- Verdadero
- Falso

**3. Indique la opción correcta**

El último estándar reconocido por 802.11, que además es compatible con todas las versiones anteriores es:

- 802.11a.
- 802.11b.
- 802.11g.
- 802.11n.

**4. Indique la opción correcta**

Al seleccionar una tarjeta de red, debe tener en cuenta algunos factores: ¿Cuál de los siguientes NO es un factor a tener en cuenta al seleccionar una tarjeta de red?

- Tipo de red.
- Tipo de medios.
- Tipo de bus del sistema.

- o Tipo de administración.

**5. Indique la opción correcta**

Las NIC ejecutan muchas funciones importantes, ¿Cuál de las siguientes NO es una función que ejecuta siempre la NIC?

- o Control del enlace lógico: Se comunica con las capas superiores del computador.
- o Creación de tramas: Forma parte del proceso de encapsulamiento, agrupando los bits para su transporte.
- o Control de acceso al medio (MAC): Proporciona un procedimiento estructurado para el acceso al medio compartido.
- o Retransmisión: si la dirección no coincide con la propia entonces pasa la señal al siguiente NIC, en todas las topologías.

**6. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

802.11a	Hasta 600 Mbps teóricos trabajando a 2.4 y 5GHz.
802.11b	Hasta 11 Mbps teóricos trabajando a 5GHz.
802.11g	Hasta 54 Mbps teóricos trabajando a 2.4GHz.
802.11n	Hasta 54 Mbps teóricos trabajando a 5GHz.

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

IEEE 802.11 define la utilización de los dos niveles inferiores del modelo OSI (Capas Física y Enlace de Datos) especificando las normas de funcionamiento en una LAN inalámbrica.

- Verdadero
- Falso

## 2. Indique la opción correcta

La velocidad teórica siempre se verá reducida por la codificación de los protocolos y la velocidad del equipamiento compatible con los anteriores se verá reducida también si el modo de operación tiene que adaptarse a otros nodos presentes en la red con los cuales son compatibles pero a frecuencias más bajas.

- Verdadero
- Falso

## 3. Indique la opción correcta

El último estándar reconocido por 802.11, que además es compatible con todas las versiones anteriores es:

- 802.11a.
- 802.11b.
- 802.11g.
- 802.11n.

## 4. Indique la opción correcta

Al seleccionar una tarjeta de red, debe tener en cuenta algunos factores: ¿Cuál de los siguientes NO es un factor a tener en cuenta al seleccionar una tarjeta de red?

- Tipo de red.
- Tipo de medios.
- Tipo de bus del sistema.
- Tipo de administración.

## 5. Indique la opción correcta

Las NIC ejecutan muchas funciones importantes, ¿Cuál de las siguientes NO es una función que ejecuta siempre la NIC?

- Control del enlace lógico: Se comunica con las capas superiores del computador.
- Creación de tramas: Forma parte del proceso de encapsulamiento, agrupando los bits para su transporte.
- Control de acceso al medio (MAC): Proporciona un procedimiento estructurado para el acceso al medio compartido.
- Retransmisión: si la dirección no coincide con la propia entonces pasa la señal al siguiente NIC, en todas las topologías.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

802.11a	Hasta 11 Mbps teóricos trabajando a 5GHz.
802.11b	Hasta 54 Mbps teóricos trabajando a 2.4GHz.
802.11g	Hasta 54 Mbps teóricos trabajando a 5GHz.
802.11n	Hasta 600 Mbps teóricos trabajando a 2.4 y 5GHz.

# SP5 / H5: El sistema de cableado - estándares y diseño

El estándar ANSI/TIA/EIA 569-A bajo el título: "Commercial Building Standard for Telecommunication Pathways and Spaces" (Estándar de espacios y recorridos de telecomunicaciones para edificios comerciales) define las especificaciones y directivas para la instalación en edificios comerciales de los sistemas de cableado de telecomunicaciones y componentes.

Esta norma identifica y aborda varios temas importantes de la infraestructura: las facilidades de acceso al edificio, la sala donde estarán los equipos principales, el sistema de cableado vertical, las salas de telecomunicaciones, el subsistema de cableado horizontal y las áreas de trabajo.

Se enlistan a continuación las cuestiones importantes, de las cuales haremos hincapié en el sistema de cableado vertical y el subsistema de cableado horizontal.

## Reglas de diseño

- Largo y configuración del tendido:  
Enlace básico (*Basic Link*: 90 metros, 294 feet).  
Canal (*Channel*: 100 metros, 328 feet).
- Proximidad a fuentes de energía.

## Recomendaciones en la instalación

- Radio de curvatura.
- Fuerza de tracción.
- Terminación / conectorización.

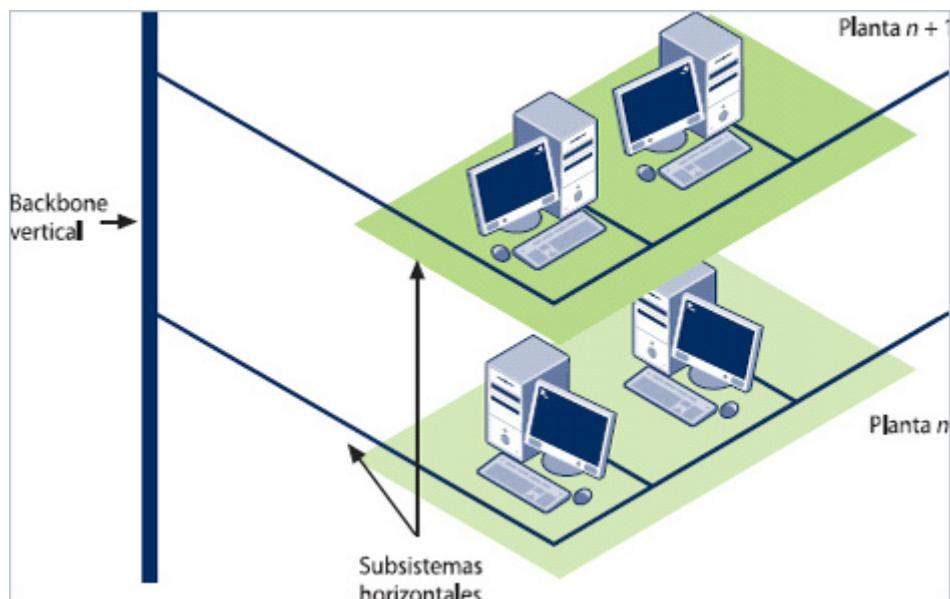
## Requerimientos TIA TSB-67

- Mapa de cableado.
- Longitud.
- Atenuación.
- Paradifonía en el extremo cercano.

## Beneficios en caso de cumplir con los estándares

- Seguridad de que el cableado soportará las aplicaciones basadas en estándares.
- Simplifica la administración.
- Facilita el crecimiento futuro.

En la siguiente figura pueden apreciarse con claridad el sistema de cableado vertical (backbone) y los subsistemas de cableado horizontal.



"Cableado Horizontal y vertical" |

[http://imagenes.mailxmail.com/cursos/imagenes/5/8/cableado-estructurado-necesidad\\_22685\\_10\\_1.jpg](http://imagenes.mailxmail.com/cursos/imagenes/5/8/cableado-estructurado-necesidad_22685_10_1.jpg)

## Sistema de cableado vertical

A continuación estudiaremos algunos de los conceptos del cableado Vertical. Para ello daremos algunas definiciones:

- **MCC (Main Cross-Connect)**

Lugar donde se encuentran equipos de telecomunicaciones y se produce la terminación mecánica de una o más partes del sistema de cableado (Centro de la Estrella). Se distinguen de los ICC (*Intermediate Cross-Connect*) y los TC's (*Telecommunication Closet*) por la cantidad y complejidad del equipo que allí se encuentra. Algunos ejemplos son salas de centrales telefónicas y centros de cómputos.

- **ICC (Intermediate Cross- Connect)**

Lugar(es) donde se encuentran equipos de telecomunicaciones para la configuración del cableado vertical. Desde estos lugares parte generalmente el Sistema de Cableado Horizontal. Constituyen las ramas del árbol de conexión vertical.

- **TC (Telecommunication Closet)**

Lugar(es) en los que se establece la conexión entre las troncales y el cableado horizontal hasta los puestos de trabajo, y en los que se ubican los dispositivos activos o pasivos que permiten dicha conexión. En este lugar se producirá el ingreso de los cables multipares de telefonía o de datos, las fibras ópticas para la transmisión de datos, y las acometidas a los puestos de trabajo del área a la que dará servicio.

## Subsistema de Cableado horizontal

Es la porción del sistema de cableado de telecomunicaciones que se extiende desde los puestos de trabajo hasta el TC.

- **Puestos de trabajo WS (Worstation)**

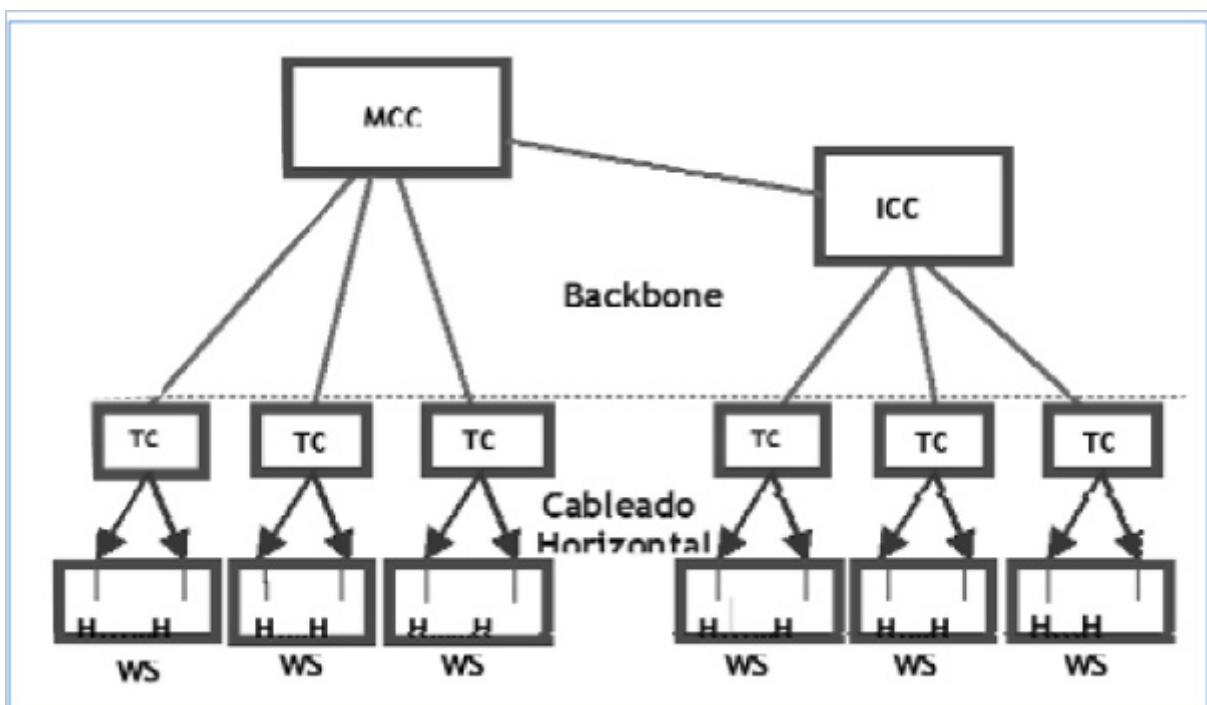
Lugares dispuestos para la posible conexión del equipamiento de telecomunicaciones del usuario.

- **Tomas de telecomunicaciones**

Es la caja terminal de la instalación que proporciona el soporte mecánico de los conectores apropiados para que cada puesto de trabajo tome los servicios que le correspondan.

- **Topología jerárquica en estrella**

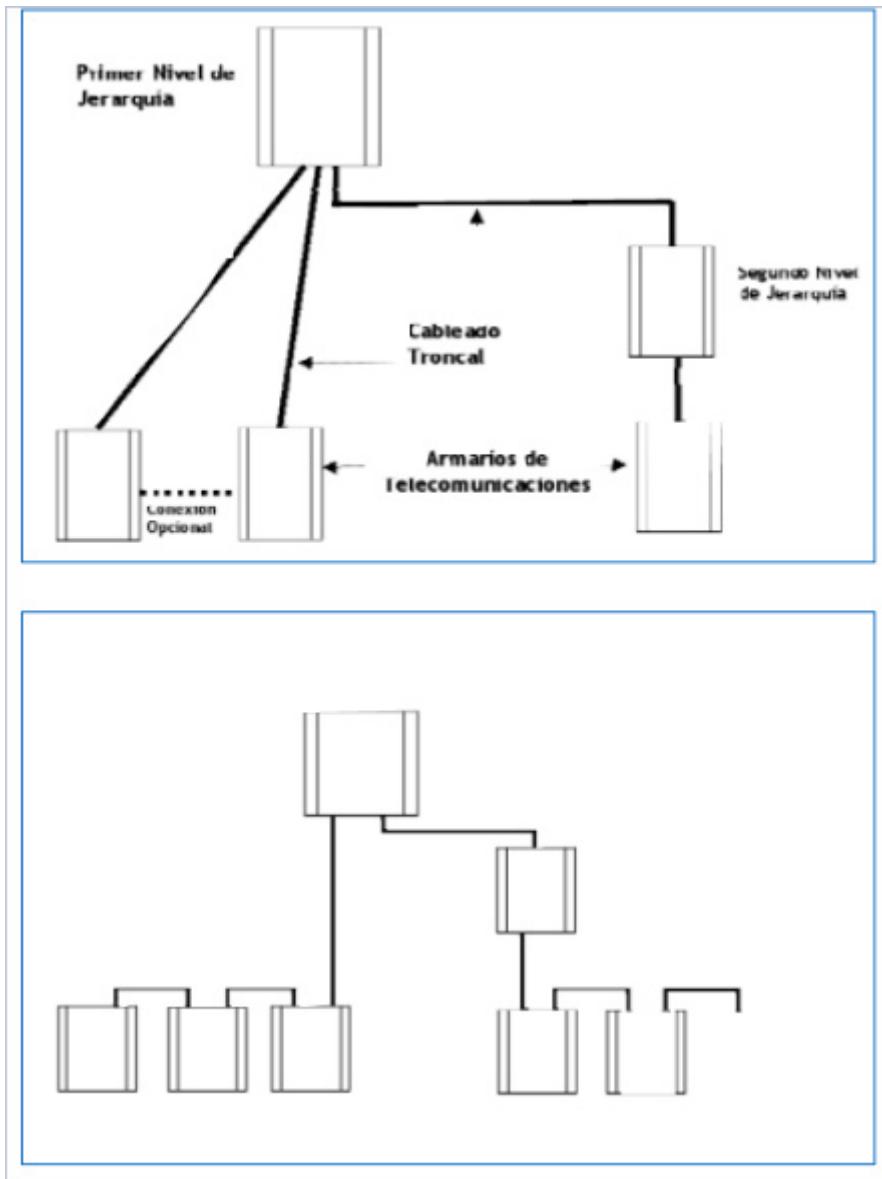
Además se permite unir los armarios entre sí para facilitar las comunicaciones. Esta parte del cableado que une Armarios se denomina backbone, o troncal. La figura que a continuación se presenta muestra este esquema.



Los tipos de cables permitidos para la red troncal son los mismos que para el cableado horizontal, pero se permite el uso de UTP multipares. En general, la distancia total permitida entre el Armario Principal y los de Telecomunicaciones es de 500 metros, salvo para Fibra Óptica para las cuales se admite una distancia de hasta 2000 metros.

## Variantes de la topología jerárquica en estrella

La topología establecida para la red Troncal es en estrella, de forma tal que otras topologías, tales como anillos o bus, deben obtenerse a partir de ésta. Las siguientes figuras muestran esto.



## Estructura del cableado

### Sistema del cableado vertical o Backbone

El estándar TIA/EIA-568-A especifica cuatro tipos de medios de networking que se pueden usar para el cableado backbone. Estos son:

- 100 \_ UTP (cuatro pares).
- 150 \_ STP-A (dos pares).
- Fibra óptica multimodo.
- Fibra óptica monomodo.

Aunque el estándar TIA/EIA-568-A reconoce el cable coaxial 50, generalmente no se recomienda usarlo para nuevas instalaciones y se anticipa que será eliminado como opción en la próxima revisión del estándar. La

mayoría de las instalaciones de la actualidad usan normalmente el cable de fibra óptica 62,5/125 µm para el cableado backbone.

## Subsistema de cableado horizontal

El subsistema de cableado horizontal se extiende desde la toma de telecomunicaciones en el área de trabajo hasta la conexión cruzada horizontal, en el centro de telecomunicaciones. Incluye la toma de telecomunicaciones, un punto de transición y las terminaciones mecánicas y cable de conexión que constituyen la conexión cruzada horizontal.

Para el subsistema de cableado horizontal se especifica lo siguiente:

- UTP de 4 pares de 100 ohmios. Se recomienda el uso de UTP CAT 5 para el cableado horizontal.
- Fibra óptica de 2 fibras (dúplex) multimodo.
- Se permite el uso de cables de múltiples pares y múltiples unidades, siempre que cumplan con los requisitos de cableado TIA/EIA-568-A-3.
- La conexión a tierra debe estar de acuerdo con los códigos de construcción y con ANSI/TIA/EIA-697.
- Se requieren dos tomas de telecomunicaciones para cada área de trabajo.
- Primera toma: 100 \_ UTP (Cat 5e recomendado).
- Segunda toma: 100 \_ UTP (Cat 5e recomendado).
- Fibra óptica multimodo de dos fibras.
- No se recomienda el cableado coaxial de 50 \_ y STP de 150 \_ para las nuevas instalaciones.
- Se pueden suministrar tomas adicionales. Estas tomas son adicionales y no pueden reemplazar los requisitos mínimos contemplados en el estándar.
- No se permite el uso de empalmes y derivaciones para el cableado horizontal basado en cobre (se acepta el uso de empalmes en fibra óptica).
- Es necesario tener en cuenta la proximidad del cableado horizontal a las fuentes de interferencia electromagnética (EMI).

## Pasos a tener en cuenta para la instalación del cableado horizontal

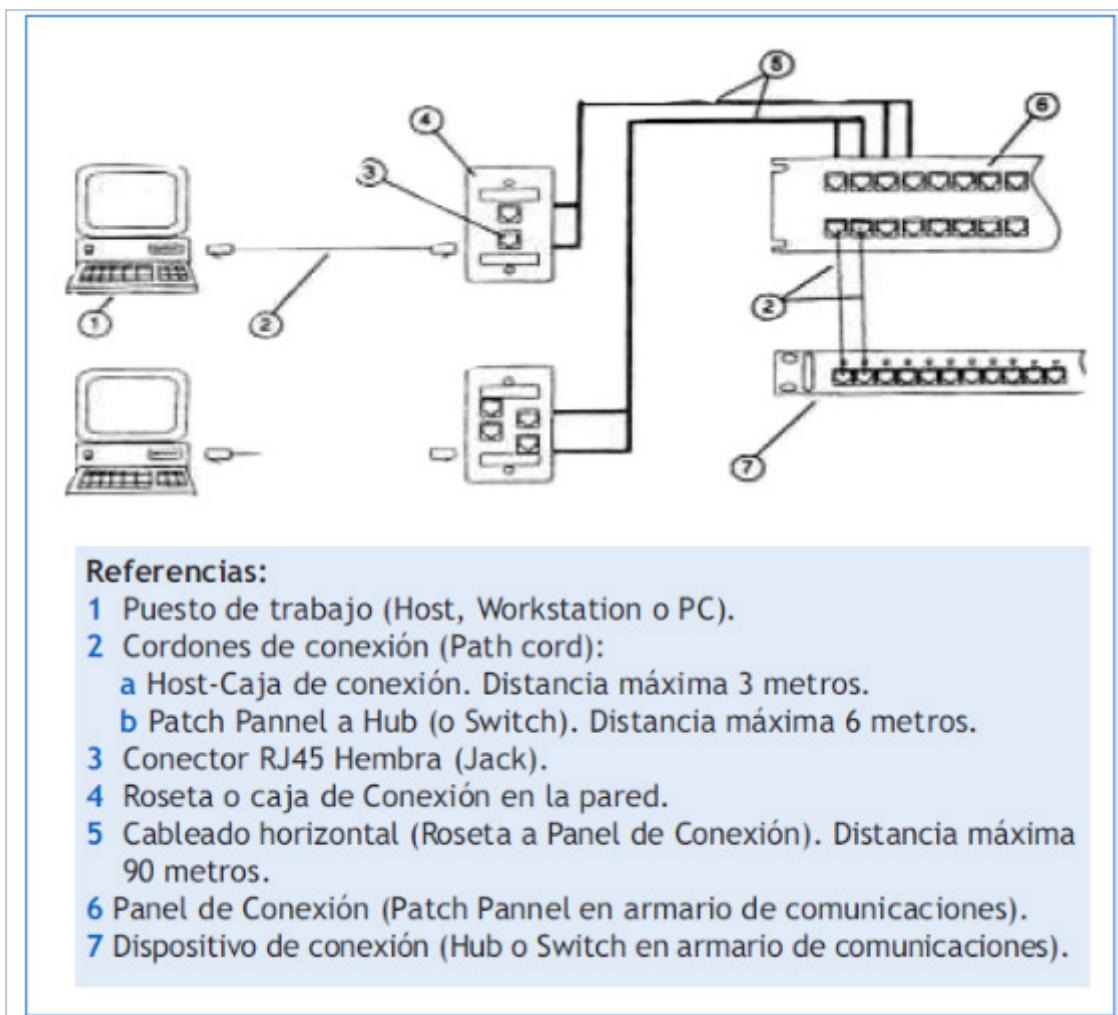
Se deben tener ciertos cuidados en la instalación del cableado horizontal. Para ello deben seguirse los siguientes pasos:

- **Paso 1.** Si se deben tender múltiples cables en una misma vía, use precintos de material plástico para sujetar el cable. Ubíquelos a intervalos al azar, luego ajústelos con cuidado. Nunca ajuste demasiado las ataduras ya que esto puede dañar los cables.
- **Paso 2.** Reduzca al mínimo el trenzado de los revestimientos de los cables. Si los trenza demasiado, los revestimientos pueden romperse. Nunca permita que los cables queden aplastados o enredados. Si esto ocurre, el rendimiento de los datos se reduce y la LAN operará a un nivel inferior al de su capacidad óptima.
- **Paso 3.** Nunca escatime la cantidad de cable necesaria para el tendido. Es importante que quede suficiente cable sobrante. Recuerde que agregar unos pocos metros más de cable es un pequeño precio si se compara con tener que volver a realizar el tendido de un cable porque quedó tirante. La mayoría de los instaladores evitan este problema dejando suficiente cable sobrante para que llegue al piso, y agregan otros 60 a 90 cm. en ambos extremos. Algunos

instaladores dejan una espiral de servicio, que son simplemente unos metros adicionales de cable colocados en forma de espiral dentro del techo o en alguna otra ubicación donde no moleste, para el caso que deba estirarse el cableado a otro sitio más alejado.

- **Paso 4.** Al sujetar el cable, use las técnicas adecuadas para las ataduras, barras de soporte, paneles de administración y cintas de Velcro removibles. Nunca use clavos, ni tornillos ni grapas para fijar los cables, éstos pueden perforar el revestimiento, provocando una pérdida de conexión.

En la figura que sigue, puede verse al esquema desde el armario de telecomunicaciones hasta el puesto de trabajo, o sea, hasta la PC.



#### • Cableado Horizontal - Definiciones

En la estructura del cableado horizontal existen algunas definiciones que es importante conocer. Así tenemos:

- Enlace (Link)

Es el cableado que va desde la caja en la pared (outlet) al patch panel en el armario de conexión horizontal o al armario de conexiones cruzadas (cross-connet). La distancia máxima según TIA/EIA 569 es de 90 metros.

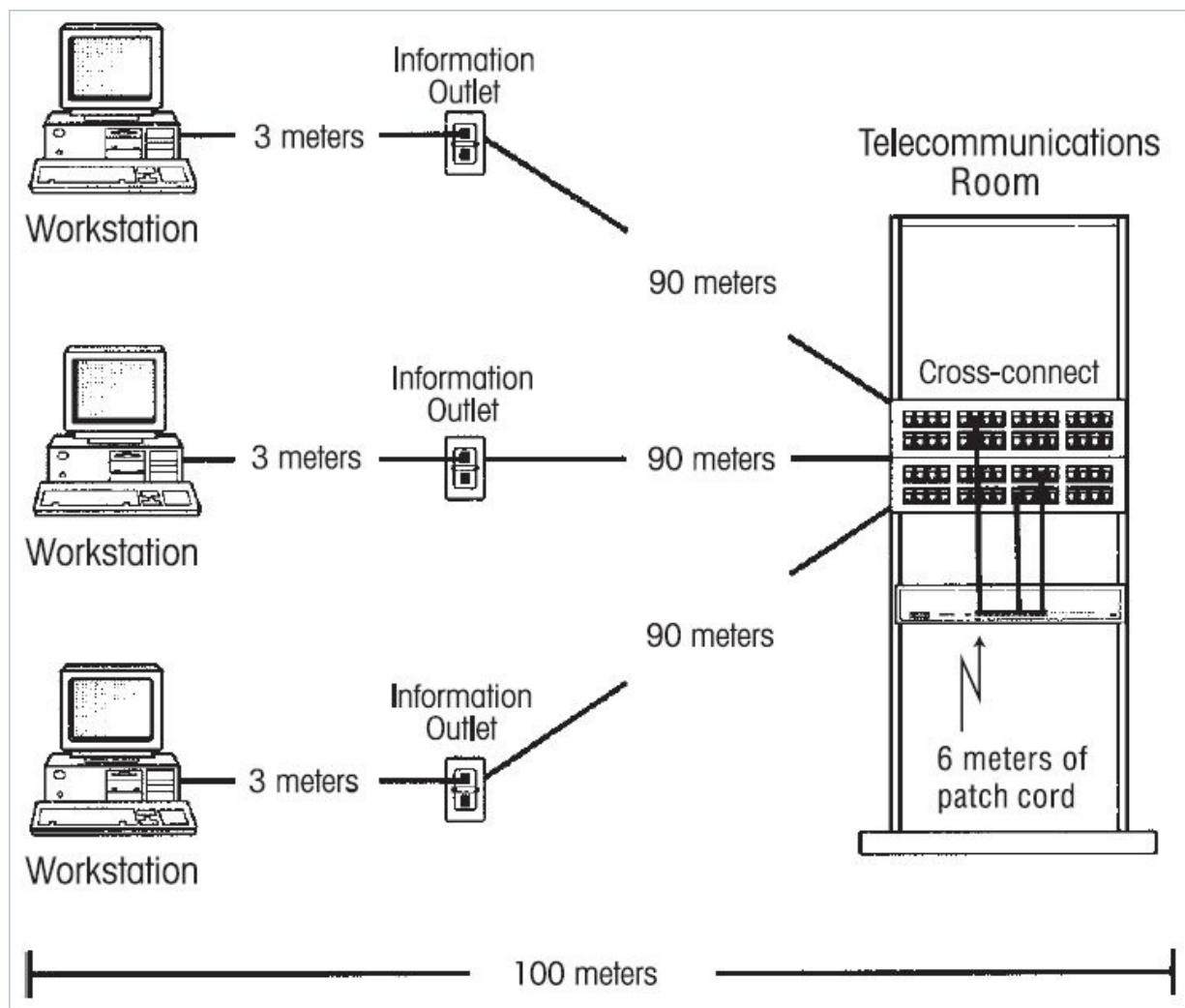
Link = Distancia del Outlet al Patch Panel o Cross Connect



- Canal (Channel)

Es el cableado que va desde la Tarjeta de Red (NIC) del Host (PC) hasta el dispositivo de comunicaciones (HUB o Switch). La distancia máxima, según TIA/EIA 569 es de 100 metros.

Channel = Distancia de la Network Interface Card al Hub o Switch.



"Cableado horizontal" | <http://cableado-horizontal.blogspot.com.ar/>

## Panel de conexión

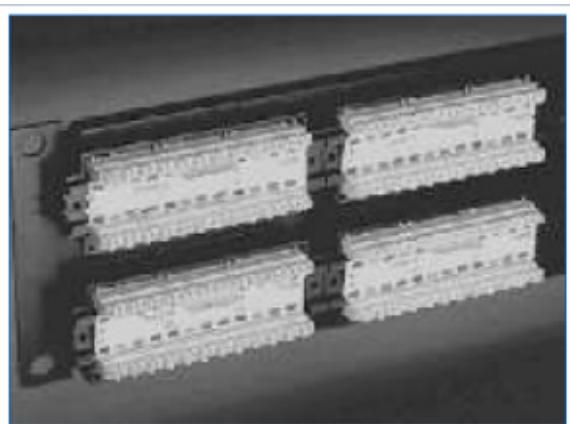
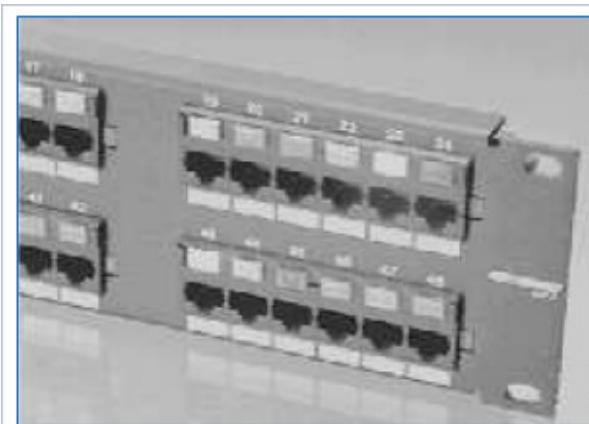
En una topología LAN Ethernet en estrella, el cableado horizontal, que provienen de las áreas de trabajo, generalmente termina en un panel de conexión (*Patch Panel*). Un panel de conexión es un dispositivo a través del cual el cableado horizontal se puede conectar con otros dispositivos de red, como por ejemplo, hub y switch. Más específicamente, un panel de conexión es una agrupación de pines y puertos. El panel de conexión actúa como un conmutador, donde los cables horizontales que provienen de las estaciones de trabajo se pueden conectar a otras estaciones de trabajo para formar una LAN.

En algunos casos, el panel de conexión también puede suministrar ubicaciones para que los dispositivos se conecten a una WAN o a Internet. TIA/EIA-568-A describe a esta conexión como una interconexión cruzada horizontal (HCC - *Horizontal Cross-Connect*).

En cualquier sistema de LAN, los conectores son el eslabón más débil de la cadena. Si no están debidamente instalados, pueden producir ruido eléctrico y pueden provocar un contacto eléctrico intermitente entre los hilos y los pines. Cuando esto ocurre, la transmisión a través de la red puede distorsionarse.

Para asegurarse de que el cable está instalado correctamente, debe hacer lo que indican los estándares TIA/EIA:

1. Cuando conecta varios tendidos de cable CAT 5 al panel de conexión, debe colocar los cables en orden ascendente, según el número de cable. Al colocarlos en ese orden en el panel de conexión, es mucho más fácil ubicar y diagnosticar cualquier problema en el futuro.
2. A medida que realiza el trabajo, es importante que mantenga los extremos de los cables centrados por encima de las ubicaciones de los pines. Si no tiene cuidado, los cables se pueden torcer, lo que dará como resultado una reducción en el rendimiento de los datos una vez que la LAN esté totalmente conectada.
3. Asegúrese de mantener el revestimiento a una distancia de 6,4 mm (máximo) de las ubicaciones de los pines en las que está trabajando para evitar que quede demasiado cable expuesto. Una buena forma de hacer esto es tomar la medida antes de eliminar el revestimiento: 38-50 mm debería ser suficiente. Si deja demasiado cable a la vista, la consecuencia será una reducción en el rendimiento de la red.
4. No se deben destrenzar los pares de cables más de lo necesario. Los cables no trenzados disminuyen el rendimiento de los datos y pueden provocar diafonía.



Los cables pueden montarse en distintas canalizaciones dispuestas a tal fin. Éstas pueden ser caños empotrados o no, cables canal o bandejas porta cables. En todos los casos debe tenerse en cuenta que el montaje del cableado horizontal de datos, no debe hacerse cerca de los cables de energía eléctrica. En el caso que no quede alternativa (por ejemplo, al pasarlos dentro de muebles o columnas montantes estrechas), deberá aislarlo electromagnéticamente alguno de los cables. La forma de aislarlo magnéticamente es colocando, ya sea el cable de señal o el de energía, dentro de una cañería o canaleta metálica.

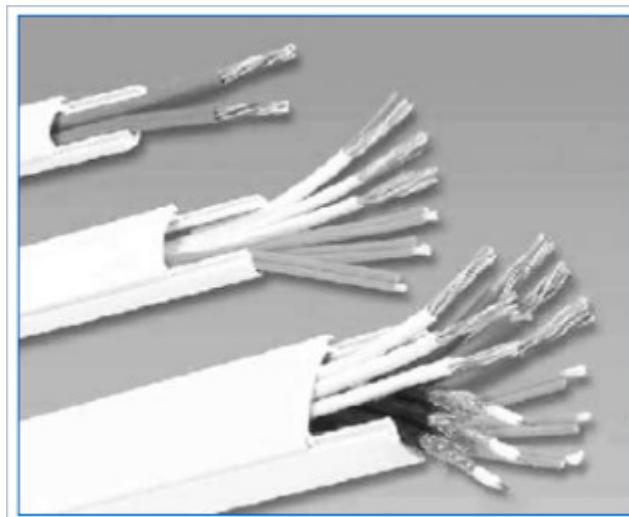
## Cable canal

El cable canal es una especie de canaleta montada sobre la pared con una cubierta móvil. Existen dos tipos de canaletas.

- Cable canal decorativo: tiene una terminación más acabada. Se utiliza para colocar cables pareados de una habitación, donde la instalación queda a la vista.
- Bandeja portacable: una alternativa menos atractiva que la de la canaleta decorativa. Su principal ventaja, es ser lo suficientemente grande como para contener varios cables. Generalmente, el uso del canal se ve restringido a espacios como áticos y el espacio sobre un techo falso.

Los cables canal suelen ser de plástico o de metal y se puede montar con adhesivo o con tornillos.

Después de montar el cable canal, coloque el cable en su interior y fije la tapa. Esto ayuda a proteger el cable.





Distancias máximas recomendadas para el tendido de los cables.

Tipos de medios de red	Distancia HCC A MCC	Distancia HCC A ICC	Distancia ICC a MCC
62.5/125 Cable de Fibra Óptica	2000 metros (6560 pies)	500 metros (1640 pies)	1500 metros (4820 pies)
Cable de Fibra Óptica Monomodo	3000 metros (9840 pies)	500 metros (1640 pies)	2500 metros (8200 pies)
UTP (voz)	800 metros (2624 pies)	500 metros (1640 pies)	300 metros (984 pies)
UTP (datos)	Aplicaciones de datos, limitadas a un total de 90 metros (295 pies)		

"Distancias máximas para el tendido de los cables." | Elaboración Autor

## Especificaciones TIA/EIA 606 para rotulado de cables

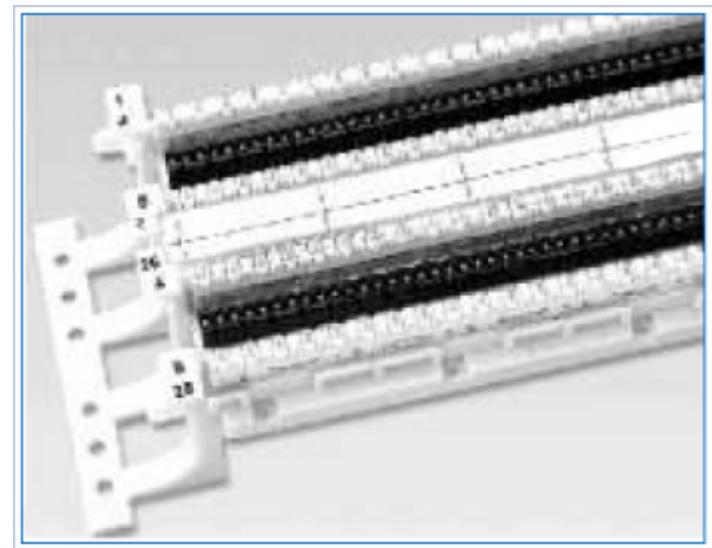
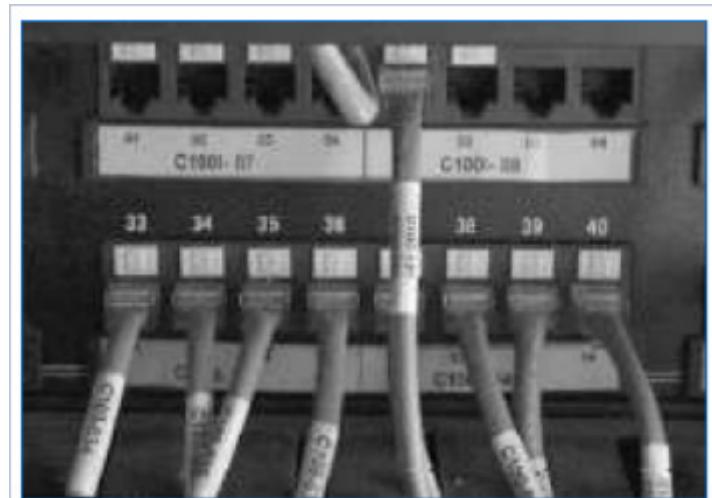
El estándar TIA/EIA-606 especifica que cada unidad de terminación de hardware debe tener algún tipo de identificador exclusivo. Este identificador debe estar marcado en cada unidad o en su rótulo. Cuando se utilizan identificadores en áreas de trabajo, las terminaciones de estaciones deben tener un rótulo en la placa, el bastidor o el conector mismo. Todos los rótulos, ya sean adhesivos o insertables, deben cumplir con los requisitos de legibilidad, protección contra el deterioro y adhesión especificados en el estándar UL969.

Use rótulos que sean comprensibles para alguien que deba trabajar en el sistema muchos años después.

Pueden incorporarse números de habitaciones o asignar letras a cada cable que llega hasta una habitación. Algunos sistemas de rotulado, especialmente en redes muy grandes, también incorporan una codificación con color. Por ejemplo, un rótulo azul puede identificar el cableado horizontal solamente del centro de cableado, mientras que un rótulo verde puede identificar el cableado del área de trabajo.

Coloque las conexiones de manera tal que los rótulos queden ordenados de forma ascendente. Esto facilita el diagnóstico y ubicación de los problemas cuando se presenten en el futuro. También rotule los cables en cada extremo.

Observe los distintos tipos de rotulados al frente y en la parte posterior:



55	805	C-2531	65
80	85	C-2631	90
5	10	C-3031	14
30	35	C-3031	40



¿Estás listo para un desafío?

**1. Indique la opción correcta**

Según las reglas de diseño, las distancias máximas son: para el enlace básico 90 metros y para el canal 100 metros.

- Verdadero
- Falso

**2. Indique la opción correcta**

El estándar ANSI/TIA/EIA-569 A hace recomendaciones en cuanto al radio de curvatura, la fuerza de tracción y la conectorización.

- Verdadero
- Falso

**3. Indique la opción correcta**

El requerimiento TIA TSB-67 hace referencia al Mapa de cableado, la longitud, la atenuación y la paradifonía.

- Verdadero
- Falso

**4. Indique la opción correcta**

Los beneficios en caso de cumplir con los estándares son: la seguridad de que el cableado soportará las aplicaciones basadas en estándares, la simplificación de la administración y facilidad del crecimiento futuro.

- Verdadero
- Falso

**5. Indique la opción correcta**

¿Cuál es el estándar que especifica cómo debe hacerse el rotulado de cables?

- ANSI/TIA/EIA 568-A.

- o ISO IEC 11801.
- o TIA/EIA 606.
- o ANSI/TIA/EIA 568-B.

**6. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Subsistema de Cableado  
Horizontal  
Enlace (link) en el  
cableado horizontal  
Canal (channel) en el  
cableado horizontal

va desde la NIC del Host hasta  
el concentrador (Switch).  
se extiende desde los puestos  
de trabajo hasta el TC.  
va desde la caja en la pared al  
patch panel hasta el TC.

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Según las reglas de diseño, las distancias máximas son: para el enlace básico 90 metros y para el canal 100 metros.

- Verdadero
- Falso

## 2. Indique la opción correcta

El estándar ANSI/TIA/EIA-569 A hace recomendaciones en cuanto al radio de curvatura, la fuerza de tracción y la conectorización.

- Verdadero
- Falso

## 3. Indique la opción correcta

El requerimiento TIA TSB-67 hace referencia al Mapa de cableado, la longitud, la atenuación y la paradiaphonía.

- Verdadero
- Falso

## 4. Indique la opción correcta

Los beneficios en caso de cumplir con los estándares son: la seguridad de que el cableado soportará las aplicaciones basadas en estándares, la simplificación de la administración y facilidad del crecimiento futuro.

- Verdadero
- Falso

## 5. Indique la opción correcta

¿Cuál es el estándar que especifica cómo debe hacerse el rotulado de cables?

- ANSI/TIA/EIA 568-A.
- ISO IEC 11801.
- TIA/EIA 606.
- ANSI/TIA/EIA 568-B.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Subsistema de Cableado Horizontal  
Enlace (link) en el cableado horizontal  
Canal (channel) en el cableado horizontal

va desde la caja en la pared al patch panel hasta el TC.  
va desde la NIC del Host hasta el concentrador (Switch).  
se extiende desde los puestos de trabajo hasta el TC.

## SP5 / Ejercicio resuelto

Para cumplir con lo solicitado, participar en cableado físico del nuevo edificio para poder armar esa red local (LAN), determinamos entonces que el tipo de medio físico (cableado) será de acuerdo a los estándares.

En una topología en estrella utilizaremos en cada piso cableado horizontal UTP utilizando los estándares EIA/TIA 568 A o B, basándonos en criterios estándares basados en parámetros tales como velocidad de transferencia, seguridad, longitud de los cables y facilidad de instalación.

Cada puesto de trabajo utilizará un cable de conexión Patch Cord para enlazar el host (computadora, impresora o cualquier otro equipo en la red) con la boca de conexión que lo unirá a la red

A cada puesto de trabajo llegarán, desde los armarios de telecomunicaciones (TC) dos bocas de conexión lo que configurará el cableado horizontal en cada piso.

De ser necesario se preverá también se preverá un ICC (*Intermediate Cross Connect*) en cada piso como puntos de partida para el cableado vertical.

Concentraremos en un MCC (*Main Cross Connect*) el sistema de cableado vertical o backbone. Aquí colocaremos los equipos más complejos de conectividad.

Para el armado de los conectores RJ-45 procederemos de acuerdo a los siguientes pasos:

- Paso 1: cortar un trozo de cable del tamaño adecuado.
- Paso 2: cortar el revestimiento.
- Paso 3: separar y destrenzar los pares de cables.
- Paso 4: organizar y aplanar los hilos, según TIA/EIA 568 A o B.
- Paso 5: cortar los hilos a la distancia adecuada (1/2 pulgada ó 13 mm).
- Paso 6: insertar el cable en la ficha RJ45.

Deben reunirse los alambres que forman los pares para que puedan insertarse en el Plug RJ45.

- Paso 7: empujar los hilos hacia adentro hasta que hagan tope en la ficha.
- Paso 8: inspeccionar el código de colores.
- Paso 9: engarzar (crimpear) con la herramienta adecuada (pinza de crimpear).
- Paso 10: inspeccionar ambos extremos.
- Paso 11: probar la calidad del cable con el analizador de cables (Tester LAN).

## SP5 / Ejercicio por resolver

Para fijar lo aprendido en esta SP complemente su trabajo con una descripción para los directivos de la empresa, del porque utilizar cableado UTP para el cableado horizontal y una topología tipo estrella.

Mencione en su informe cuáles son las ventajas de tomar esta decisión, frente a otras topologías y cableados, ya que ellos son los que habrán de invertir y quieren estar seguros de que la decisión que usted propone es la mejor.



¡Vamos a comprobar cuánto aprendiste!

**1. Indique la opción correcta**

En la topología bus, los nodos se conectan a través de sus placas de red a un dispositivo concentrador o hub.

- Verdadero
- Falso

**2. Indique la opción correcta**

La topología estrella se caracteriza por poseer nodos activos, ya que cada nodo participa activamente en la retransmisión de la señal.

- Verdadero
- Falso

**3. Indique la opción correcta**

Los cables que van a ser insertados en el conector plug RJ-45 deben ser cortados a una distancia de 13mm de su cobertura.

- Verdadero
- Falso

**4. Indique la opción correcta**

Canal (Channel) es el cableado que va desde la Tarjeta de Red (NIC) del Host (PC) hasta el dispositivo de comunicaciones (HUB o Switch). La distancia máxima, según TIA/EIA 569, es de 99 metros.

- Verdadero
- Falso

**5. Indique la opción correcta**

Según las características de una topología bus, los dispositivos están:

- Conectados a través de sus placas de red a un mismo medio de transmisión compartido cuyos extremos no se unen.

- Conectados a través de sus placas de red a un dispositivo concentrador del tipo Hub o Switch.
- Conectados a través de sus placas de red a un mismo medio de transmisión compartido cuyos extremos se unen.
- Conectados a través de sus placas de red a un dispositivo concentrador del tipo MAU.

**6. Indique la opción correcta**

En la topología estrella, el mal funcionamiento de un nodo:

- Afecta el funcionamiento total de la red.
- Afecta el funcionamiento parcial de la red.
- No afecta el funcionamiento de la red.
- Ninguna de las anteriores.

**7. Indique la opción correcta**

El dispositivo concentrador o HUB tiene por funcionalidad:

- Proveer encaminamiento.
- Proveer enrutamiento.
- Difundir los mensajes entre los nodos.
- Todas las anteriores.

**8. Indique la opción correcta**

Una de las características de la topología anillo es que:

- No posee extremos ni terminadores.
- Utiliza un dispositivo concentrador del tipo Hub o Switch.
- Posee nodos pasivos.
- Si falla una computadora no afecta a la red.

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

En la topología bus, los nodos se conectan a través de sus placas de red a un dispositivo concentrador o hub.

- Verdadero
- Falso

## 2. Indique la opción correcta

La topología estrella se caracteriza por poseer nodos activos, ya que cada nodo participa activamente en la retransmisión de la señal.

- Verdadero
- Falso

## 3. Indique la opción correcta

Los cables que van a ser insertados en el conector plug RJ-45 deben ser cortados a una distancia de 13mm de su cobertura.

- Verdadero
- Falso

## 4. Indique la opción correcta

Canal (Channel) es el cableado que va desde la Tarjeta de Red (NIC) del Host (PC) hasta el dispositivo de comunicaciones (HUB o Switch). La distancia máxima, según TIA/EIA 569, es de 99 metros.

- Verdadero
- Falso

## 5. Indique la opción correcta

Según las características de una topología bus, los dispositivos están:

- Conectados a través de sus placas de red a un mismo medio de transmisión compartido cuyos extremos no se unen.
- Conectados a través de sus placas de red a un dispositivo concentrador del tipo Hub o Switch.
- Conectados a través de sus placas de red a un mismo medio de transmisión compartido cuyos extremos se unen.
- Conectados a través de sus placas de red a un dispositivo concentrador del tipo MAU.

## 6. Indique la opción correcta

En la topología estrella, el mal funcionamiento de un nodo:

- Afecta el funcionamiento total de la red.
- Afecta el funcionamiento parcial de la red.
- No afecta el funcionamiento de la red.
- Ninguna de las anteriores.

## 7. Indique la opción correcta

El dispositivo concentrador o HUB tiene por funcionalidad:

- Proveer encaminamiento.
- Proveer enrutamiento.
- Difundir los mensajes entre los nodos.
- Todas las anteriores.

**8. Indique la opción correcta**

Una de las características de la topología anillo es que:

- No posee extremos ni terminadores.
- Utiliza un dispositivo concentrador del tipo Hub o Switch.
- Posee nodos pasivos.
- Si falla una computadora no afecta a la red.

# **Situación profesional 6: ¿Qué modelo de aplicación práctica utilizaremos?**

## **El Modelo TCP/IP**

Además de realizar el "cableado" de la red LAN, y estudiar los accesos al medio, la empresa debe tener acceso a Internet. Para ello debe obtener su propio dominio. Actualmente, la empresa cuenta con computadoras conectadas en red, tanto en Casa Central, como en las Sucursales. Se prevé, además, un importante crecimiento futuro. Para ello deberá conocer cómo es el modelo usado actualmente tanto en Internet como en la red privada (Intranet).

# SP6 / H1: El modelo arquitectónico de Internet

El crecimiento explosivo de Internet, que pasó de 6000 computadoras conectadas a fines de 1986 a más de 600.000 en 1991, 2.000 millones en 2011 y superó los 2.400 millones en junio de 2012, duplicándose el tráfico cada dos años, demuestra la increíble demanda de servicios de esta red, que es la más grande del mundo.

Debido a la naturaleza de las computadoras para generar y procesar información, esta tiene una serie de propiedades (por ejemplo la exactitud) de las cuales una muy interesante de ellas es la oportunidad: brindar la información en el momento que se necesita y además, que este actualizada.

Esto le da mucho valor a la información y el medio que permite que esto se produzca es, en gran medida, la red Internet, que es sin dudas la red más grande del mundo.

El conductor común que enlaza esta enorme red Internet es el software de red TCP/IP.

TCP/IP es un grupo de protocolos de comunicación que define cómo los diferentes tipos de computadoras se comunican entre sí.

Además en la actualidad existen normalmente en esta gran red no solo computadoras, sino también una gran variedad de dispositivos tales como notebooks, tablets, teléfonos inteligentes y hasta televisores que hacen uso de la red Internet. Todos estos dispositivos utilizan para comunicarse el grupo de protocolos de comunicación TCP/IP

## Una visión de TCP/IP

La conectividad de los sistemas de computación como ingeniería, educación, científicos y de negocios, ha generado una nueva actividad conocida como la administración de red.

La administración de red y administración de sistemas son dos tareas diferentes.

Las tareas del administrador de sistemas son tales como agregar usuarios y hacer backups de sistema de computación aislado. No es lo mismo que el administrador de red, ya que éste interactúa con otros sistemas y las acciones que tome, no sólo pueden tener efecto en el propio sistema, sino en otros.

TCP/IP es uno de los paquetes de software que domina la comunicación de datos. Éste juega un rol importante como software de comunicaciones para las redes actuales.

El nombre TCP/IP se refiere a un conjunto completo de protocolos de comunicación. Este conjunto lleva el nombre de dos de los principales protocolos: TCP (Transmission Control Protocol) e IP (Internet Protocol). No obstante ello, existen en este grupo muchos otros protocolos.

## TCP/IP e Internet

En 1969, DARPA (Defense Advanced Research Projects Agency) fue fundada para investigar y desarrollar un proyecto para crear una red experimental de conmutación de paquetes. Esta red, llamada ARPANET, fue definida y construida para estudiar técnicas para la provisión de sistemas de comunicación robustos y seguros, independiente de los proveedores.

Muchas de las técnicas de comunicación de datos fueron desarrolladas en ARPANET.

La red experimental tuvo éxito, ya que muchas de las organizaciones conectadas a ella la comenzaron a usar para la comunicación de datos cotidiana.

En 1975 ARPANET fue convertida desde una red experimental a una red operacional y la responsabilidad de administración de la red fue dada al DCA (*Defense Communications Agency*), cuyo nombre fue luego cambiado por DISA (*Defense Information Systems Agency*).

El desarrollo de ARPANET no paró debido al uso de la red operacional; el protocolo básico TCP/IP fue desarrollado después que ARPANET se transformó en operacional.

El protocolo TCP/IP fue adoptado como "Estándar Militar" (MIL STD) en 1983 y todos los host conectados a la red fueron convertidos al nuevo protocolo. En el tiempo que TCP/IP fue adoptado como estándar, el término "Internet" comenzó a tener un uso común. En 1983, la vieja ARPANET fue dividida en MILNET, la parte clasificada de la Red de Defensa (DDN = *Defense Data Network*) y una ARPANET más pequeña.

El término "Internet" fue usado para referirse a la red completa, MILNET más ARPANET.

En 1990, la ARPANET dejó de existir formalmente, pero actualmente Internet es más grande y comprende muchas redes en todo el mundo.

Existe cierta confusión en el término "internet" (con minúscula). Originalmente éste fue usado sólo como el nombre de la red construida bajo el Protocolo Internet.

Actualmente el término "internet" es una expresión genérica usada para referirse a una clase de red.

Una "internet" es una colección de redes físicamente separadas, interconectadas por un protocolo común, para formar una red lógica única.

"Internet" (con I mayúscula) es la colección mundial de redes interconectadas, la cual crece fuera de ARPANET original, que usa el protocolo IP (*Internet Protocol*) para enlazar varias redes físicas en una red lógica única.

Dado que es requerido TCP/IP para una conexión "Internet", es necesario comprender y poner un especial interés en TCP/IP.

El protocolo de Internet es a menudo usado para interconectar redes locales, aun cuando la red local no está conectada a la gran Internet. Es común usar TCP/IP para comunicarse sobre una LAN Ethernet, es decir utilizar la tecnología de Internet para una red local, lo cual ha dado en llamarse "intranet" o "Intranet".

## Un modelo de comunicaciones de datos

Para discutir la conectividad entre computadores, es necesario usar términos que tienen especial significado en la comunicación de datos. Una referencia común es necesaria para comprender la terminología de la comunicación.

El modelo desarrollado por la International Standard Organization (ISO), conocido como "Modelo de Referencia OSI" (*Open System Interconnection*), que ya hemos estudiado anteriormente, es frecuentemente usado para describir la estructura y funciones de los protocolos de comunicaciones de datos. Este modelo provee una referencia común para la discusión de comunicaciones.

No obstante haber ya estudiado el modelo de referencia OSI, vamos a hacer un pequeño repaso que nos llevará a entender cómo es el funcionamiento del conjunto TCP/IP. Como ya sabemos, OSI contiene 7 capas que definen las funciones de los protocolos de comunicaciones de datos. Cada una de las capas representa una función característica, cuando los datos son transferidos entre aplicaciones cooperativas a través de una intervención de la red.

A continuación se provee una identificación de cada una de las capas, una breve descripción funcional. Contemplando al Modelo de Referencia OSI, el protocolo es semejante a un conjunto de bloques apilados unos sobre otros. Debido a esta presentación, la estructura es frecuentemente llamada una pila (stack) o pila de protocolos (protocol stack).

Una capa no define un único protocolo, sino que define una función de comunicación de datos que puede ser caracterizada por muchos protocolos. Además, cada una de las capas puede contener múltiples protocolos, cada uno proveyendo un servicio adecuado para la función de la capa. Por ejemplo, un protocolo de transferencia de archivos y un protocolo de correo electrónico, ambos proveen servicios a usuarios y ambos son parte de la capa de Aplicación.

Cada uno de los protocolos de comunicación tiene su igual (peer). Un "peer" es una implementación del mismo protocolo en la capa equivalente sobre un sistema remoto; por ejemplo, el protocolo de transferencia de archivos es un "peer" de un protocolo de transferencia de archivos remoto.

En forma abstracta, cada uno de los protocolos se comunica sólo con su par de la misma capa y no se preocupa de la capa inferior ni superior.

No obstante, debe también acordar cómo pasará los datos entre las capas del mismo host, debido a que cada capa está involucrada en el envío de datos desde una aplicación local a su aplicación remota equivalente. Las capas superiores confían en las capas inferiores para transferir los datos sobre la red subyacente.

Los datos son pasados hacia abajo en la pila desde una capa a la próxima, hasta que son transmitidos sobre la red por el Protocolo de Capa Física. En el extremo remoto, los datos son pasados hacia arriba de la pila hasta la aplicación receptora.

Cada capa individualmente no necesita saber cuál es la función de la capa inferior o superior; sólo necesita saber cómo pasar los datos entre ellas.

Al aislar las funciones de comunicación en diferentes capas, se minimiza el impacto de los cambios tecnológicos de todo el conjunto de protocolos. Pueden agregarse nuevas aplicaciones sin cambiar la red física y puede ser instalado nuevo hardware sin rescribir el software de aplicación.

Si bien el modelo OSI es eficiente, los protocolos TCP/IP no son exactamente iguales a esta estructura. Por lo tanto, en la discusión de TCP/IP, pueden usarse las capas del modelo OSI en los siguientes sentidos:

- **CAPA DE APLICACIÓN:** consiste de programas de aplicación que usa la red. Es el nivel donde los usuarios acceden a los procesos de la red. En este contexto, una aplicación TCP/IP es cualquier proceso de red que ocurre por debajo de la Capa de Transporte. Esto incluye todos los procesos que actúan directamente con los usuarios.
- **CAPA DE PRESENTACIÓN:** estandariza la presentación de los datos para las aplicaciones cooperativas para intercambio de datos, deben convenir acerca de cómo son representados los datos. En OSI, esta capa provee rutinas de presentación de datos estándar; esta función es manejada, en TCP/IP dentro de la capa de aplicación.
- **CAPA DE SESIÓN:** administra sesiones entre aplicaciones. Como sucede con la Capa de Presentación, la Capa de Sesión no es una capa separadamente identifiable en la jerarquía de protocolos TCP/IP. En el modelo OSI, la Capa de Sesión maneja las sesiones (conexiones) entre aplicaciones cooperativas. En TC-P/IP esta función en gran parte ocurre en la Capa de Transporte y el término "sesión" no es usado. Para TCP/IP, son usados los términos "conexión o socket" y "puerto" (port) para describir el camino sobre el cual se comunican las aplicaciones cooperativas.
- **CAPA DE TRANSPORTE:** provee detección y corrección de errores extremo a extremo y

acondicionamiento de los mensajes a la capa de Red. Muchas de las discusiones de TCP/IP, están referidas a lo que ocurre con los protocolos en la Capa de Transporte. En esta capa del modelo OSI, se garantiza que el receptor obtenga los datos exactamente como fueron emitidos. En TCP/IP esta función es realizada por el "Transmission Control Protocol" (TCP). No obstante, TCP/IP ofrece un segundo servicio de Capa de Transporte, el "User Datagram Protocol" (UDP), que no realiza el chequeo de exactitud extremo a extremo (end-to-end).

- **CAPA DE RED:** administra conexiones a través de la red para las capas superiores. Provee encaminamiento para los datos. La Capa de Red administra conexiones a través de la red y aísla los protocolos de capas superiores de los detalles de la red subyacente. El "Internet Protocol" (IP), es el que aísla las capas superiores de la red y maneja las direcciones y entrega de datos y es usualmente descrito como la Capa de Red del TCP/IP.
- **CAPA DE ENLACE DE DATOS:** provee acceso al medio de comunicación o enlace físico. La entrega segura de los datos a través de la red subyacente es manejada por la Capa de Enlace de Datos. TCP/IP raramente crea protocolos en la Capa de Enlace de Datos. La mayoría de los RFC que se relacionan con la Capa de Enlace de Datos discuten acerca de cómo IP puede hacer uso de los protocolos de enlace de datos existentes.
- **CAPA DE FÍSICA:** define las características físicas de los medios de red y del hardware necesario para transportar la señal de transmisión de datos. Asuntos tales como niveles de tensión eléctrica y el número y ubicación de los pines (pinup), son definidos en esta capa. Ejemplos de estándares de Capa Física son las interfaces de conexión, tales como RS-232-C, V.35 y TIA/EIA 568 A y B y estándares para cableado de redes de red local tales como IEEE 802.3. TCP/IP no definen estándares físicos sino que hacen uso de los estándares existentes.

La terminología del modelo de referencia OSI ayuda a describir a TCP/IP, pero no a comprenderlo completamente; para ello usaremos el modelo de arquitectura que más se asemeja a la estructura de TCP/IP.

## Protocolos estándar

Los protocolos son reglas formales de comportamiento. En relaciones internacionales, los protocolos minimizan el problema causado por diferencias culturales, cuando varias naciones trabajan juntas. Por convención, se generan un grupo de reglas comunes, que son ampliamente conocidas por cualquier nación; los protocolos diplomáticos minimizan los conocimientos de cómo otros interpretan la acción.

Similarmente, cuando se comunican las computadoras es necesario definir un conjunto de reglas para gobernar esas comunicaciones.

En comunicación de datos, estos grupos de reglas son también llamados "protocolos".

En redes homogéneas, un único computador (servidor) especifica las reglas de comunicación a ser usada por el sistema operativo y arquitectura del hardware; por ejemplo, lo que sucede en una red LAN (Ethernet, Token Ring, etc.). Pero las redes homogéneas son semejantes a la cultura de un único país, solo los nativos las comprenden.

TCP/IP intenta crear una red heterogénea con protocolos abiertos independientes de los sistemas operativos y diferentes arquitecturas de red. Los protocolos TCP/IP están disponibles para todos y son desarrollados y cambiados por consenso, no por capricho de un fabricante. Todos están liberados para desarrollar productos que reúnan las especificaciones de protocolo abierto.

La naturaleza de los protocolos TCP/IP requieren documentos de estándares disponibles públicamente. Todos los protocolos en la serie TCP/IP están definidos en una de las tres publicaciones Internet estándar. Un número de protocolos ha sido adoptado como *Military Standards* (MIL STD).

Toda la información acerca de TCP/IP es publicada como "Requests for Comments" (RFC) conteniendo las últimas versiones de las especificaciones de los protocolos TCP/IP.

Como lo indica el nombre "Request For Comments", el estilo y contenido de esos documentos es mucho menos rígido que la mayoría de los estándares.

Los RFC contienen un amplio rango de información de interés y no están limitado a la formal especificación de los protocolos de comunicaciones de datos.

El administrador de red debe leer muchos de esos documentos. Algunos contienen noticias prácticas y guías que simplifican la comprensión. Otros RFC contienen implementación de protocolos definidos en terminología que es única para la comunicación de datos.



¿Te animás a medir cuánto aprendiste?

**1. Indique la opción correcta**

La administración de sistemas y administración de red son la misma tarea, ambos conceptos hacen referencia a las mismas funciones.

- Verdadero
- Falso

**2. Indique la opción correcta**

El conjunto de protocolos sobre el que funciona Internet se conoce como:

- Ethernet.
- Token Ring.
- CSMA/CA.
- TCP/IP.

**3. Indique la opción correcta**

La red sobre la cual se basó la construcción de Internet se llamó:

- Intranet.
- Ethernet.
- CSMA/CA.
- ARPANET.

**4. Indique la opción correcta**

Un protocolo es:

- Una de las capas del modelo de referencia OSI.
- Un conjunto de reglas formales de comportamiento.
- Un estándar para el cableado de redes.
- Un estándar para el armado de los conectores.

**5. Indique la opción correcta**

La información acerca de TCP/IP se pueden encontrar en documentos denominados:

- Estándares ANSI/TIA/EIA.
- Estándares ISO/IEC.
- Request For Comments.
- 802.3 y sus grupos de trabajo

## 6. Ordene relaciones

En la discusión TCP/IP pueden usarse las capas del modelo OSI en los siguientes sentidos:

Capa Física	Provee encaminamiento para los datos
Capa de Enlace	Define las características físicas de los medios de red
Capa de Red	Provee acceso al medio de comunicación
Capa de Transporte	Provee detección y corrección de errores extremo a extremo

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

La administración de sistemas y administración de red son la misma tarea, ambos conceptos hacen referencia a las mismas funciones.

- Verdadero
- Falso

## 2. Indique la opción correcta

El conjunto de protocolos sobre el que funciona Internet se conoce como:

- Ethernet.
- Token Ring.
- CSMA/CA.
- TCP/IP.

## 3. Indique la opción correcta

La red sobre la cual se basó la construcción de Internet se llamó:

- Intranet.
- Ethernet.
- CSMA/CA.
- ARPANET.

## 4. Indique la opción correcta

Un protocolo es:

- Una de las capas del modelo de referencia OSI.
- Un conjunto de reglas formales de comportamiento.
- Un estándar para el cableado de redes.
- Un estándar para el armado de los conectores.

## 5. Indique la opción correcta

La información acerca de TCP/IP se pueden encontrar en documentos denominados:

- Estándares ANSI/TIA/EIA.
- Estándares ISO/IEC.
- Request For Comments.
- 802.3 y sus grupos de trabajo

## 6. Ordene relaciones

En la discusión TCP/IP pueden usarse las capas del modelo OSI en los siguientes sentidos:

Capa Física	Provee acceso al medio de comunicación
Capa de Enlace	Provee encaminamiento para los datos
Capa de Red	Provee detección y corrección de errores extremo a extremo
Capa de Transporte	Define las características físicas de los medios de red



## SP6 / H2: Arquitectura TCP/IP: capas de acceso a la red e Interred

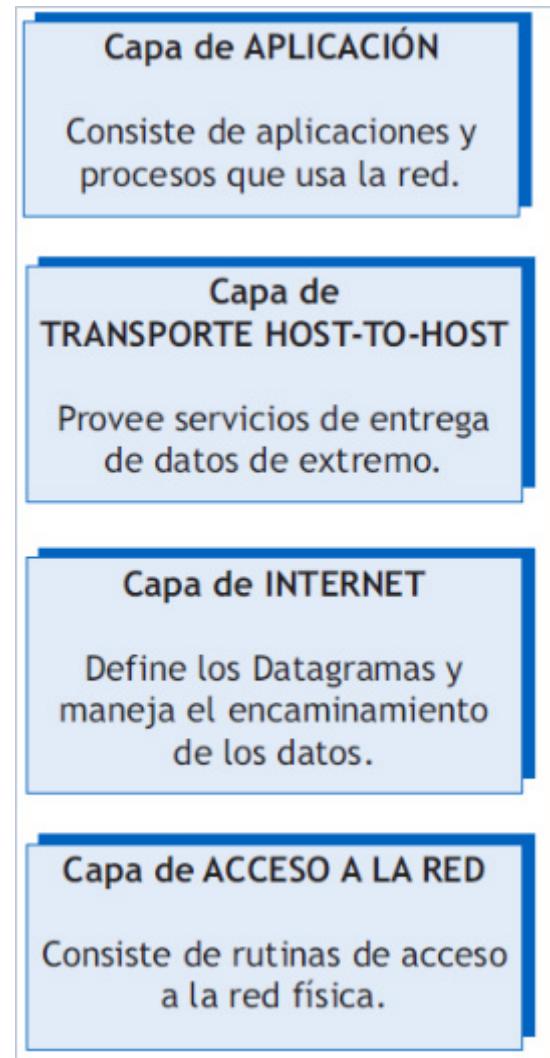
La arquitectura TCP/IP está basada sobre una visión de comunicaciones que involucra tres agentes:

- Procesos.
- Hosts.
- Redes.

Los procesos son las entidades fundamentales que se comunican. Un ejemplo es una operación de transferencia de archivos (File Transfer). En este caso, un proceso de transferencia de archivos en un sistema que intercambia datos con un proceso de transferencia de archivos sobre otro sistema. Otro ejemplo es el "logon" remoto en el cual un usuario es conectado a un sistema y controlado por el proceso de administración de terminales. El usuario puede ser remotamente conectado a un sistema de tiempo compartido; entonces los datos son intercambiados entre el proceso de manejo de terminales en un computador y el sistema de tiempo compartido del otro. Los procesos se ejecutan sobre los host, los cuales, a menudo, pueden soportar procesos múltiples simultáneos. Los host son conectados por redes y los datos a ser intercambiados son transmitidos por la red desde uno a otro host. Estos tres conceptos producen el principio fundamental de la arquitectura.

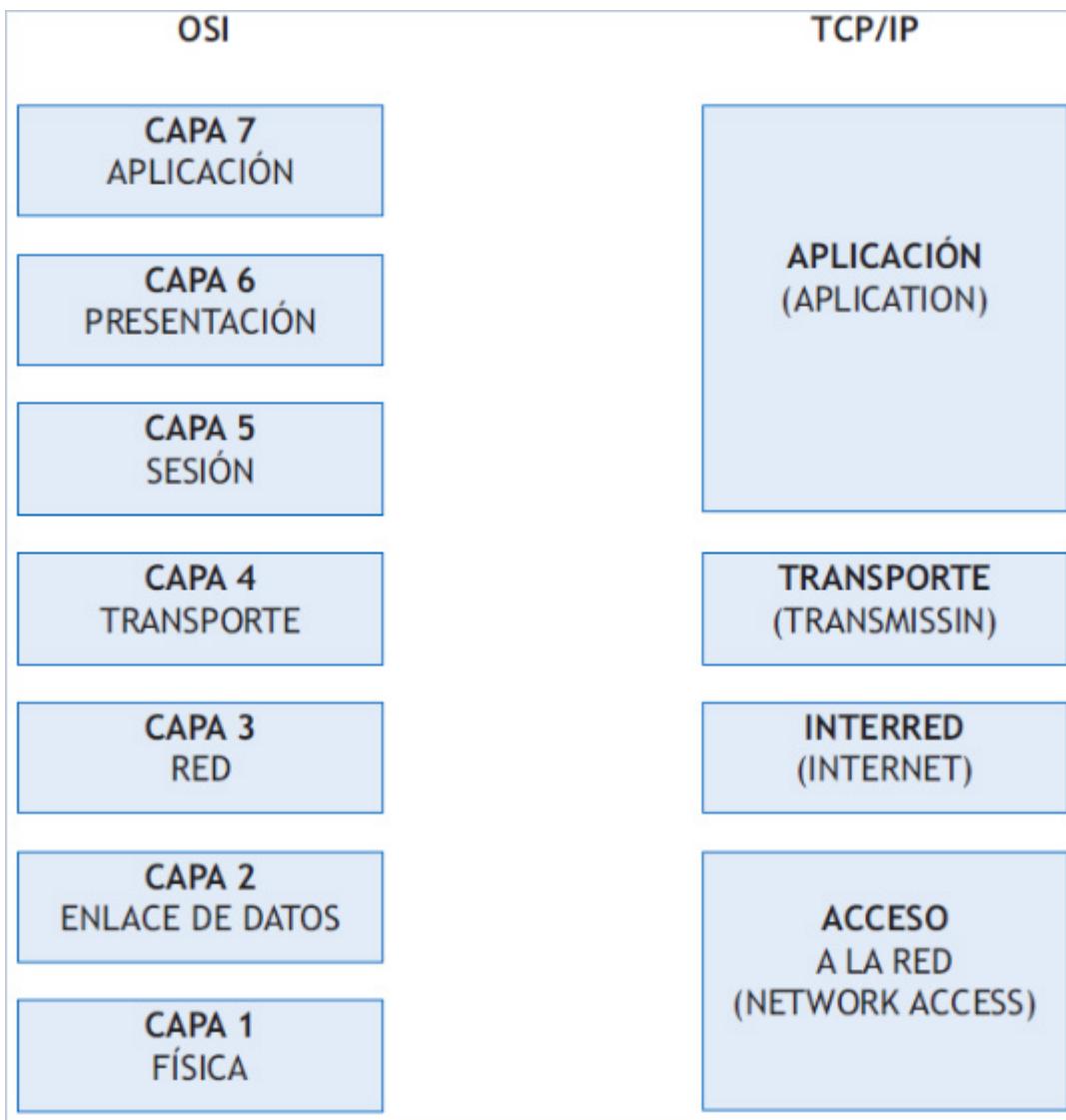
Mientras no hay un acuerdo universal acerca de cómo describir a TCP/IP mediante un modelo de capas, es generalmente estudiado con menos capas que las del modelo OSI. Usando estos conceptos es natural organizar el protocolo en cuatro capas.

Los cuatro niveles del modelo mostrados en el siguiente cuadro representan gráficamente la jerarquía de protocolos TCP/IP.



"Cuatro niveles del modelo" | *Elaboración Autor*

Decíamos que el Modelo TCP/IP consta de menos capas que el OSI, sólo tiene 4. También decíamos que esto no significa que TCP/IP tenga que realizar menos funciones sino que varias de ellas no se encuentran discriminadas en capas distintas. La equivalencia entre ambos modelos se muestra en la siguiente figura:



En el modelo TCP/IP las tres capas superiores de OSI se encuentran englobadas en una única capa, y sobre las dos capas inferiores, TCP/IP, no revela detalles, dejando a los protocolos ya estandarizados la función de presentar el acceso a la red o acceso al medio.

Otra diferencia se da en las capas inferiores, ya que TCP/IP no establece características para las capas que se encuentren debajo de la capa de Internet (Red); los diseñadores de TCP/IP confiaron plenamente en las soluciones que la industria había establecido, siempre que fueran capaces de comunicarse con la capa Internet, y dado que aquéllas se apoyan fundamentalmente en OSI, es natural considerar que TCP/IP tiene las mismas capas bajas.

Sin entrar en detalles (ya lo hicimos anteriormente), simplemente comentaremos que las capas bajas de ambos modelos se encargan de las topologías de red, las placas de red, los cableados y la forma eléctrica en que se transmitirán los bits a través del medio.

El modelo define protocolos para las tres capas superiores, a saber:

- Capa Proceso/**Aplicación**: Protocolo de Transferencia de Archivos (FTP = File Transfer Protocol),

Protocolo Simple de Transferencia de Correo (SMTP = Simple Mail Transfer Protocol), TEL-NET, HTTP y otros.

- Capa de **Transmisión** (Host-to-Host): Protocolo de control de Transmisión (TCP = Transmission Control Protocol).
- Capa **Internet**: Protocolo Internet (IP = Internet Protocol).

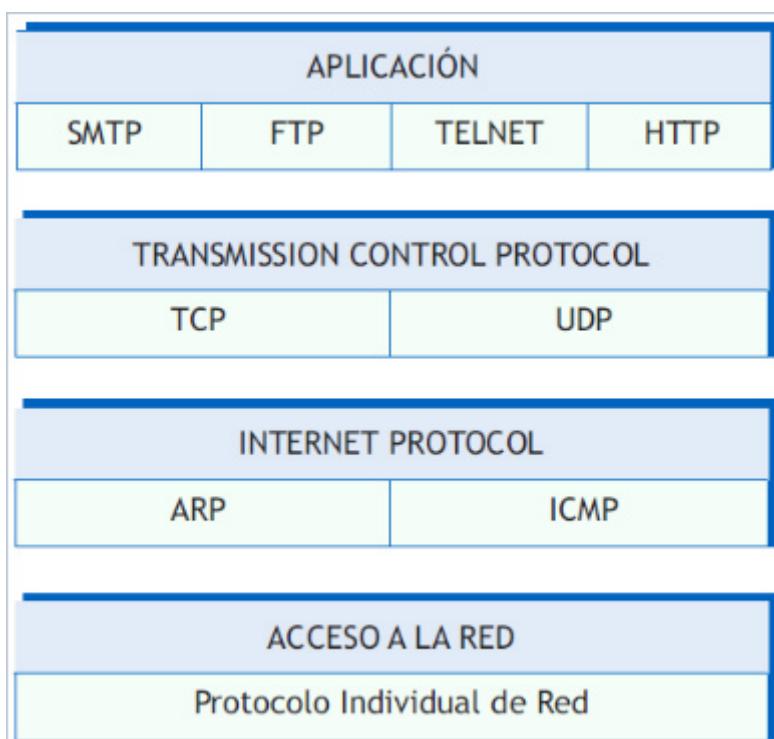
En la capa de **Acceso a la Red**, el host puede tener interfaces a una variedad de redes. Por lo general TCP/IP confía en los estándares internacionales tales como Ethernet y Token Ring para redes LAN y X.25, PPP, Frame Relay, ISDN, etc. para redes WAN.

Como en el modelo OSI, los datos son pasados hacia abajo en la pila cuando son enviados a la red y hacia arriba, cuando son recibidos desde la red.

La estructura de cuatro capas de TCP/IP será vista en el sentido de manejo de los datos como pasando desde arriba hacia abajo de la pila de protocolos, o sea desde la Capa de Aplicación a la red física subyacente.

Cada capa en la pila agrega información de control para asegurar la entrega apropiada. Esta información de control es llamada "Encabezamiento" (Header) debido a que es ubicado al comienzo de los datos a ser transmitidos. Cada capa trata toda la información recibida de su capa superior como "datos" y agrega su propio encabezamiento al frente de la información.

El siguiente cuadro nos muestra algunos de los protocolos usados por TCP/IP en las distintas capas. En realidad, los protocolos de la Capa de Acceso a la Red, no son definidos en los RFC.



"Relación entre los protocolos Internet" | *Elaboración autor*

En realidad TCP/IP se dedica a las capas de TRANSPORTE y RED respectivamente, del modelo OSI.

Por eso podemos decir que los protocolos TCP/IP constan de dos capas específicas: la superior (TCP) y la inferior.

En la capa superior está el protocolo de extremo a extremo (TCP), que asegura que un paquete cumpla todo el recorrido en una trayectoria multisalto.

La capa inferior (IP) corresponde a un protocolo para nodos adyacentes y consiste en crear un canal confiable para la transmisión de paquetes. Esto nos lleva a pensar, que si cada salto entre nodos es confiable, todo el camino es confiable, por lo que no sería necesario un protocolo de extremo a extremo, pero pueden fallar los nodos inmediatamente después de haber realizado la transmisión y por lo tanto el camino se interrumpirá.

TCP/IP no tiene realmente un protocolo de enlace, por lo que el acceso al medio puede estar dado por distintos medios, como puede ser Ethernet, Token Ring o FDDI en una LAN, o PPP, X.25, Frame Relay u otros en una WAN.

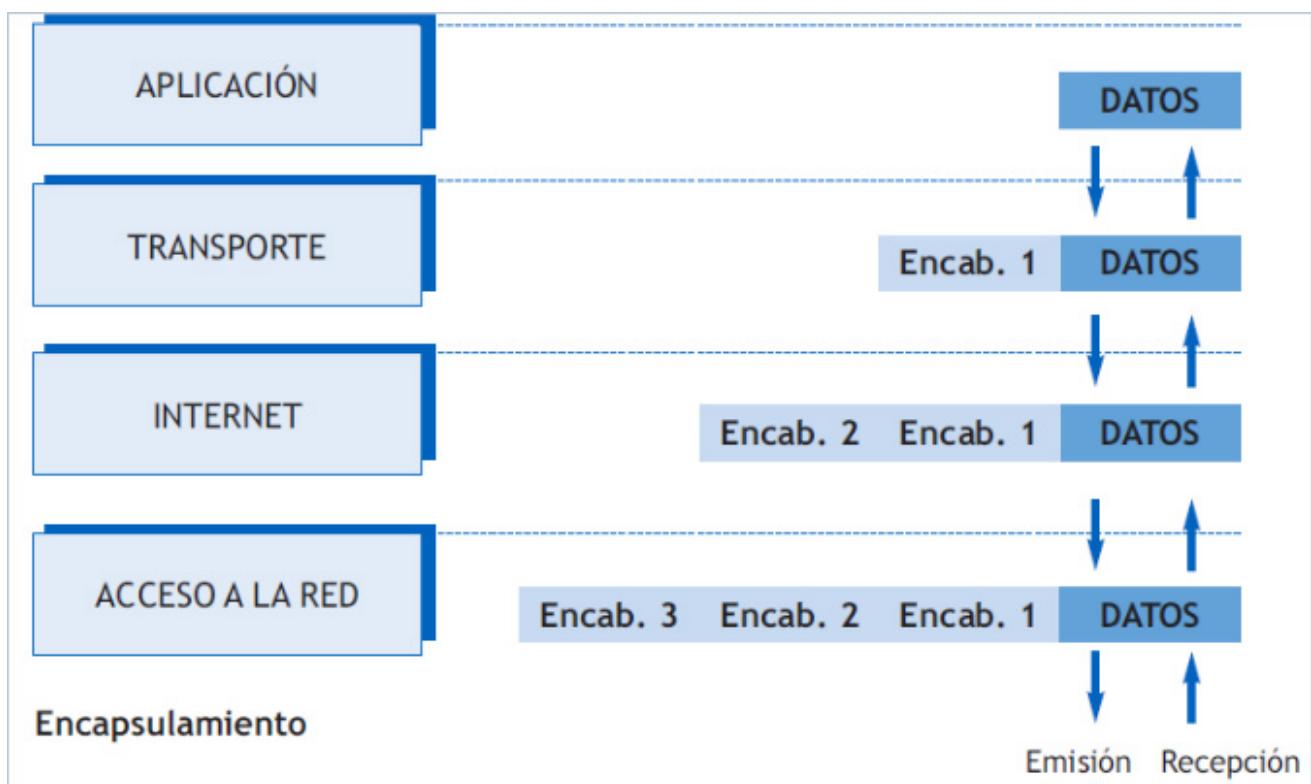
#### La transmisión del flujo de datos se realiza de la siguiente manera:

El Sistema Operativo del Host emisor envía el flujo de datos en mensajes prefijados de hasta 8063 bits con cabeceras de 40 bits. Estos mensajes son transmitidos por la subred en forma transparente.

El agregado de información por cada una de las capas es llamado "encapsulamiento" (encapsulation). Esto es mostrado en la figura siguiente.

Cuando los datos son recibidos, sucede lo opuesto. Cada una de las capas extrae el encabezamiento correspondiente antes de pasar los datos hacia arriba. En el flujo ascendente, la información recibida desde las capas inferiores es interpretada como encabezamiento y datos.

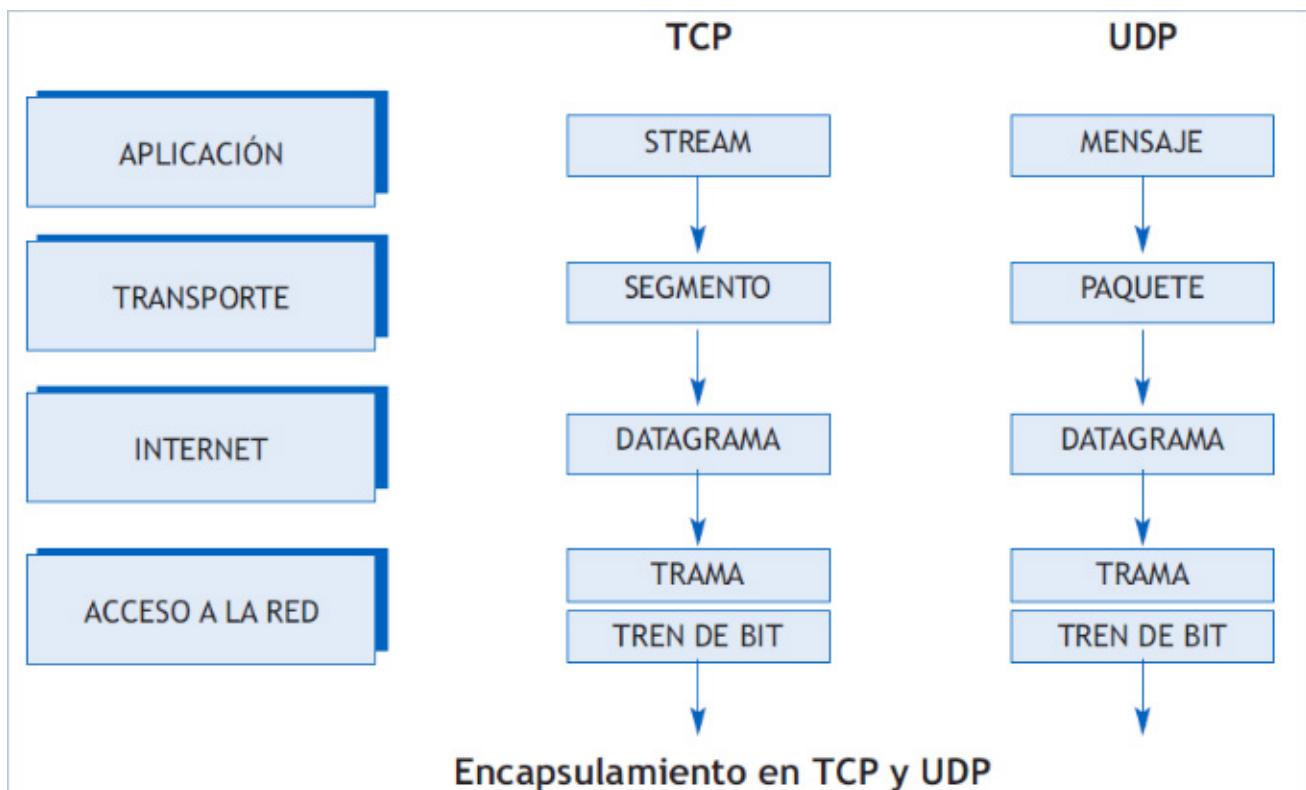
En la figura puede apreciarse cómo se realiza el encapsulamiento en TCP/IP:



"El encapsulamiento en TCP/IP" | Elaboración autor

Cada una de las capas tiene su propia estructura de datos independiente. Conceptualmente, una capa desconoce la estructura de datos usada por la capa superior e inferior. En realidad, la estructura de datos de

una capa está diseñada para ser compatible con la estructura usada por la capa adyacente para hacer más eficiente la transmisión. Sin embargo, cada capa tiene su propia estructura y su propia terminología para describir esa estructura.

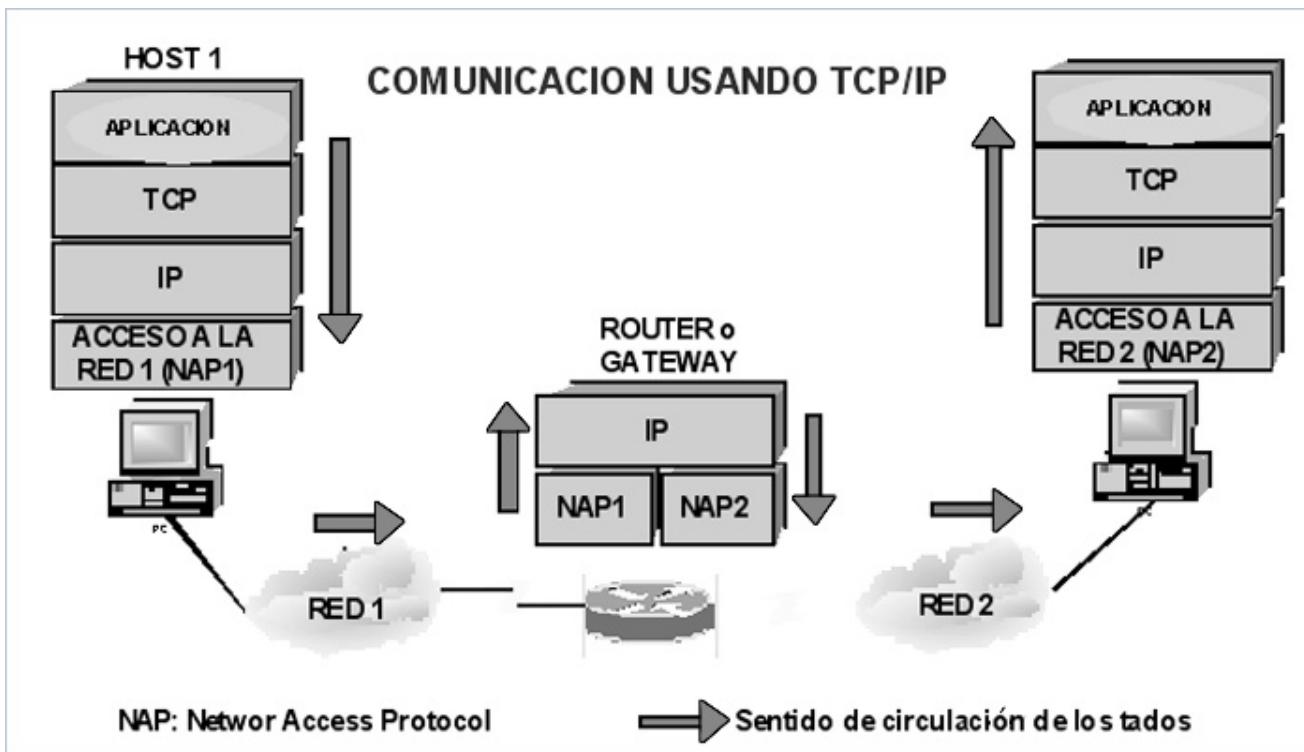


"Encapsulamiento en TCP y UDP" | Elaboración Autor

La figura muestra los términos usados por las diferentes capas de TCP/IP para referirse a las estructuras de datos transmitidos. Las aplicaciones de TCP se refieren a los datos como un "flujo o corriente" (*stream*), mientras las aplicaciones que usan UDP lo llaman "mensajes" (*message*). TCP llama a los datos "segmentos" (*segment*) y UDP los llama "paquetes" (*packets*). La capa Internet ve a los datos como bloques llamados "datagramas" (*datagrams*).

TCP/IP usa diferentes tipos de redes subyacentes, cada una de las cuales puede tener diferentes terminologías para los datos transmitidos. Muchas redes se refieren a los datos transmitidos como "paquetes" o "tramas". En la figura que vimos y en la siguiente, se asume que la red transmite piezas de datos llamadas "tramas" (*frames*).

La capa de Acceso a la Red tiene que ver con el intercambio de datos entre un host y la red a la cual está conectada. El host emisor debe proveer a la red la dirección del host destino, de manera que la red pueda encaminar los datos apropiadamente.



El protocolo específico usado en esta capa depende del tipo de red a ser usada. Diferentes protocolos han sido desarrollados para redes de conmutación de circuitos (p. ej. X.21), redes de conmutación de paquetes (p. ej. X.25), redes de área local (p. ej. ISO 8802, IEEE 802.x, FDDI) e ISDN. De esta manera, habrá que distinguir para separar esas funciones manteniendo el acceso a la red en capas separadas. Haciendo esto, el resto del software de comunicación por encima de la capa de acceso a la red no necesita ser relacionado con las especificaciones de la red a ser usada.

Veremos a continuación en forma resumida las características principales de las cuatro capas del modelo TCP/IP. En las Situaciones Profesionales posteriores profundizaremos en las específicas: en las SP8 y SP9 veremos en profundidad la capa INTERRED o INTERNET que corresponde a la capa RED del modelo OSI y en la SP10 la capa de TRANSPORTE equivalente a la capa TRANSPORTE del modelo OSI.

## Capa de Acceso a la Red

Ésta es la capa más baja del modelo TCP/IP. La capa de acceso a la red encamina datos entre dos dispositivos conectados a la misma red.

El protocolo en esta capa provee el medio para que el sistema pueda enviar datos a otro dispositivo conectado directamente a la red. Este define cómo usar la red para transmitir un paquete IP. Distinto de los protocolos de alto nivel, el Protocolo de Acceso a la Red debe conocer los detalles de la red subyacente (estructura de paquetes, direccionamiento, etc.) para dar el formato correcto a los datos que van a ser transmitidos, dando cumplimiento a lo impuesto por la red.

Esta Capa de Acceso a la Red es frecuentemente ignorada por los usuarios. El diseño de TCP/IP oculta las funciones de las capas inferiores y el mejor conocimiento de los protocolos (IP, TCP, UDP, etc.) se refiere a todos los protocolos de alto nivel.

En la medida en que aparece nueva tecnología, se desarrollan nuevos protocolos de Acceso a la Red, de modo que las redes TCP/IP pueden usar el nuevo hardware. Consecuentemente, tienen muchos protocolos de acceso, uno por cada estándar de red física.

Las funciones desempeñadas en este nivel incluyen encapsulamiento de los datagramas IP dentro de tramas transmitidas por la red y representación (mapeado) de direcciones IP para el direccionamiento físico usado por la red. Una de las ventajas de TCP/IP es este esquema de direccionamiento que identifica únicamente cada uno de los host en la Internet. Esta dirección IP (dirección lógica) debe ser convertida a una dirección física sobre la cual el datagrama será transmitido.

Dos ejemplos de RFC que definen protocolos de acceso a la red son:

- RFC 826 - *Address for the Transmission Protocol* (ARP): que permiten resolver direcciones Físicas (MAC Address) a partir de direcciones IP para direccionamiento Ethernet.
- REF 894 - *A Standard for the Transmission of IP Datagrams over Ethernet Networks*: los cuales especifican cómo son encapsulados los paquetes para su transmisión sobre redes Ethernet.

## Capa Interred o Internet

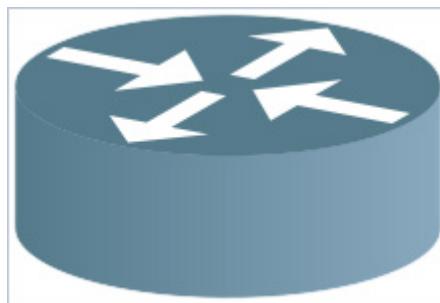
En los casos, donde dos host son conectados a diferentes redes, son necesarios procedimientos para permitir que los datos atravesen múltiples redes. Ésta es la función de la Capa Internet.

El nivel por encima de la Capa de Acceso a la Red en la jerarquía de protocolos es la "Capa Internet". El Protocolo Internet (RFC 791), es el corazón de modelo TCP/IP y el más importante protocolo en la Capa Internet. El Internet Protocol (IP) provee el servicio básico de entrega de paquetes sobre la cual la red TCP/IP está construida. Todos los protocolos, en la capa superior e inferior a IP, usan el IP para la entrega de datos. Todo el flujo de datos TCP/IP pasa a través de IP, tanto de entrada (*incoming*) como de salida (*outgoing*), sin considerar el destino final.

El protocolo IP se introdujo a comienzo de la década del 80. A partir de aquí muchas redes lo han adoptado, por lo general en conjunto con TCP, que analizaremos más adelante, cuando veamos la capa de transporte.

Un protocolo internet es usado por esta capa para proveer la función de encaminamiento a través de múltiples redes. Este protocolo es implementado no sólo en el host, sino también en el "*gateway o router*" (originalmente en TCP/IP se conocían como "*gateway*", y en este texto usaremos ambos nombres)

Un "*router*" es un equipamiento que **sirve para conectar dos o más redes**, cuya función primaria es retransmitir datos de una red a otra eligiendo el camino correcto (**encaminamiento**). La siguiente imagen representa un router:



"Router figura" | <http://upload.wikimedia.org/wikipedia/commons/thumb/5/5c/Router.svg/220px-Router.svg.png>

Actualmente se prefiere reservar el término "**gateway**" (puerta de enlace) a los dispositivos que, cumpliendo las funciones de "routers" **interconectan redes con protocolos y arquitecturas diferentes a todos los niveles**. Su propósito, además de encaminar, es también traducir la **información de protocolo utilizada en una red, al protocolo utilizado en la red destino**.

Esta capacidad para traducir diferentes direcciones (NAT: *Network Address Translation*) permite que podamos mediante estos equipos dar acceso a Internet a los hosts de una red de área local compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa. Por esta función se los llama Puerta de Enlace Predeterminada o *Default Gateway*.

Como ejemplo en nuestros hogares podemos ver entonces routers funcionando como gateways.

## Protocolo Internet

Las grandes redes de conmutación de paquetes y las redes de área local van más allá del sólo hecho de permitir que los usuarios tengan acceso a recursos disponibles dentro de un simple sistema de computación. Los recursos de una sola red son a menudo inadecuados para las necesidades de los usuarios. Lo que se necesita es la capacidad para interconectar varias redes, de manera que las estaciones de las redes constituyentes puedan comunicarse.

Un grupo de redes interconectadas se conoce como una "internet". Cada red constituyente soporta comunicación hacia los dispositivos conectados. Además, las redes están conectadas por dispositivos conocidos como "**gateways**" o "**routers**".

El protocolo IP es implementado en cada host y en cada router. El protocolo IP corriendo en un host acepta datos en bloques, o unidad de datos de protocolos (PDU = *Protocol Data Unit*), que son enviados desde el protocolo de Capa de Transmisión (TCP o UDP), que lo envía entonces a través de la internet, pasando por tantos routers como fuera necesario, hasta que alcancen el destino.

El protocolo IP provee lo que es conocido como un inseguro servicio no orientado a conexión; por esta razón, algunos PDU nunca podrán conseguir llegar al otro extremo y otros pueden arribar fuera de secuencia. Esto es lo máximo que se asegura como exactitud en la entrega de datos.

La operación de IP puede ser descrita considerando dos *Host*, "A" y "B", sobre diferentes redes en la internet. El Host A envía datos al Host B. El proceso comienza en el host A. El módulo IP en el host A construye una PDU, que consiste de datos provenientes del TCP, más información de control usada por IP. La PDU es enviada a través de la red conectada al router apropiado.

Cuando el router recibe la PDU, son posibles dos escenarios de encaminamiento:

- El host destino (B) está conectado directamente a la red a través del gateway. Si es así, el módulo IP del router envía la PDU a través de la red a "B".
- Para alcanzar el host destino, deben atravesarse uno o más routers adicionales. Si es así, la PDU es enviada a través de la red al próximo router en la ruta apropiada.

De esta manera, el módulo IP en un *host* o *gateway* debe tener información que le permita proclamar la decisión de encaminamiento apropiada. Además, esto debe promover el empleo del protocolo de acceso apropiado para que sea posible enviar datos a través de cada red a la cual está conectado.

El Protocolo Internet es un bloque constructivo de Internet. Sus funciones incluyen:

- Definición de datagramas, que es la unidad básica de transmisión en la Internet.
- Definición del esquema de direccionamiento Internet.

- Movimiento de datos entre la Capa de Acceso a la Red y la Capa de transporte Host-to-Host.
- Encaminamiento de los paquetes al Host remoto.
- Ejecución de la fragmentación y re-ensamblado de paquetes.

Antes de describir en detalle estas funciones, veamos algunas características de IP. IP es un "protocolo no orientado a conexión". Esto significa que IP no intercambia información de control (llamada "*handshake*") para establecer una conexión extremo a extremo antes de la transmisión de datos. En contraste, un "protocolo orientado a conexión" intercambia información de control con el sistema remoto para verificar que está en condiciones de recibir datos, antes de que le sean enviados. Cuando el "*handshaking*" es exitoso, el sistema está en condiciones de establecer una "conexión".

El Protocolo Internet confía en que protocolos de otras capas de la arquitectura TCP/IP proveen este control, cuando son requeridos servicios orientados a conexión.

El protocolo IP trabaja de la siguiente manera: la capa de transporte toma los mensajes y los divide en segmentos o datagramas de hasta 64 kbytes cada uno. Cada segmento se transmite a través de la red, posiblemente fragmentándose en unidades más pequeñas.

Al final, cuando todas las piezas llegan al destino, la capa de transporte las re-ensambla para reconstituir el mensaje original.

Un datagrama IP consta de una cabecera y un texto (datos). La cabecera tiene una parte fija de 20 bytes (5 palabras de 4 bytes cada una) y una opcional de longitud variable.

# Autoevaluación 2



¿Estás listo para un desafío?

**1. Indique la opción correcta**

TCP/IP está basado en los siguientes agentes de red: Procesos, Hosts y Redes.

- Verdadero
- Falso

**2. Indique la opción correcta**

La arquitectura TCP/IP está compuesta de cuatro capas: Acceso a la Red, Capa Interred, Transporte y Aplicación.

- Verdadero
- Falso

**3. Indique la opción correcta**

¿Qué capas del modelo OSI, están involucradas en la capa de Acceso a la Red de TCP/IP?

- La capa de Acceso a la Red de TCP/IP incluye las capas Físicas y de Enlace de Datos de OSI.
- La capa de Acceso a la Red de TCP/IP incluye la capa de Red del modelo OSI.
- La capa de Acceso a la Red de TCP/IP incluye la capa de Transporte del modelo OSI.
- La capa de Acceso a la Red de TCP/IP incluye las capas de Sesión, Presentación y Aplicación de OSI.

**4. Indique la opción correcta**

¿Cómo se llama al proceso de pasar los mensajes de una capa hacia la otra dentro de un host?

- Transmisión.
- Envío y Recepción.
- Encapsulamiento.
- Trama.

**5. Indique la opción correcta**

La tarea de encaminar datos entre dispositivos conectados a la misma red es una tarea de la capa:

- Acceso a la red.

- Interred o Internet.
- Transporte o Transmisión.
- Aplicación.

#### 6. Ordene relaciones

El modelo TCP/IP define protocolos para cada capa, a saber:

Capa Internet	FTP, SMTP y TEL-NET
Capa de Transmisión	TCP
Capa de Aplicación	IP

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

TCP/IP está basado en los siguientes agentes de red: Procesos, Hosts y Redes.

Verdadero

Falso

## 2. Indique la opción correcta

La arquitectura TCP/IP está compuesta de cuatro capas: Acceso a la Red, Capa Interred, Transporte y Aplicación.

Verdadero

Falso

## 3. Indique la opción correcta

¿Qué capas del modelo OSI, están involucradas en la capa de Acceso a la Red de TCP/IP?

La capa de Acceso a la Red de TCP/IP incluye las capas Físicas y de Enlace de Datos de OSI.

La capa de Acceso a la Red de TCP/IP incluye la capa de Red del modelo OSI.

La capa de Acceso a la Red de TCP/IP incluye la capa de Transporte del modelo OSI.

La capa de Acceso a la Red de TCP/IP incluye las capas de Sesión, Presentación y Aplicación de OSI.

## 4. Indique la opción correcta

¿Cómo se llama al proceso de pasar los mensajes de una capa hacia la otra dentro de un host?

Transmisión.

Envío y Recepción.

Encapsulamiento.

Trama.

## 5. Indique la opción correcta

La tarea de encaminar datos entre dispositivos conectados a la misma red es una tarea de la capa:

Acceso a la red.

Interred o Internet.

Transporte o Transmisión.

Aplicación.

## 6. Ordene relaciones

El modelo TCP/IP define protocolos para cada capa, a saber:

Capa Internet

FTP, SMTP y TEL-NET

Capa de Transmisión

IP

Capa de Aplicación

TCP

# SP6 / H3: Capas de transporte y aplicación

## Capa de transporte

Sin considerar la naturaleza del proceso que intercambia datos (p. ej. transferencia de archivo, logon remoto, etc.), se requiere que los datos sean intercambiados fidedignamente.

El mecanismo para proveer exactitud es esencialmente independiente de la naturaleza del proceso. Por esta razón, esto da sentido a la colección de estos mecanismos en una capa común compartida por todos los procesos; esto está puntualizado como la capa "host-to-host".

El protocolo de la Capa de Transporte, que está ubicado justamente encima de la Capa Internet, es la "Capa de Transporte Host-to-Host". Este nombre normalmente es abreviado como "Capa de Transporte". Los dos protocolos más importantes de la Capa de Transporte son: el "*Protocolo de Control de Transmisión*" (TCP = *Transmission Control Protocol*) y el "*Protocolo de Datagramas de Usuario*" (UDP = *User Datagram Protocol*).

TCP provee servicio de entrega segura de datos con detección de errores extremo a extremo.

UDP provee un servicio "no orientado a conexión" de entrega de datagramas de baja sobrecarga (low-overhead).

Ambos protocolos pasan datos entre la Capa de Aplicación y la de Internet. Los programadores de aplicación pueden elegir cualquiera, sin importar qué servicio es más apropiado para cada aplicación específica.

### Protocolo de Datagrama de Usuario (UDP – User Datagram Protocol)

El UDP provee acceso directo a las aplicaciones, al servicio de entrega de datagramas IP. Éste permite que las aplicaciones intercambien mensajes sobre la red con una sobrecarga de protocolo mínima.

UDP es un protocolo poco seguro, no orientado a conexión. Debe notarse que antes, "poco seguro" simplemente significaba que el protocolo no contenía una técnica de verificación de que los datos hubieran alcanzado correctamente el otro extremo de la red. Este "NO" es el caso de UDP, ya que puede entregar datos correctamente entre host.

UDP usa 16 bits de la primera palabra de 32 bit del encabezado del mensaje para identificar los "Puertos Origen" (Source Port), y otros 16 para "Puertos Destinos" (Destination Port), para entregar datos al proceso de aplicación adecuado. Ya veremos el protocolo UDP en la Situación Profesional 10.

Si UDP es un protocolo inseguro, ¿por qué razón las aplicaciones lo eligen como un servicio de transporte de datos?.

Hay un buen número de razones. Si la cantidad de datos que está siendo transmitida es pequeña, la sobrecarga (overhead) del establecimiento de conexiones y la seguridad de una entrega confiable, puede ser mayor que el trabajo de retransmisión completa del conjunto de datos. En este caso, UDP es la opción más eficiente como protocolo de la Capa de Transporte.

Las aplicaciones que acceden a modelos "pregunta-respuesta" (query-response), son también excelentes candidatos para usar UDP. La respuesta puede ser usada como un reconocimiento positivo a la consulta. Si una respuesta no es recibida en un cierto período de tiempo, la aplicación debe enviar nuevamente la consulta. Sin embargo, otras aplicaciones proveen su propia técnica para la entrega segura de datos y no requieren los servicios del protocolo de la Capa de Transporte. La imposición de reconocimientos en cualquier otra capa en estos tipos de aplicaciones es ineficiente y no tiene sentido.

## Protocolo de Control de Transmisión (TCP = Transmission Control Protocol)

Aplicaciones que requieren un protocolo de transporte para proveer entrega confiable de datos usan TCP, debido a que éste verifica que los datos son fielmente entregados a través de la red y en la secuencia apropiada.

TCP es un protocolo que se diseñó para tolerar el funcionamiento de redes inseguras. Asociado a éste, se creó el protocolo de capa de red IP que ya hemos visto.

Una entidad de transporte TCP acepta mensajes de longitud arbitrariamente grandes, procedentes de los procesos de usuarios; los separa en trozos que no excedan de 64 kBytes y transmite cada segmento como si fuera un datagrama separado.

La capa de red no garantiza que los datagramas se entreguen correctamente, por lo que TCP deberá utilizar temporizadores y retransmitir los segmentos, si es necesario. Los datagramas que consiguen llegar pueden hacerlo en desorden y dependerá de TCP el reensamblarlos en mensajes, con la secuencia correcta.

Cada byte de datos transmitido por TCP tiene su propio número de secuencia privado. El espacio de números de secuencia tiene una extensión de 32 bits, para asegurar que los duplicados antiguos hayan desaparecido.

TCP es un protocolo por trenes de bytes, seguro y orientado a conexión. Vamos a ver cada uno de los términos: seguro, orientado a conexión y trenes de bytes con más detalles.

La unidad de datos intercambiada entre módulos TCP cooperativos es llamada "segmento", que veremos en detalles más adelante.

TCP utiliza un protocolo de establecimiento de conexión llamado "handshake a tres vías", debido a que son intercambiados tres segmentos para el establecimiento del circuito virtual.

TCP ve a los datos que envía como un "tren continuo de bytes", no como paquetes independientes. Además, TCP toma cuidado de mantener la secuencia en la cual los bytes son enviados y recibidos.

El TCP estándar no requiere que cada sistema comience numerando los bytes con algún número específico; cada sistema elige el número que puede usar como punto de comienzo. Para mantener la pista del tren de bytes correctamente, cada extremo de la conexión sincroniza el sistema de numeración de bytes intercambiando la secuencia durante el handshake.

TCP es también responsable de la entrega de datos recibidos desde IP, a la aplicación correcta. La aplicación a la cual el dato está dirigida se identifica por un número de 16 bit llamado el "Número de Puerto" (Port Number).

Los "Puertos Origen" (Source Port) y "Puertos Destinos" (Destination Port) están contenidos en la primera palabra del encabezamiento del segmento.

TCP provee un mecanismo seguro para el intercambio de datos entre procesos en diferentes computadores. El protocolo asegura que los datos son entregados libres de errores, en secuencia, sin pérdidas ni duplicación. El servicio TCP asiste al software de las capas superiores ofreciendo servicios de comunicación. A causa de que TCP provee servicios de alta calidad y dado que puede necesitar administrar un amplio rango de servicios, es uno de los más complejos de los protocolos de comunicación.

El servicio básico provisto por TCP es la transferencia de datos entre dos usuarios TCP, tal como el FTP. Los datos son pasados desde un usuario TCP a otro.

TCP encapsula esos datos en una PDU, la cual contiene los datos del usuario más información de control, tales como la dirección de destino. Para conseguir una exacta transferencia de datos, las PDU salientes son numeradas secuencialmente y subsecuentemente reconocidas por ese número por la entidad del TCP destino.

Si las PDU arriban fuera de orden, pueden ser reordenadas basándose en el número de secuencia. Si una PDU se pierde, ésta será reconocida y la entidad del TCP emisor deberá retransmitirla.

Más allá de este servicio básico, existen otros servicios ofrecidos por TCP, como ser:

- Calidad de Servicio: TCP permite a los usuarios especificar la calidad del servicio de transmisión provista. El protocolo TCP puede optimizar al protocolo IP subyacente y los recursos de red, al mejorar la capacidad de los servicios ofrecidos. Los parámetros especificados incluyen precedencia, exactitud y productividad.
- Entrega Urgente: algunos datos pueden tener especial urgencia. TCP puede hacer que la transferencia de datos sea lo más rápida posible. En el extremo receptor, el TCP puede interrumpir al usuario para notificar de la recepción de un dato urgente. De esta manera este mecanismo de interrupción es usado para transferir datos urgentes ocasionales, tales como un carácter de ruptura desde una terminal o una condición de alarma.
- Seguridad: una clasificación de seguridad o rango puede ser usada para rotular los datos provistos al TCP. Esto puede influenciar en la ruta tomada por los datos y si estos están encriptados.

## Características de TCP/IP

El protocolo TCP/IP ha ganado una creciente aceptación entre los usuarios del mundo entero. Si bien el grupo estaba constituido originalmente por cinco protocolos, se lo conoce por el nombre de dos de ellos: Protocolo de Control de Transmisión (TCP = *Transmission Control Protocol*) y Protocolo Internet (IP = *Internet Protocol*). Esos protocolos son ampliamente usados por la comunidad de Internet.

Lo más importante e interesante es que esos protocolos fueron construyendo un estándar internacional para la comunicación de datos. La popularidad de los protocolos TCP/IP en la Internet no tuvo, al comienzo un rápido crecimiento debido a que el protocolo no estaba disponible, o porque las agencias militares impedían su uso.

Estos protocolos tienen varias características importantes. Ellas son:

- Estándar de protocolos abiertos, libremente disponibles y desarrollados por cualquier hardware o sistema operativo. TCP/IP es ideal para unificar diferente hardware y software, sobre todo si se comunica sobre Internet.
- Independencia del hardware de red. Esto permite integrar diferentes clases de redes. TCP/IP puede ser ejecutado sobre Ethernet, Token Ring, líneas commutadas, X.25, PPP, Frame Relay y, virtualmente, sobre cualquier clase de medios de transmisión.
- Un esquema de direccionamiento común permite que cualquier dispositivo pueda direccionar únicamente con cualquier otro dispositivo sobre la red, aunque la red sea una gran red mundial.
- Protocolos de alto nivel estandarizados para proveer servicios de usuarios ampliamente disponibles.

## Capa de aplicación

Al tope de la arquitectura de protocolos TCP/IP está la capa de aplicación, la cual incluye todos los procesos que usa la Capa de Transporte para la entrega de datos. Existen muchos protocolos de aplicaciones. La mayoría proveen servicios a los usuarios y siempre se están agregando nuevos servicios en esta capa.

Si bien las siguientes aplicaciones no pertenecen al conjunto TCP/IP, son aplicaciones consideradas como un estándar, por lo tanto trataremos de ellas.

La capa de aplicación contiene protocolos para recursos compartidos (p. ej. *Host a Host*) y acceso remoto (por ejemplo terminal a computador).

Los protocolos de aplicaciones más ampliamente conocidos son:

- TELNET: el "Protocolo de Terminal de Red" (*Network Terminal Protocol*), provee acceso remoto (*remote login*) sobre la red.
- FTP: el "Protocolo de Transferencia de Archivos" (*File Transfer Protocol*), es usado para transferencia de archivos interactiva.
- SMTP: el "Protocolo de Transferencia Simple de Correo" (*Simple Mail Transfer Protocol*), distribuye correo electrónico.
- HTTP: El "Protocolo de Transferencia de Hipertexto" (*HiperText Transfer Protocol*), es utilizado en aplicaciones Web.

Mientras FTP, SMTP, HTTP y TELNET, son las aplicaciones TCP/IP más implementadas, se puede trabajar con muchos otros, tanto los usuarios como los administradores de sistemas.

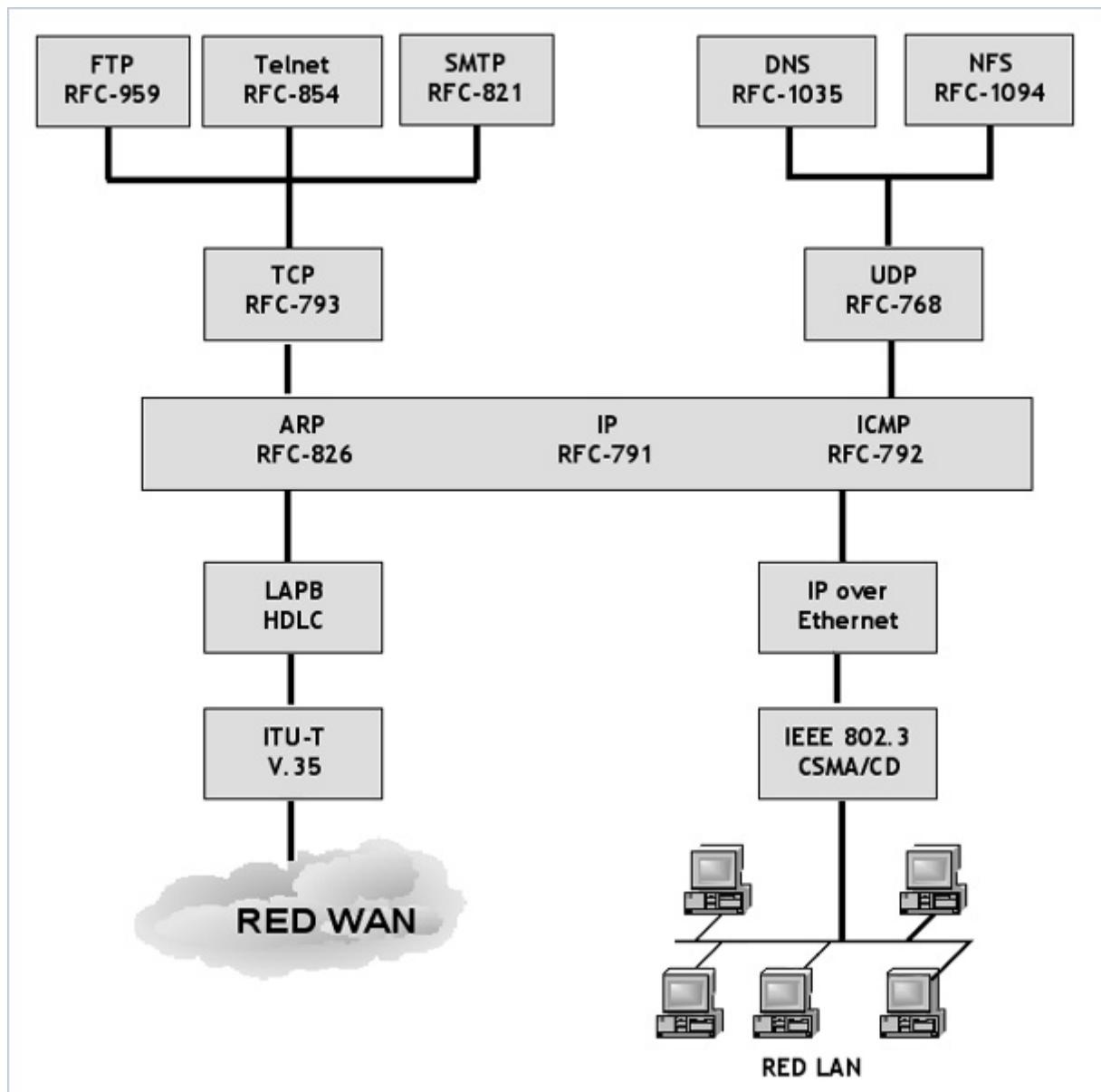
Algunas otras aplicaciones comúnmente usadas son:

- DNS (*Domain Name Service*): "Servicio de Nombres de Dominios", o también llamado "Servicios de Nombre", esta aplicación permite obtener una dirección IP a partir de un "Nombre de Dominio", esencial para rutear paquetes en la red.
- NFS (*Network File System*): "Sistemas de Archivos de Red", este protocolo permite compartir archivos por varios host sobre la red.

Algunos protocolos, tales como TELNET y FTP, pueden ser usados sólo si el usuario tiene algún conocimiento de la red. Otros protocolos se ejecutan sin que el usuario tenga conocimiento de ellos. El administrador de red debe saber de todas estas aplicaciones y todos los protocolos de todas las capas de TCP/IP.

La figura siguiente muestra la jerarquía de protocolos en un computador imaginario. Como puede notarse, la reducción de la complejidad de la pila de protocolos a un diagrama en bloques es, por naturaleza, una simplificación y tiene como fin ayudar a visualizar la relación de los diferentes protocolos en un único host. No todos estos protocolos han sido discutidos en este capítulo, pero lo han sido o lo serán a lo largo del libro y pueden ayudar a tener una idea de la estructura completa.

En la parte superior de la figura están los protocolos de aplicación, tales como FTP o TELNET. Cada protocolo es mostrado con el número de RFC (Request For Comments) que lo define. La línea que va desde un bloque a otro hacia la parte inferior indica el servicio que el protocolo usa. Podemos ver que FTP, TELNET y SMTP utilizan TCP; mientras NFS y DNS lo hacen con UDP.



Debajo de las aplicaciones están los protocolos de la Capa de Transporte: TCP y UDP. Ellos actúan directamente con IP.

IP entrega datos desde las capas superiores a la red apropiada y entrega datos desde la red al servicio de transporte específico. Asimismo, los servicios de transporte entregan los datos recibidos desde IP a la aplicación adecuada.

Los protocolos agrupados debajo de IP son considerados como Protocolos de Acceso a la Red. El apilado de esos protocolos en capas no implica jerarquía alguna, aunque del lado de la WAN, los protocolos indicados corresponden a las capas inferiores del modelo de referencia OSI (Enlace de Datos y Física). Para TC-P/IP, todos esos protocolos son de Acceso a la Red.

## Protocolo de Transferencia de Archivos (FTP = File Transfer Protocol)

El modelo de transferencia de archivos no se basa en la idea de un almacén de archivos virtual, sino como la idea de transferir un archivo de una máquina real a otra, tomando en cuenta las diferencias que existen en dichas PC.

Estas diferencias pueden obligar a realizar ciertas conversiones durante la transferencia, lo cual es algo que maneja el protocolo. No es lo mismo transferir un archivo bit a bit, que hacerlo a una impresora, que requiere ciertas convenciones para el control de carro.

El propósito de FTP es transferir un archivo desde un host a otro, bajo comandos interactivos de usuario.

La comunicación con FTP se realiza con intervención del sistema operativo, el cual contiene manejadores (redireccionadores) de entrada/salida (driver I/O). Si el usuario sobre un sistema A desea acceder a un archivo sobre el sistema B, entonces la entidad FTP de "A" se comunica con la entidad FTP de "B".

Existen tres posibilidades:

1. El usuario del sistema "A" puede desear que un archivo del sistema "B" sea transferido al sistema "A". Éste puede ceder al usuario local acceso al contenido del archivo.
2. El usuario puede tener preparado un archivo localmente (en el sistema "A") y enviarlo al sistema "B".
3. Finalmente, el usuario puede requerir que un archivo sea intercambiado entre el sistema "B" y un tercer sistema "C". Esto es referido como transferencia de tercera parte e involucra entidades FTP sobre el sistema "A", "B" y "C".

FTP debe interactuar con tres entidades:

1. Primero, debe haber una interfaz de usuario para aceptar los requerimientos del usuario interactivo, o posiblemente un programa. Esta interacción tiene lugar sólo en el host requerido. El FTP remoto en un evento de transferencia de archivo no interactúa con un usuario.
2. Segundo, el FTP debe estar disponible para comunicarse con otra entidad FTP para lograr la transferencia del archivo. Esto se hace usando el servicio de TCP.
3. Tercero, para transferir un archivo, FTP debe estar disponible para adquirir el archivo. Para esto, es necesaria una interfaz al sistema de administración de archivos local (file management system).

Distingue cuatro tipos de archivos:

- Archivo de Imagen
- Archivo ASCII
- Archivo EBCDIC
- Archivo de bytes lógicos

Los Archivos ASCII son los normalizados para el intercambio de textos, excepto con los ordenadores IBM que utilizan el código EBCDIC.

Los de Bytes Lógicos son archivos binarios con un tamaño de byte distinto de 8 bits.

Los archivos paginados están constituidos por bloques de datos, cada uno con una cabecera que proporciona el tamaño, posición y tipo.

Soporta una gran variedad de comandos, de los cuales algunos se ocupan del envío y recepción de archivos, otros del manejo de directorios y otros relacionados con el establecimiento de los parámetros y los modos de transferencia.

## Protocolo Simple de Transferencia de Correo (SMTP = Simple Mail Transfer Protocol)

El correo electrónico es una de las aplicaciones más importantes. El formato de la correspondencia está definido por un documento llamado RFC 822. Al protocolo se le llama SMTP (Protocolo Simple de Transferencia de Correo).

El RFC 822 fue diseñado para enviar mensajes que contengan líneas de texto en ASCII y no es soportado ningún otro carácter. Tampoco tiene mecanismos para expedir Facsímil, voz digitalizada, imágenes u otras formas de comunicación.

El RFC 822 no hace distinción entre el sobre y el mensaje. Cada pieza de correspondencia se considera como un archivo sencillo, que contiene ciertos campos de cabeceras al comienzo. Cada campo de cabecera es una palabra clave en ASCII, seguida de dos puntos y el valor.

SMTP provee la base para la facilidad de red de correo electrónico. Típicamente, una facilidad de correo electrónico se ejecuta en un host. Para cada usuario con acceso al host, existe un buzón (mailbox). Cuando un usuario ingresa al host, puede enviar un correo ubicando un mensaje en el buzón de otro usuario y recibir correo leyendo el mensaje en su propio buzón.

Típicamente, los buzones son mantenidos a través del sistema de administración de archivos. Cada buzón es un directorio que puede contener archivos de texto que llamamos mensajes.

SMTP hace uso de TCP para enviar y recibir mensajes a través de la red. El estándar SMTP no especifica la interface de usuario. De esta manera, el usuario ve la misma interface si está enviando correo local o correo remoto.

## TELNET (Terminal Virtual)

El protocolo de terminal virtual, se diseñó con modo desplazamiento. Por defecto de la red posee una sola línea de longitud ilimitada.

El protocolo se ocupa de fijar y manejar dos flujos de datos, uno en cada sentido. Este protocolo no tiene el concepto de una estructura de datos que se deben mantener idénticas en los extremos. A medida que se teclean caracteres en el terminal, se transmiten sobre la línea un flujo de bytes de ocho bits. El proceso del terminal debe convertir cualquier código de caracteres a la norma de la red, que es el ASCII.

Existe, además, un número de comandos que pueden intercalarse libremente con los datos. Todos los comandos vienen precedidos de la sigla IAC (*Interpreter At Comand*) que indica que el carácter que le sigue es un comando.

TELNET es un protocolo usado para enlazar terminales a aplicaciones. Éste puede ser caracterizado como sigue:

- Especifica una terminal estándar de red. Así, las características específicas de la terminal son representadas dentro del estándar. Esto permite conectar host de distintos proveedores.
- Especifica el protocolo entre la terminal y el host. Esto permite negociar ciertas características de terminal (por ej. ancho de línea, tamaño de página, full-dúplex versus half-dúplex eco remoto versus local).
- Provee exactitud en el intercambio de datos por intermedio de TCP.
- Permite a los usuarios de terminales un control de las aplicaciones en host remotos, como si el usuario fuera local de ese host.

TELNET actualmente está implementado en dos módulos:

- Usuario TELNET: un Usuario TELNET interactúa con el módulo de E/S de terminal para comunicar

con una terminal local. Éste convierte las características de la terminal real en un estándar de red y viceversa.

- Servidor TELNET: el Server TELNET interactúa con un proceso o aplicación y se comporta como una terminal sustituta que maneja a la terminal remota, haciéndola aparecer como local al proceso o aplicación.



¡Vamos a comprobar cuánto aprendiste!

**1. Indique la opción correcta**

UDP es un protocolo seguro, orientado a conexión.

- Verdadero
- Falso

**2. Indique la opción correcta**

La comunicación FTP se realiza con intervención del sistema operativo, el cual contiene manejadores (redirectores) de entrada/salida.

- Verdadero
- Falso

**3. Indique la opción correcta**

SMTP fue originalmente diseñado para enviar mensajes que contengan líneas de texto en ASCII y no soporta ningún otro carácter.

- Verdadero
- Falso

**4. Indique la opción correcta**

La primera palabra de 32 bit del encabezado UDP:

- Comienza numerando los bytes con un número específico.
- Sincroniza el sistema de numeración de bytes.
- Identifica "Puerto Origen" y "Puerto Destino".
- Entrega los datos a la aplicación correcta.

**5. Indique la opción correcta**

¿Qué aplicaciones usan TCP como protocolo de la capa de Transporte?

- Aplicaciones que requieren un protocolo de aplicación confiable.
- Aplicaciones que requieren un protocolo de red confiable.

- Aplicaciones que requieren un protocolo de transporte no confiable.
- Aplicaciones que requieren un protocolo de transporte confiable.

#### 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Las aplicaciones de TCP se refieren a los datos como

segmentos (segment)

Las aplicaciones de UDP se refieren a los datos como

mensajes (message)

TCP llama a los datos

paquetes (packet)

UDP llama a los datos

flujo de corriente  
(stream)

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

UDP es un protocolo seguro, orientado a conexión.

Verdadero

Falso

## 2. Indique la opción correcta

La comunicación FTP se realiza con intervención del sistema operativo, el cual contiene manejadores (redirectores) de entrada/salida.

Verdadero

Falso

## 3. Indique la opción correcta

SMTP fue originalmente diseñado para enviar mensajes que contengan líneas de texto en ASCII y no soporta ningún otro carácter.

Verdadero

Falso

## 4. Indique la opción correcta

La primera palabra de 32 bit del encabezado UDP:

Comienza numerando los bytes con un número específico.

Sincroniza el sistema de numeración de bytes.

Identifica "Puerto Origen" y "Puerto Destino".

Entrega los datos a la aplicación correcta.

## 5. Indique la opción correcta

¿Qué aplicaciones usan TCP como protocolo de la capa de Transporte?

Aplicaciones que requieren un protocolo de aplicación confiable.

Aplicaciones que requieren un protocolo de red confiable.

Aplicaciones que requieren un protocolo de transporte no confiable.

Aplicaciones que requieren un protocolo de transporte confiable.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Las aplicaciones de TCP se refieren a los datos como

paquetes (packet)

Las aplicaciones de UDP se refieren a los datos como

flujo de corriente  
(stream)

TCP llama a los datos

mensajes (message)

UDP llama a los datos

segmentos (segment)

## SP6 / H4: Máxima unidad de transferencia (MTU) y fragmentación

Debemos tener en cuenta el hecho de que un datagrama IP debe ir encapsulado dentro de una trama, lo cual simplemente significa que el tamaño del datagrama a transferir no podrá superar el permitido por la trama.

El problema es importante si consideramos que el envío puede pasar por varias redes, cada una con características de hardware distintas. Por ejemplo, hemos visto que un datagrama IP puede contener hasta 65.536 Bytes; sin embargo, una red Ethernet puede transferir hasta 1500 Bytes, y una red FDDI (anillo de fibra óptica) permite aproximadamente 4470 Bytes.

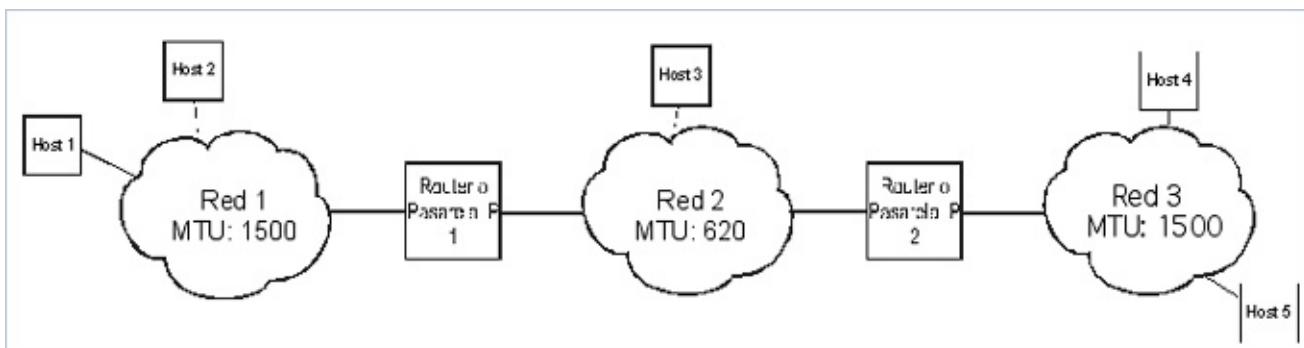
Cada tipo de red tiene una "Unidad Máxima de Transmisión" (MTU = Maximum Transmission Unit) **ver con lo de arriba**, el cual es el mayor paquete que puede ser transferido. Si el datagrama recibido es mayor que el MTU de la otra red, es necesario dividirlo en "fragmentos" más pequeños para su transmisión. Este proceso es llamado "fragmentación".

El asunto pasa por decidir de qué tamaño deben ser los datagramas; en principio, podríamos plantearnos lo siguiente: si se usan datagramas muy pequeños, el sistema puede ser ineficiente ya que si bien conseguirá transitar por todas las redes, en aquéllas que permiten transferir tramas grandes, se estarán desaprovechando; por otro lado, si se usan datagramas IP muy grandes podría ocurrir que éstos no transitaran por alguna de las redes.

La mejor solución es hacer que los datagramas fueran pequeños en aquellas redes que permiten tramas pequeñas, y grandes en aquellas redes que permiten tramas grandes.

**Ésta es justamente la idea central de la fragmentación:**

Supongamos, según el diagrama de la figura siguiente, que el host 1 desea enviar un datagrama de 1400 Bytes al Host 5. Tanto el Host 1 como el 5 forman parte de redes Ethernet, que poseen un MTU de 1500 Bytes; pero como puede verse en la figura, la conexión deberá pasar por una red intermedia con un MTU menor, de 620 Bytes.



"Idea central de la fragmentación" | xxx

Es decir: los routers realizan fragmentaciones cuando las redes que comunican tienen diferente MTU.

**¿Cómo será el proceso?**

El software IP del Host 1 armará el datagrama IP, con su encabezado y su área de datos (como éste consta de 1400 Bytes y Ethernet tiene un MTU de 1500 Bytes lo puede enviar sin fragmentarlo), y solicita el servicio

ARP para resolver la dirección del Host 5; como éste no pertenece a la misma red, ARP resuelve la dirección del Router 1, encapsula el mensaje IP agregando el encabezado ARP (con las direcciones de hardware del Host 1 y del Router 1), y envía el paquete.

Lo recibe el Router 1, éste elimina la cabecera de la trama (es decir, elimina la dirección origen y destino ARP), lee la dirección IP del Host 5, y determina que no pertenece a ninguna de las redes a las que está conectado, revisa sus tablas de enrutamiento y decide que debe rutearlo hacia el Router 2; cuando lo va a enviar se da cuenta de que el paquete es de 1400 Bytes, pero la red que debe atravesar para llegar hasta el Router 2 tiene un MTU de sólo 620.

Por lo tanto, decide fragmentar el datagrama IP.

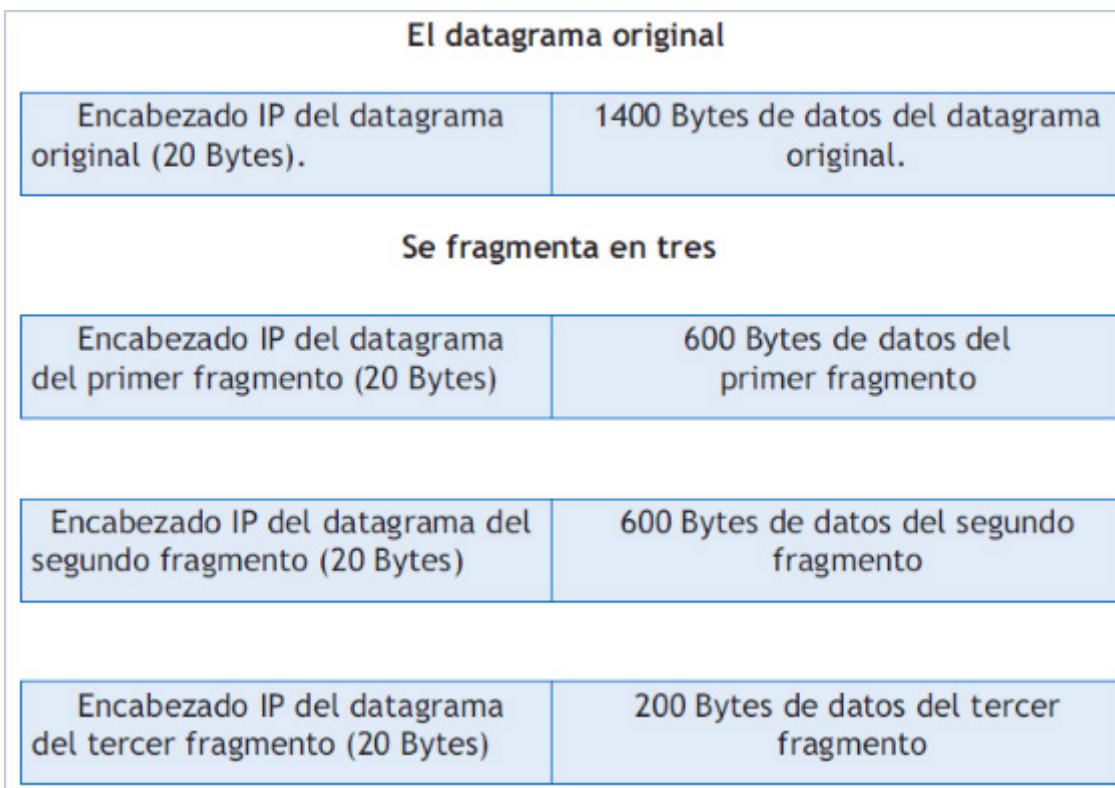
Cada fragmento tendrá la misma estructura que el datagrama IP original, es decir encabezado IP más datos. Las direcciones IP Origen y destino, seguirán siendo las de los Host 1 y 5 respectivamente. ¿De qué tamaño será cada fragmento? Obviamente que cada fragmento debe ser menor que el MTU de la red que debe atravesar.

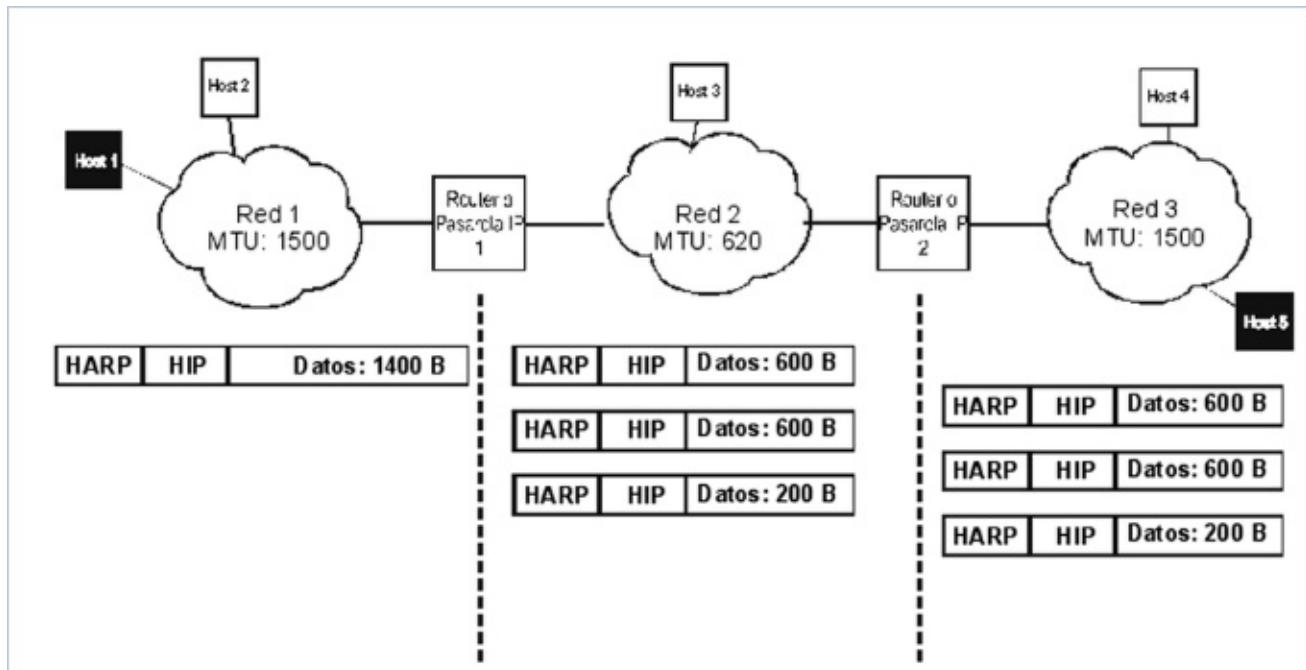
Además, su tamaño medido en Bytes debe ser múltiplo de 8, ya que en el encabezado IP, el campo Desplazamiento guarda su información de esta forma.

Supongamos que el encabezado IP es el típico, que ocupa 5 palabras de 4 Bytes cada una, es decir 20 Bytes, ¿cuál es el mayor tamaño de fragmento posible?

La MTU es de 620, le restamos los 20 Bytes, con lo cual nos quedan 600 Bytes disponibles. Como 600 es múltiplo de 8, elegimos un tamaño de fragmento de 600 Bytes (si no hubiera sido múltiplo de 8, deberíamos elegir el mayor múltiplo de 8 menor que el máximo tamaño permitido).

Este tamaño nos permite utilizar 2 fragmentos de 600 Bytes, más un último fragmento de 200 Bytes, para conformar los 3 nuevos datagramas. El proceso se indica en la siguiente figura:





"Fragmentaciones de los Routers" | Los Routers realizan fragmentaciones cuando las redes que comunican tienen diferente MTU, pero no efectúan reensamblados.

Referencias:

HARP: Header ARP: Encabezado ARP

HIP: Header IP: Encabezado IP

**Los routers realizan fragmentaciones cuando las redes que comunican tienen diferente MTU, pero no efectúan reensamblados**

¿Alguna vez se ha molestado por la baja velocidad de su conexión a Internet? ¿Alguna vez ha estado tentado de "bajar" alguno de esos programas que se pueden comprar en diversos sitios Web que prometen acelerar su velocidad en Internet?

Esté atento a lo que hemos dicho sobre el MTU, porque allí reside uno de los "trucos" para mejorar el rendimiento de su conexión a la red de redes.

En la actualidad, los Routers que trabajan sobre líneas telefónicas están diseñados para utilizar datagramas de hasta 576 Bytes. Uno de los "trucos" que se utilizan para acelerar las comunicaciones en Internet bajo entorno Windows consiste en modificar el registro del sistema operativo para que utilice datagramas de "hasta" 576 Bytes, aunque la red a la que está conectado permita una cifra mayor; de esta forma, el trabajo de fragmentación se da en el host y no en el router, lo cual habitualmente hace que la transferencia sea más rápida.

El Sistema operativo asignan valor predeterminado de MTU a cada conexión de acuerdo a su tipo. No obstante es necesario comprobar en la práctica si ese valor funciona de forma adecuada en cada conexión.

¿Qué efecto tiene un valor MTU inadecuado?

Si el MTU es demasiado alto puede causar fragmentación.

Si el valor es inferior no se aprovecha la capacidad e la red de forma adecuada.

Los valores que el sistema operativo Windows asigna estan acordes a la red utilizada y son:

- En redes locales (Ethernet) = 1500 bytes
- En redes punto a punto sobre redes locales (PPPoE: Point to Point Protocol over Ethernet) = entre 1492 y 1480 bytes.
- En redes con conexiones dial-up = 576 bytes

Cada unidad de transmisión (TU) está compuesta por los encabezados o headers más los datos utilizados.

A los datos se los denomina MSS (Maximum Segment Size) y este tamaño es la cantidad verdadera de información a ser enviada, por lo que la máxima unidad de transmisión (MTU) sería:

MTU=Encabezados TCP/IP+MSS.

### Como conocer el MTU de nuestra conexión

Para saber en nuestro sistema operativo cual es le MTU asignado actualmente a una conexión se puede utilizar el comando NETSH (Network Shell) de la siguiente manera:

Necesitaremos abrir una consola: pulse **Tecla De Windows + R** y escribir **cmd** y **Enter**.

Tras este paso tendremos que ver nuestras interfaces y sus MTU:

**netsh interface ipv4 show subinterfaces** y **Enter**

MTU	MediaSenseState	Bytes In	Bytes Out	Interface
4294967295		1	590745	Loopback Pseudo-Interface 1
1500		65359752	23577306	Wireless Network Connection
1500		5	131200	Wireless Network Connection 2
1500		5	0	Local Area Connection
1500		5	0	Local Area Connection 3
1500		1	1740194	VMware Network Adapter VMnet1
1500		1	1731836	VMware Network Adapter VMnet8

"Netsh" | Sistema Operativo Windows 7

Allí se pueden observar en una lista todos los adaptadores de red instalados en el equipo: el primer valor a la izquierda es el MTU.

En la figura anterior aparece el valor MTU=1500.

Para hallar el valor límite o MSS, hay que restarle los 28 bits usados en los encabezados (IP [20 bytes] y ICMP [8 bytes])

1500-28 = 1472.

Por lo que entonces 1472 es el valor límite de datos o MSS usado en la conexión.

El paso siguiente es comprobar si utilizando dicho valor existe o no fragmentación en los datos enviados.

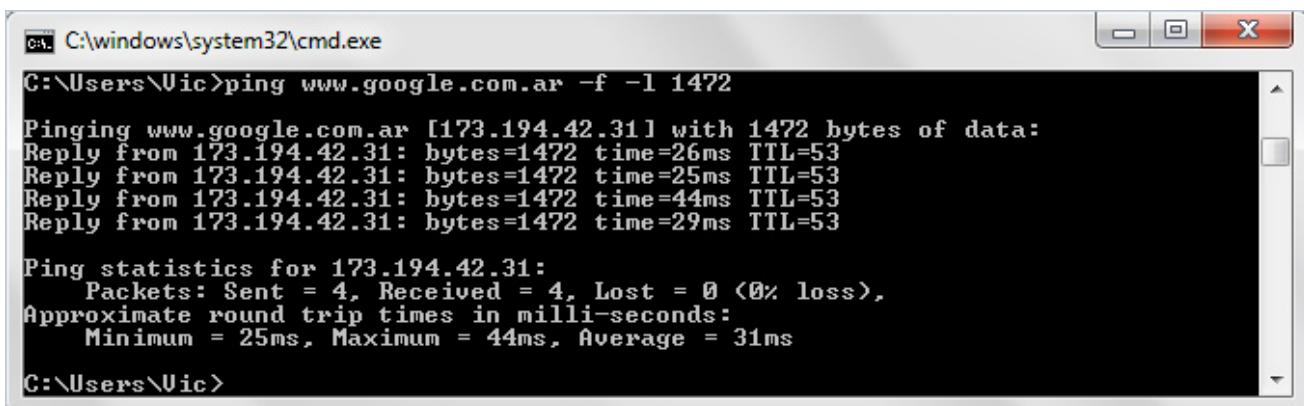
### Como comprobación de la eficiencia del valor MTU asignado a una conexión

El ISP (proveedor de acceso a internet) es quien establece el valor máximo de MTU que se puede usar a través de su red, dado que toda la conexión pasa a través de sus equipos.

Para comprobar si existe o no fragmentación en los datos enviados usando el valor MTU anterior, es necesario hacer PING a través de la red a la dirección IP del ISP, o a cualquier servidor que se sepa que esté disponible y que sea eficiente.

En el siguiente ejemplo usamos los servidores de Google.

ping www.google.com.ar -f -l 1472



```
C:\Windows\system32\cmd.exe
C:\Users\Vic>ping www.google.com.ar -f -l 1472
Pinging www.google.com.ar [173.194.42.31] with 1472 bytes of data:
Reply from 173.194.42.31: bytes=1472 time=26ms TTL=53
Reply from 173.194.42.31: bytes=1472 time=25ms TTL=53
Reply from 173.194.42.31: bytes=1472 time=44ms TTL=53
Reply from 173.194.42.31: bytes=1472 time=29ms TTL=53

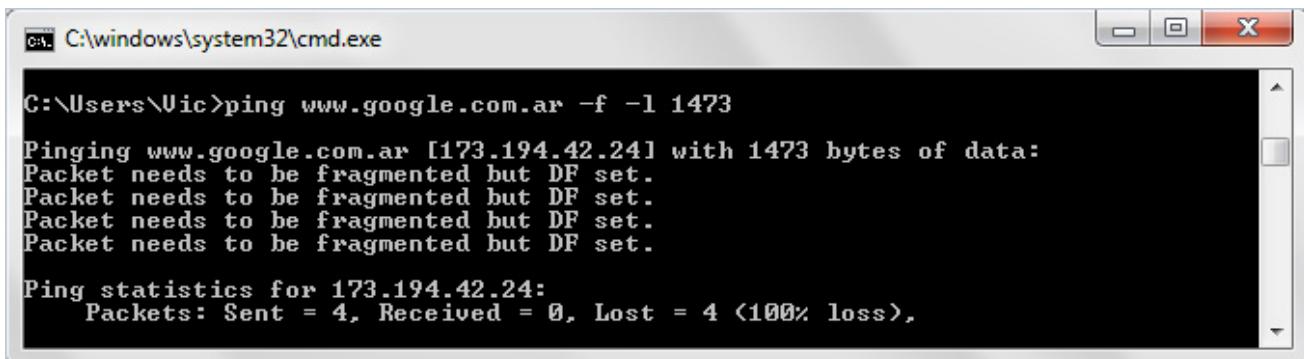
Ping statistics for 173.194.42.31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 25ms, Maximum = 44ms, Average = 31ms

C:\Users\Vic>
```

"Ping google 1472" | Sistema operativo Windows 7

La respuesta no muestra que exista fragmentación.

Si existiera fragmentación lo expresaría en la respuesta, para comprobar esto repetimos el comando PING con un valor más alto (1473) y vemos que responde (no es necesario teclear todo de nuevo, puede utilizar el atajo de teclado F3 y cambiar solo el último carácter):



```
C:\Windows\system32\cmd.exe
C:\Users\Vic>ping www.google.com.ar -f -l 1473
Pinging www.google.com.ar [173.194.42.24] with 1473 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 173.194.42.24:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

"Ping google 1473" | Sistema operativo Windows 7

Allí vemos entonces (*Packets needs to be fragmented*) que el valor MTU no sería el adecuado.

Para encontrar el valor adecuado, repetimos entonces la solicitud de PING pero en este caso disminuyendo el valor hasta dar con un valor en el que el paquete de datos enviado retorne sin ningún error. Si llegamos a este punto disminuyendo el valor por ejemplo de a 10 bytes, entonces es necesario seguir realizando el PING pero ahora incrementando el valor en un byte hasta llegar a un punto exacto.

Al valor alcanzado exacto no olvidemos que hay que sumarle la cantidad 28 por los Encabezados que hablamos antes, y ese será el valor MTU óptimo para nuestra conexión.

### Como asignar el valor MTU en una conexión

Y finalmente para poner la MTU que queremos:

```
netsh interface ipv4 set subinterface "el nombre de la interface" mtu=TAMAÑO store=persistent
```

Por ejemplo para una computadora conectada a la red LAN cableada:

```
netsh interface ipv4 set subinterface "Local Area Connection" mtu=1500 store=persistent
```

O si usted esta utilizando una conexión inalámbrica:

```
netsh interface ipv4 set subinterface "Wireless Network Connection" mtu=1500 store=persistent
```

Usted puede preguntarse ¿por qué se permiten otros valores de MTU, siendo que algunos Routers trabajan con 576 Bytes?

La respuesta es la siguiente: no olvide que TCP/IP puede también implementarse sobre una red no abierta, como una interconexión de LAN privadas o una WAN también privada; en esos casos, puede ser más veloz utilizar valores superiores de MTU en la configuración TCP/IP de los host. Para la nueva versión de IP, (IPv6) está propuesto que cada enlace soporte una MTU de 576 bytes por defecto, pero este valor, está sujeto a cambios.

## Conexión de Diferentes Tipos de Redes con Routers

Internet conecta muchos tipos de redes a través de router, los cuales transmiten datagramas y permiten encaminamiento adaptativo. Precisamente, mientras la tecnología de commutación de paquetes ha madurado y extendido su aplicación al mercado, la tecnología de interconexión pasó del ambiente de investigación al mundo comercial. Los router son fabricados para interconectar redes públicas de commutación de paquetes y están planificados para enlazar varias redes locales tales como Ethernet.

Internet posee un enfoque para la interconexión, con el principio tecnológico suministrado por Bolt Beranek y Newman (BBN) de Cambridge. El router transmite información en la forma de datagramas y permite diferentes esquemas de enrutamiento, determinados dinámicamente dependiendo del mejor camino disponible. El acceso alternativo al modelo de datagramas por gateway es el acceso por circuito virtual, el cual determina y establece una ruta antes de transmitir los datos. Cada esquema tiene ventajas y desventajas relacionadas con la congestión, la seguridad y la sobrecarga.

En general, los routers extienden las posibilidades de acceso a máquinas remotas, para la transferencia de información entre diferentes usuarios. También proveen una solución al problema de decidir cuál de los distintos métodos de interconexión es mejor, permitiendo el uso de todos ellos, dependiendo de la aplicación. Los diferentes tipos de redes pueden entonces ser interconectados por *router* o *gateway* y, de esta manera, dan al usuario una vista de una configuración de una extensa red.

Los router múltiples proveen redundancia y capacidad de carga adicional. La visión del usuario de la red interconectada se simplifica, si el gateway es considerado como un nodo de commutación y la red como líneas. Entonces la configuración entera puede ser vista como una red única, construida a partir de una colección de redes separadas.

El router encamina mensajes a través de la red a otros routers de un sistema interconectado como un nodo de commutación, enviando mensajes a través de las líneas a otros nodos en una única red de computadores. El *gateway* debe proveer funciones de nodo de commutación, tales como encaminamiento adaptativo, control de flujo y monitoreo y administración de red.



¿Te animás a medir cuánto aprendiste?

**1. Indique la opción correcta**

Un datagrama debe ir encapsulado dentro de una trama, lo cual significa que el datagrama a transferir no podrá superar el tamaño permitido por la trama.

- Verdadero
- Falso

**2. Indique la opción correcta**

La principal función de un router es la de tomar una decisión de encaminamiento entre redes.

- Verdadero
- Falso

**3. Indique la opción correcta**

Internet conecta muchos tipos de redes a través de routers, los cuales transmiten datagramas y permiten encaminamiento adaptativo.

- Verdadero
- Falso

**4. Indique la opción correcta**

Los routers realizan fragmentaciones cuando las redes que comunican tienen diferente MTU y también realizan los reensamblados.

- Verdadero
- Falso

**5. Indique la opción correcta**

En la actualidad, los Routers que trabajan sobre líneas telefónicas están diseñados para utilizar datagramas de hasta:

- 576 Bytes.
- 1500 Bytes.

- 4470 Bytes.
- 65536 Bytes.

#### 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Un datagrama IP puede contener  
Una red Ethernet puede transferir  
Una red FDDI puede permitir  
Una red PPP puede transferir

hasta 1500 Bytes  
hasta 4470 Bytes  
hasta 576 Bytes  
hasta 65.536 Bytes

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Un datagrama debe ir encapsulado dentro de una trama, lo cual significa que el datagrama a transferir no podrá superar el tamaño permitido por la trama.

- Verdadero
- Falso

## 2. Indique la opción correcta

La principal función de un router es la de tomar una decisión de encaminamiento entre redes.

- Verdadero
- Falso

## 3. Indique la opción correcta

Internet conecta muchos tipos de redes a través de routers, los cuales transmiten datagramas y permiten encaminamiento adaptativo.

- Verdadero
- Falso

## 4. Indique la opción correcta

Los routers realizan fragmentaciones cuando las redes que comunican tienen diferente MTU y también realizan los reensamblados.

- Verdadero
- Falso

## 5. Indique la opción correcta

En la actualidad, los Routers que trabajan sobre líneas telefónicas están diseñados para utilizar datagramas de hasta:

- 576 Bytes.
- 1500 Bytes.
- 4470 Bytes.
- 65536 Bytes.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

- Un datagrama IP puede contener
- Una red Ethernet puede transferir
- Una red FDDI puede permitir
- Una red PPP puede transferir

- hasta 65.536 Bytes
- hasta 1500 Bytes
- hasta 4470 Bytes
- hasta 576 Bytes

## SP6 / H5: Diferentes tipos de interconexión

Hay dos métodos de interconexión:

- Circuito virtual
- Datagrama

En la arquitectura que recomienda el ITU-T (*International Communications Unit*), la interconexión de nodos conmutados provee servicio de circuito virtual entre redes. Para hacer esto, cada nodo de conmutación, está directamente conectado a otros nodos sobre otras redes. Cuando se efectúa un llamado entre dos redes, se establece un circuito virtual entre el host fuente y un nodo sobre la red fuente, entre routers vecino y entre el router remoto y el host destino.

Después que se ha provisto el circuito virtual, se pueden emitir mensajes en forma segura y en secuencia a los gateway vecinos. El control de flujo impide que un gateway envié más tráfico que lo que los vecinos puedan manejar, lo cual es una ventaja.

En forma opuesta al método del circuito virtual del ITU-T, la comunidad Internet ha desarrollado una arquitectura de interconexión que permite conectividad entre redes con diferentes protocolos de acceso. El Sistema Internet difiere en varios aspectos importantes de la arquitectura ITU-T. Los gateway están conectados a otros gateways. Además, el tráfico es enviado a través de la red en forma de datagramas sin establecer previamente un circuito virtual. Y, más importantemente, Internet usa un esquema de encaminamiento adaptativo que garantiza que los paquetes sean intercambiados entre host de diferentes redes, viajando sobre el camino óptimo a través de los routers. Esto tiene como intención, que si un router falla, existe un gateway disponible como alternativa, que puede ser usado automáticamente sin interrumpir la conexión entre host.

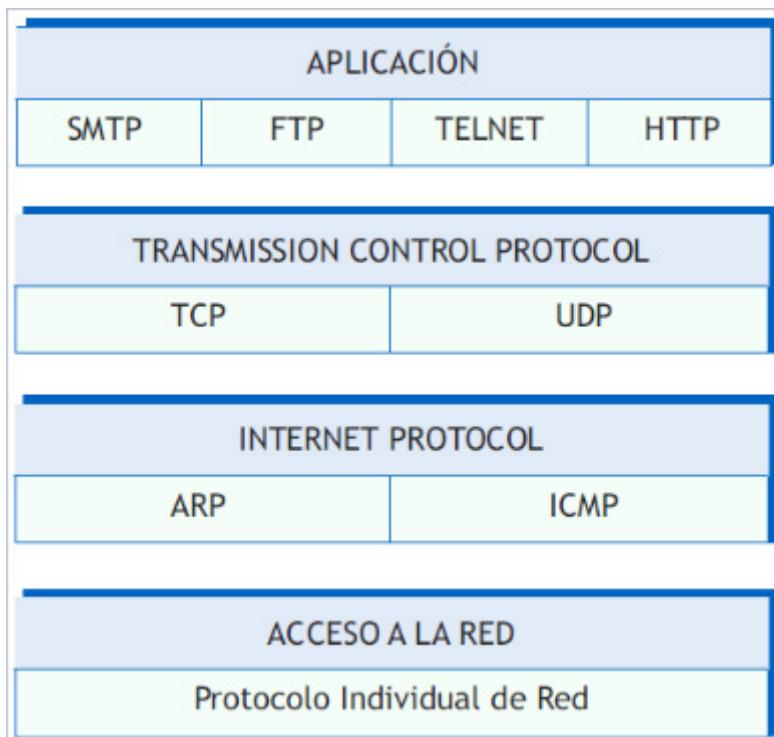
La red Internet está conectada en modo distribuido, con múltiples rutas entre redes. El router decide dinámicamente el mejor camino para rtear mensajes hasta el destino, llevando la cuenta de los cambios de topología cuando ellos ocurren.

La comunidad Internet ha desarrollado una familia de protocolos que ofrecen servicios que pueden carecer las redes subyacentes que forman Internet. Como resultado de esto, pueden ser agregadas fácilmente nuevas redes.

La familia de protocolos Internet provee los siguientes servicios:

- Datagramas
- Direcciónamiento
- Fragmentación y reensamblado de mensajes
- Exactitud y fidelidad de datos
- Secuenciamiento de mensajes
- Control de flujo
- Conexiones

Los protocolos para redes individuales no están especificados en Internet. En lugar de eso, cada red tiene su propio protocolo de acceso. Por ejemplo, Ethernet usa el CSMA/CD.



"Relación entre los protocolos Internet" | Elaboración autor

Los protocolos de redes individuales son usados para encapsular el protocolo IP para transmitirlo a través de la red. Cuando un mensaje atraviesa Internet, cada router crea un nuevo encabezamiento de red apropiado a la próxima red.

## Encaminamiento y entrega de datagramas

El IP, en la segunda capa de la familia de protocolos Internet, transporta datagramas a través de una interconexión de red. Los datagramas son mensajes que contienen "direcciones origen y destino", más los datos. Ellos, al no requerir una entrega segura o en secuencia, (por principio del protocolo IP), no necesitan establecer tipos de conexión para después enviar o recibir. En contraste al servicio de circuito virtual, los cuales están provistos por protocolos punto a punto de extremo a extremo (*end-to-end*).

Una gran ventaja del acceso por datagramas, es que no se requieren muchos servicios de red. Por esta razón, es comparativamente más fácil interconectar redes de características diversas.

IP provee dos servicios básicos: direccionamiento y fragmentación/reensamblado, manteniendo un formato de dirección común a través de Internet.

En la jerga tradicional de TCP/IP, hay sólo dos tipos de dispositivos de red, los "*gateway o router*" y los "*host*".

Los router envían paquetes entre redes y hosts. Si un host es conectado a más de una red (llamado *multi-homed host*), puede enviar paquetes entre las redes. Cuando un multi-homed host envía paquetes, actúa justamente como un gateway y es considerado como tal.

La terminología corriente en la comunicación de datos algunas veces hace distinción entre *gateway* \* 10.1 y *router*, pero en TCP/IP el término *gateway* y *router* son indistintos.

El direccionamiento, que veremos más adelante, es de longitud fija (32 bits) y consiste de la identificación de la red y del host. El campo identificación de red contiene la dirección de una red particular y el campo de dirección local contiene la dirección del host dentro de la red.

Las redes que conforman la Internet tienen diferentes tamaños de mensajes. IP provee un servicio de fragmentación/reensamblado para superar esas variaciones, como ya vimos anteriormente.

Los Routers son los encargados de direccionar los "mensajes", de tal forma que éstos lleguen a destino; no importa qué tan lejos se encuentren las computadoras que establecen la comunicación.

Quizá en este momento esté pensando que los routers tienen que ser equipos formidables, con grandes microprocesadores, discos y espacios en memoria RAM. Nada más alejado de la realidad. En realidad, los routers pueden ser computadoras bastante sencillas, que a veces ni siquiera poseen disco rígido, con microprocesadores que hoy día diríamos antiguos corriendo un software de ruteo. Por ejemplo, se puede implementar un Router con una computadora basada en un microprocesador 286 y 1 MB de RAM.

Si bien la cantidad de redes interconectadas es grande, no es tan grande como la cantidad de host que hay en el mundo. Además cada router no necesita conocer información específica sobre "todas" las redes del mundo, sino simplemente sobre la situación de unos pocos routers vecinos.

Por supuesto que también existen dispositivos electrónicos que actúan específicamente como routers y que poseen prestaciones muy superiores a las ofrecidas por una simple PC que actúa como tal. Por otro lado, una red puede poseer más de un **Router** \* 10.2 lo cual es habitual en redes de gran tamaño.

TCP es un protocolo seguro, orientado a conexión. Éste provee el servicio necesario para la transmisión segura de mensajes sobre el Sistema Internet.

El emisor no necesariamente conoce a través de qué red será ruteado el datagrama para arribar al destino. Por esta razón, es necesario proveer a los mensajes seguridad extremo a extremo (end-to-end), o sea desde la fuente hasta el destino final. Para direccionar estos requerimientos, TCP provee seguridad, control de flujo, multiplexación y funciones de conexión.

La seguridad se logra a través de controles con códigos detectores de errores (checksums error-detecting codes) y reconocimientos positivos (acknowledgements) de los datos. Los datos que no son reconocidos son retransmitidos.

El control de flujo extremo a extremo permite al receptor regular la tasa con la cual estos son enviados. Para permitir muchos procesos (aplicaciones) en un único computador, usar el protocolo simultáneamente, que provee puertos para permitir que los procesos individuales sean identificados. El protocolo también provee un mecanismo para comunicación de procesos entre computadores.

El Protocolo Internet de Control de Mensajes (ICMP = *Internet Control Message Protocol*) es un protocolo de control asociado con IP que es usado para transmitir información de error y de estado al usuario Internet.

## Múltiples Saltos

Entre otras funciones, el router debe tomar una decisión de encaminamiento para todos los datagramas enviados. El procedimiento de encaminamiento provee dos partes:

- Cuál interface de red debe ser usada para enviar el paquete.
- Cuál dirección destino debe estar en el encabezamiento de red local del paquete.

El router mantiene una tabla que contiene una entrada por cada red alcanzable. La entrada consiste, de un

número de red o la dirección del router vecino sobre la ruta más corta (más conveniente según la métrica usada). Un router vecino es aquél que comparte una red común. La medición de distancia que es usada para determinar cuál es el destino final, depende del tipo de protocolo de enrutamiento utilizado. Por ejemplo RIP (*Routing Internet Protocol*, usa el "número de saltos", IGRP usa una métrica compuesta de varios parámetros, como ancho de banda retardo (*delay*), número de saltos, etc. Un router es considerado como de cero saltos, si está directamente conectado a la red; un salto si la red es alcanzable vía otro gateway, y así sucesivamente. Los protocolos de enrutamiento son utilizados para construir la tabla de red o de enrutamiento.

El router verifica la dirección de red destino del encabezamiento del datagrama y compara con la Tabla de Enrutamiento. Si en la tabla no existe esa dirección de red, se destruye el datagrama y envía un paquete ICMP (*Internet Control Message Protocol*) al origen. Si encuentra una entrada para la red en la tabla, usa la dirección de red como dirección destino datagrama.

## El Camino Correcto

El gateway IP usa protocolos de enrutamiento para cuatro funciones específicas:

- Determinación de operatividad de la interface de red.
- Determinación de si el router vecino está operacional.
- Construcción de una tabla de enrutamiento para las redes que pueden ser alcanzadas a través de los gateway vecinos.
- Agregado de un nuevo router vecino y una nueva red a la Tabla de Enrutamiento.

El router usa la información obtenida de los protocolos de enrutamiento para asegurar que un datagrama usa la mejor ruta para alcanzar el destino.

Siempre que un router determina que ha habido cambios en el encaminamiento, Internet envía una actualización de enrutamiento a cada uno de los vecinos. Esta actualización indica para cada red la distancia y dirección del router sobre el camino óptimo a la red.

Cuando se recibe una actualización de encaminamiento, el router recalcula la Tabla de Enrutamiento para asegurarse que está usando el vecino sobre el camino más corto a cada red. Si el paquete de actualización es de un nuevo vecino o contiene información acerca de una nueva red, el gateway actualiza este vecino en la Tabla de Encaminamiento. Si, como resultado de ello, se entera acerca de un nuevo vecino y otra red externa, tendrá que experimentar una reconfiguración.

## El Camino Alternativo

El router usa la información de la tabla de encaminamiento para minimizar la congestión y demora por situaciones de enrutamiento. Por ejemplo, supongamos que hay dos routers, "X" e "Y", que pueden ser usados para alcanzar la red "A". Cuando el router "X" está "caído", todos sus vecinos pueden enviar un reporte de actualización que la red "A" no podrá alcanzarse a través del gateway "X". Cuando un router recibe esta actualización de encaminamiento, recalcula la Tabla y encuentra que puede ser usado el gateway "Y" para alcanzar la red "A". El router ahora envía datagramas a través del gateway "Y" para alcanzar la red "A" sin interrumpir la conexión entre los host.

## Protocolo de Control de Mensajes Internet (*Internet Control Message Protocol*)

Una parte integral de IP es el Internet Control Message Protocol (ICMP) definido en la RFC 792. Este protocolo es parte de la Capa Internet y usa la facilidad de entrega de datagramas IP para enviar los mensajes que realizan los siguientes controles, que reportan errores y funciones informativas para TCP/IP:

- Control de Flujo: cuando los paquetes arriban demasiado rápido para el procesamiento, el host destino o un router intermedio, envía un mensaje (ICMP *Source Quench Message*) para reducir la velocidad del emisor. Éste comunica al origen que cese temporariamente la emisión de datagramas.
- Detección de Destinos Inalcanzables: cuando un destino es inalcanzable, el sistema detecta el problema enviando un "Mensaje de Destino Inalcanzable" (*Destination Unreachable Message*) al origen. Si el destino no alcanzable es una red o host, el mensaje es enviado por un router intermedio. Pero si el destino es un puerto inalcanzable, el host destino envía el mensaje.
- Redirección de rutas: un router envía el "Mensaje de Re-direccionamiento" (ICMP *Redirect Message*) para comunicar al host que debe usar otro router, debido a que este es una opción mejor. Este mensaje sólo puede ser usado cuando el host origen está sobre la misma red.
- Chequeo de Host Remotos: un *host* puede enviar un "Mensaje ICMP de Eco" (ICMP *Echo Message*), más conocido como "*ping*" para verificar si un sistema remoto está operacional. Cuando un sistema recibe un mensaje de eco, éste devuelve el mismo paquete al host origen.

# REFERENCIAS 10

## 10.1 : Gateway

Vale la pena aclarar que en la terminología corriente un gateway mueve datos entre diferentes protocolos y un router mueve datos entre diferentes redes. Así, un sistema que envía correo (mail) entre TCP/IP y OSI es un gateway. Pero en el IP tradicional un gateway es un router. De aquí la confusión que muchas veces se produce al usar esta terminología.

---

## 10.2 : Router

Como acotación para aquellos que hayan tenido algún tipo de contacto con redes; hace algunos años se popularizó el uso de los programas WinRoute y WinGate como software de ruteo. Ambos pueden ejecutarse sobre una simple plataforma Windows. La nueva versión de Windows NT, el Windows 2000; ofrece capacidad propia de ruteo.

---



¿Estás listo para un desafío?

**1. Indique la opción correcta**

TCP es un protocolo seguro, orientado a conexión.

- Verdadero
- Falso

**2. Indique la opción correcta**

El protocolo ICMP (Internet Control Message Protocol) es un protocolo de control asociado con IP que se utiliza para transmitir información de error y de estado al usuario Internet.

- Verdadero
- Falso

**3. Indique la opción correcta**

Además de proveer el servicio necesario para la transmisión segura de mensajes, TCP ofrece otros servicios tales como control de flujo, multiplexación y funciones de conexión.

- Verdadero
- Falso

**4. Indique la opción correcta**

¿Cuáles son los dos métodos de interconexión que se usan en las redes?

- Router y Gateways.
- Circuito virtual y Datagramas.
- Hubs y Switches.
- Bus lineal y Estrella.

**5. Indique la opción correcta**

¿Qué protocolos se utilizan en la Capa de Transmisión en el modelo TCP/IP?

- FTP y HTTP.
- TCP y UDP.

- ARP e ICMP.
- Ethernet y Token Ring.

#### 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

TCP

Reporta errores y funciones informativas.

IP

Provee direccionamiento y fragmentación/reensamblado.

ICMP

Provee seguridad, control de flujo, multiplexación y funciones de conexión.

Circuito virtual

Permite conectividad entre redes con diferentes protocolos de acceso.

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

TCP es un protocolo seguro, orientado a conexión.

Verdadero

Falso

## 2. Indique la opción correcta

El protocolo ICMP (Internet Control Message Protocol) es un protocolo de control asociado con IP que se utiliza para transmitir información de error y de estado al usuario Internet.

Verdadero

Falso

## 3. Indique la opción correcta

Además de proveer el servicio necesario para la transmisión segura de mensajes, TCP ofrece otros servicios tales como control de flujo, multiplexación y funciones de conexión.

Verdadero

Falso

## 4. Indique la opción correcta

¿Cuáles son los dos métodos de interconexión que se usan en las redes?

Router y Gateways.

Circuito virtual y Datagramas.

Hubs y Switches.

Bus lineal y Estrella.

## 5. Indique la opción correcta

¿Qué protocolos se utilizan en la Capa de Transmisión en el modelo TCP/IP?

FTP y HTTP.

TCP y UDP.

ARP e ICMP.

Ethernet y Token Ring.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

TCP

Permite conectividad entre redes con diferentes protocolos de acceso.

IP

Provee seguridad, control de flujo, multiplexación y funciones de conexión.

ICMP

Provee direccionamiento y fragmentación/reensamblado.

Círculo  
virtual

Reporta errores y funciones informativas.



# SP6 / Ejercicio resuelto

Previendo que el nuevo edificio de la empresa debe tener acceso a Internet, haremos uso del modelo TCP/IP para asegurar la conexión lógica que nos permitirá administrar tanto la red privada (intranet) como el acceso a Internet.

Para armar la LAN en el nuevo edificio donde funcionará su primer sucursal y realizar, además de la instalación física, la instalación lógica de la red y establecer la conexión física de las computadoras mediante los cables y los equipos concentradores necesarios realizamos los siguientes pasos:

Armado de una red LAN

1. Instalar las Placas de Red (NIC, por Network Interface Adapter)

- a) Instalación Física
- b) Instalación Lógica

2. Asignar los nombres de usuario y los grupos

3. Definir los recursos compartidos y los accesos a los mismos.

4. Instalar el cableado

5. Instalar el concentrador

**Instalar las Placas de Red (NIC, por Network Interface Adapter)**

Primero deberá verificar si las computadoras poseen o no placas de red; hacemos esta referencia en cuanto a que por lo general las computadoras traen incorporada en forma "on board" una placa de red (habitualmente Ethernet de 100 Mbps y ultimamente de 1 Gbit). Si éste es el caso, saltee este párrafo. Pero si este no es el caso deberá adquirir una NIC (Ethernet, de 100 Mb/s) por cada PC. Los precios de las NICs han disminuido bastante en los últimos tiempos.

a) Instalación Física

Si ha comprado las NICs para cada computadora, lo primero que deberá hacer es instalarlas físicamente en cada PC. El proceso es sumamente sencillo:

- Apague la PC (si estaba encendida).
- Desconecte el cable de alimentación de la misma.
- Descárguese de "estática", tocando cualquier objeto de metal que tenga cerca (o use una muñequera antiestática).
- Quite los tornillos que ajustan el gabinete de la parte trasera.
- Ubique la motherboard.
- Determine en qué slot de expansión ubicará al NIC (lo más probable es que sea un slot PCI).
- Una vez elegido el slot, deberá primero quitar la banda metálica que se encuentra adosada a la estructura del gabinete (si no no podrá poner la placa).
- Inserte la NIC en el slot . Esta operación no requiere de mucha fuerza. Verifique que quede sólidamente engarzada.
- La NIC cuenta con un ángulo metálico. Ajuste el mismo con un tornillo al gabinete. Esto impedirá que la NIC se mueva.
- Cierre el gabinete y ajuste todos los tornillos.
- Conecte nuevamente todos los cables.

Eso fue todo respecto a la instalación física. ¿Fácil, no es cierto?

#### b) Instalación Lógica

Para que su sistema pueda utilizar la NIC, debe primero reconocerla y tener los drivers o controladores que el sistema operativo utilizará para controlarla.

Primero, lea atentamente la documentación adjunta de su placa de red y siga los pasos indicados en ella. Verifique si la misma trae un CD de instalación con los drivers o los controladores de la misma. En general, los pasos a seguir serán los siguientes.

- Encienda su computadora.

El sistema operativo reconocerá que hay un nuevo componente de hardware instalado (su nueva placa de red) y automáticamente lanzará la utilería para Agregar Nuevo Hardware.

Cuando el sistema operativo le pregunte si desea utilizar un disco para cargar los drivers

- Indíquele que sí en el caso que su placa traiga un CD con los mismos, o
- permita que el sistema operativo instale los que considere convenientes, si no los trae.

Una vez que el sistema operativo cargó los drivers es posible que le indique que debe reiniciar el sistema. Aunque no lo indique, es muy conveniente hacerlo.

Una vez que su computadora ha reiniciado, podemos verificar si esta instalación ha traído algún conflicto, y para ello vamos a dar una mirada a la configuración del sistema.

- Siga la siguiente secuencia Botón Inicio > Panel de Control > Sistema y seguridad > Sistema > Administrador de Dispositivos

Se abrirá, entonces, la ventana Administrador de Dispositivos.

Observe la parte superior de la misma y verá que cuenta con 4 solapas. En la tercera de ellas (Ver) observe que tenga seleccionada la opción Ver Dispositivo por tipo.

- En el listado de dispositivos, ubique el llamado Adaptadores de Red.
- Haga clic en el signo más, para desplegar su contenido.
- Allí deberá mostrarse el adaptador de red (o placa de red) que ha instalado. Es muy probable que en muchas computadoras se observen mas de un dispositivo adaptador de red, sobre todo en las notebooks, que además del dispositivo adaptador para redes cableadas tienen el dispositivo adaptador de redes WI-FI.
- Si no hay a la vista ningún indicador amarillo sobre el adaptador, significa que no hay ningún conflicto. En general, no se suelen suscitar conflictos, pero en el caso de que ello ocurriera es muy probable que se deba a un conflicto en el uso de las IRQ (Interrupciones). Si ese es el caso, remítase a la documentación de su placa para cambiarla.

Bien, ya hemos avanzado mucho en la construcción de su red! Ha conseguido que su computadora reconozca a su NIC, de tal forma que ya forma parte de su sistema.

Los drivers instalados le permitirán al sistema operativo enviar y recibir información de la placa de red instalada.

Sin embargo, su NIC no podría todavía comunicarse con las NICs de las otras computadoras que formarán la red: falta definir "en qué idioma" se comunicarán las placas de red entre sí; técnicamente esto significa que debemos asignar un Protocolo de Comunicación a nuestra red.

En principio, el sistema operativo pone a su disposición varios protocolos; los que nos interesa en este momento es TCP/IP.

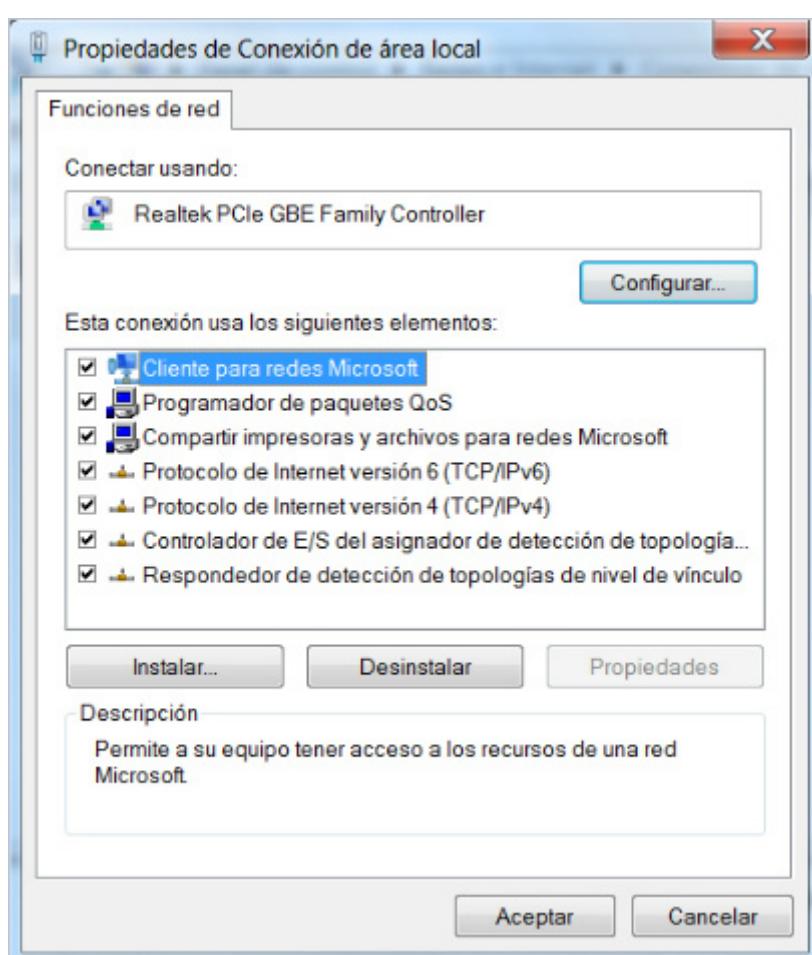
Tenga en cuenta que si bien las computadoras que formarán parte de la red pueden tener placas de red de distinta marca, todas las computadoras que formarán parte de la red deben tener asignado el mismo Protocolo de Comunicación.

Nosotros elegiremos TCP/IP, por razones que verá en las próximas situaciones profesionales (al final de esta materia Ud deberá conocer y comprender con bastante profundidad TCP/IP, ya que será un tema central).

Para asignar TCP/IP como el protocolo de comunicación de nuestra red, debe proceder de la siguiente manera:

- Diríjase al Panel de Control (sigu la secuencia Botón Inicio > Panel de Control > Redes e Internet > Conexiones de Red > Centro de Redes y Recursos Compartidos > Cambiar configuración del Adaptador)
- Sobre la conexión de área local que corresponde al adaptador NIC recientemente instalado, presionar botón derecho: propiedades.
- Se encontrará entonces en la siguiente ventana: inalámbrica y haga doble clic en él.

Se abrirá la ventana Propiedades de Conexión de área local, que presentará un aspecto como el de la siguiente figura:



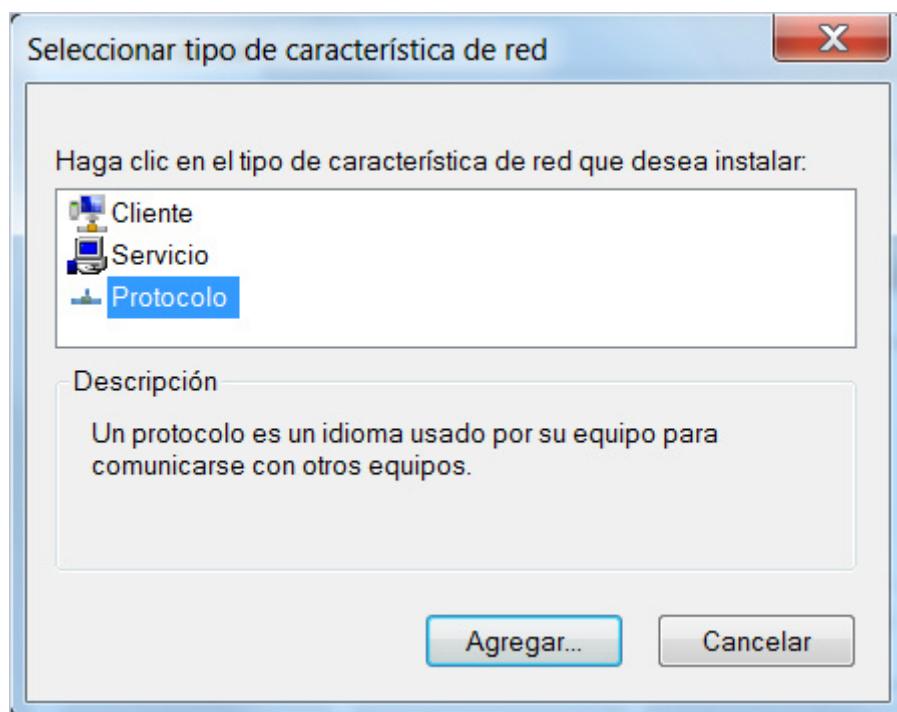
Probablemente en su sistema no figurarán "tantas cosas" como en el que se muestra.

Note que dentro de la solapa Red en la parte superior figura en "Conectar usando" el nombre del dispositivo Adaptador de Red (que es la placa de red) que habíamos instalado antes.

Verificado entonces que se trata de su Placa de Red observe en "Esta conexión usa los siguientes elementos:" si se encuentra disponible Protocolo de Internet versión 4 (TCP/IPv4) y chequeada la casilla de verificación.

Si no se encuentra en la lista haga clic en el botón Instalar...

La siguiente ventana le permite elegir "qué cosa" quiere agregarle a su placa de red,

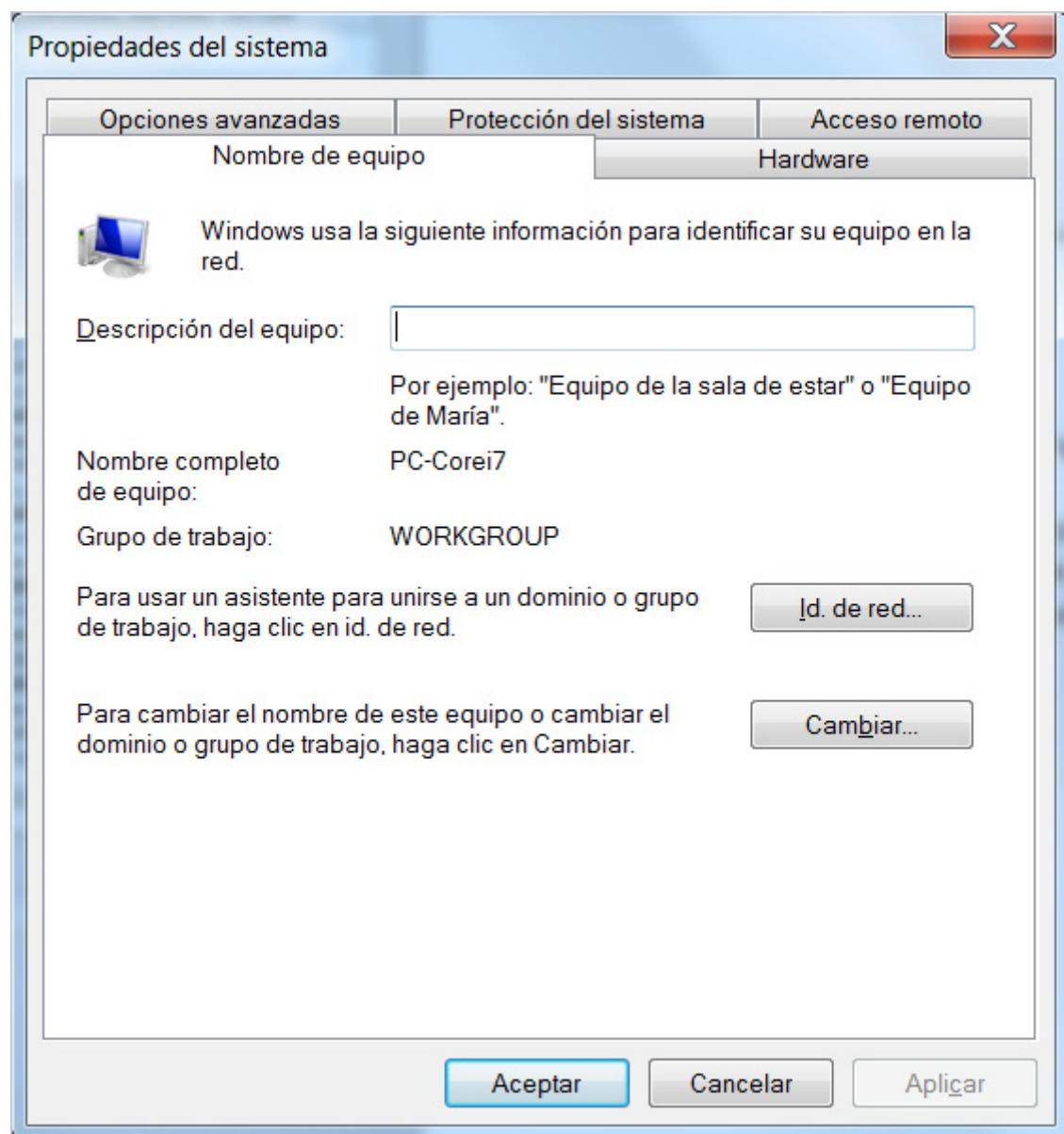


Como nosotros deseamos agregarle un protocolo, seleccionamos Protocolo y hacemos clic en el botón Agregar...

- Seleccionamos Protocolo de Internet versión 4 (TCP/IPv4).
- Por último, haga clic en Aceptar.

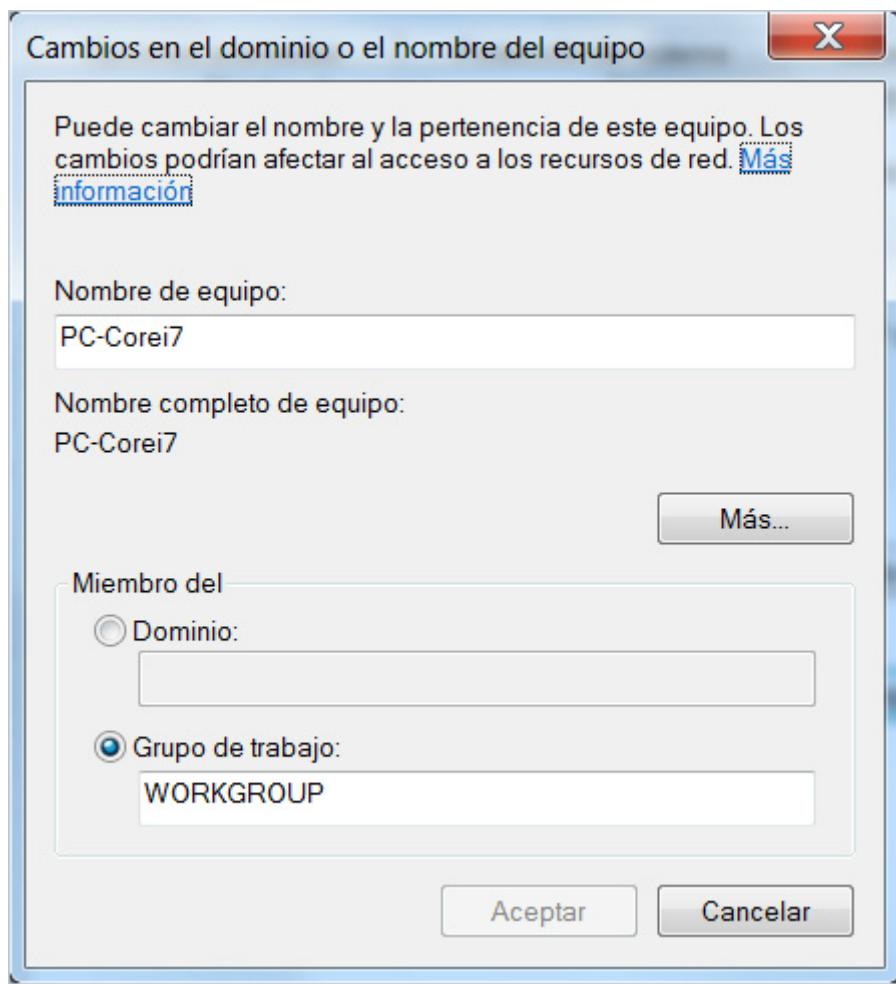
#### Identificar la computadora en la red y establecer algún nivel de seguridad.

- Para ello diríjase al Panel de Control (siga la secuencia Botón Inicio > Panel de Control > Sistema y seguridad > Sistema > Configuración avanzada del sistema)
- En la solapa Nombre del Equipo puede establecer la descripción del Equipo



"Propiedades del Sistema" | Sistema operativo Windows 7

- Para cambiar el nombre del equipo o cambiar el dominio o el grupo de trabajo presione el botón Cambiar...



"Cambiar el nombre del equipo" | Sistema Operativo Windows 7

El nombre de la PC identificará a la misma frente a las otras en la red (es el nombre que van a ver los otros usuarios de la red), por supuesto que éste debe ser distinto para cada computadora.

- En grupo de trabajo será conveniente que ponga el mismo nombre en todas las computadoras. (Si en la red existe un servidor actuando como servidor de dominio, es conveniente utilizarlo).
- Por último puede agregar una breve descripción de la PC.
- Ahora sí puede dar por finalizada su tarea en la ventana red, haciendo clic en el botón aceptar.

De ahora en más cuando haga clic con el botón derecho del mouse sobre cualquier recurso de su computadora (por ejemplo, su disco rígido, o su impresora), verá la opción Compartir. Seleccionándola, usted podrá compartir sus recursos.

Haga la prueba:

- Vaya a cualquier carpeta en su computadora.
- Haga clic con el botón derecho del mouse. Verá la opción compartir. Selecciónela y analice las opciones.

Por supuesto que deberá repetir todo lo visto para cada una de las computadoras que desee conectar a la red.

Para que nuestra red funcione, todavía nos falta algo...

## **Establecer la conexión física de las computadoras mediante los cables y el concentrador**

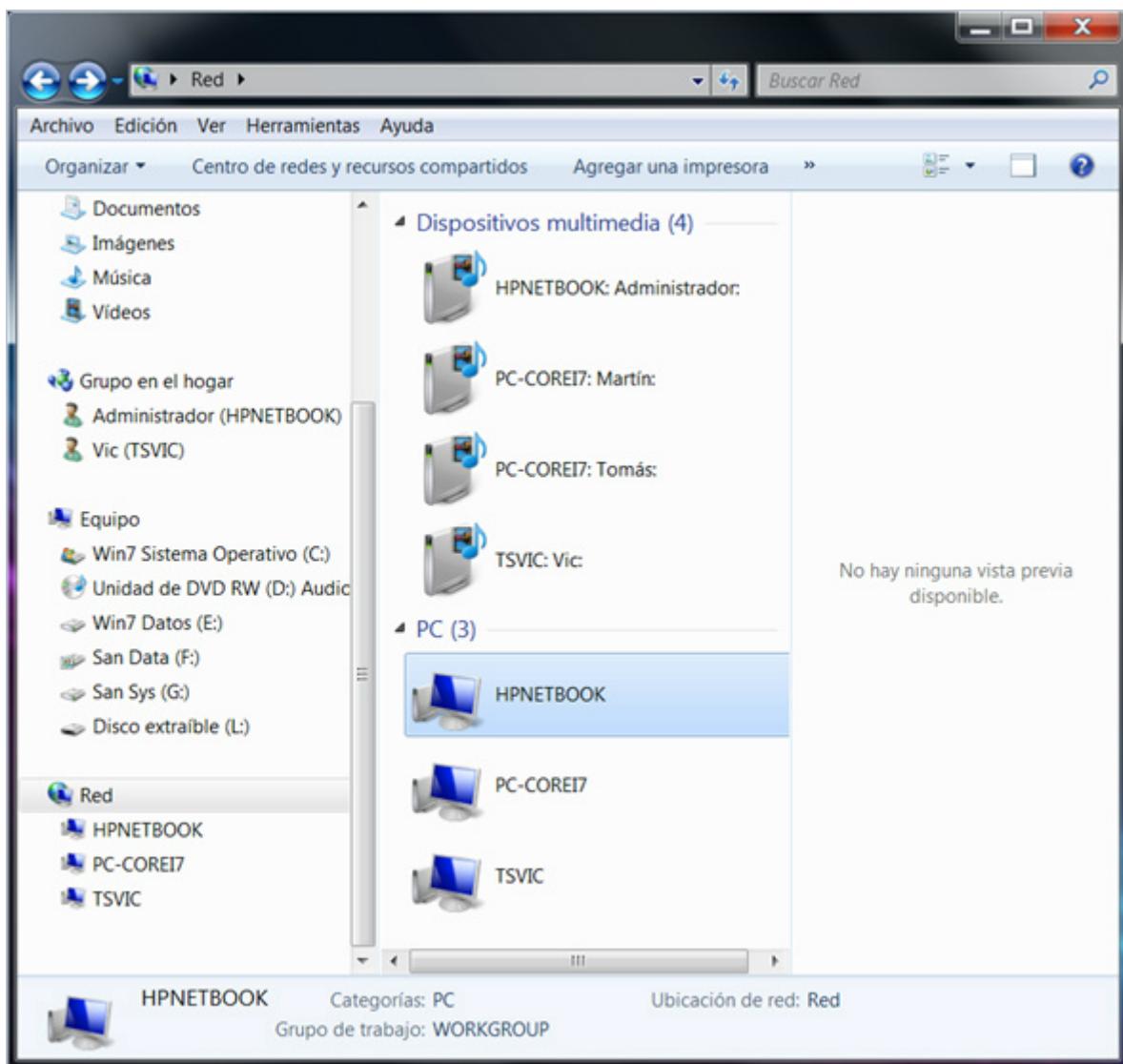
Cuando describimos las características de la red, decidimos utilizar un concentrador.

Al momento de adquirir el concentrador deberá determinar la cantidad de bocas del mismo en función de la cantidad de computadoras que deseé conectar.

- Decida en qué lugar va a ubicar el concentrador, habitualmente se lo puede fijar en una pared o sobre un pequeño estante; no olvide que debe estar en un lugar donde puedan observarse las luces que posee en su frente.
- Determine dónde ubicará cada una de las computadoras y mida la distancia desde cada una de ellas. Así podrá determinar cuánto medirá cada tramo de cable UTP.
- En cuanto al cable, es UTP con conector RJ45. El mismo puede adquirirse "armado" (es decir, con el conector ya ensamblado; suele denominarse "patch cord"). En el caso de que Ud cuente con la pinza adecuada, puede adquirir por separado el cable y los conectores).
- No es bueno que los cables "queden por el piso", así que por lo menos piense en adquirir los metros necesarios de cable canal, por dentro del cual dispondrá los cables.

Si desea vincular sólo dos computadoras, no necesita adquirir un concentrador. En este caso, es posible obviarlo y tender un cable UTP entre las placas de red de ambas. Para que funcione deberá hacer un cambio en la configuración de los pares del cable, como se indicara anteriormente.

- Con las computadoras apagadas, conecte cada placa de red a una boca del concentrador mediante el cable (es indistinto qué extremo del cable utiliza, ya que son iguales). Y ya está...
- Encienda las computadoras e inspeccione el agrupamiento Red



"Red" | Sistema Operativo Windows 7

Aquí podrá ver los dispositivos conectados a la misma y acceder a los recursos compartidos. Piense que ahora sus recursos se han expandido enormemente.

## SP6 / Ejercicio por resolver

En este caso, el ejercicio será una actividad "de laboratorio" individual de armado de conectores RJ45. Se armarán cables (patchcord) directos y cruzados (crossover) y se formarán grupos de alumnos, los que realizarán la siguiente actividad:

1. Armado de los cables usando las herramientas adecuadas.
2. Prueba de funcionamiento con el analizador de cables (LAN-tester).
3. Conexión de dos máquinas por su placa de red ¿Qué tipo de cable usarán?. Justifique su respuesta.
4. Conexión de más PC a través de un Hub o de un Switch.
5. Hacer ping y trace para verificar conectividad. Indicar qué datos de obtienen de la interpretación de la pantalla.
6. ¿Qué pasará si a una máquina se le cambia su dirección IP? Justificar la respuesta.

## SP6 / Evaluación de paso



¡Vamos a comprobar cuánto aprendiste!

**1. Indique la opción correcta**

El protocolo ICMP (Internet Control Message Protocol) realiza los siguientes controles: Control de Flujo, Detección de Destinos Inalcanzables, Redirección de rutas y Chequeo de Host Remotos.

- Verdadero
- Falso

**2. Indique la opción correcta**

En el encapsulamiento, las aplicaciones TCP se refieren a los datos como un "flujo", y las aplicaciones que usan UDP lo llaman "mensajes".

- Verdadero
- Falso

**3. Indique la opción correcta**

TCP utiliza un protocolo de establecimiento de conexión llamado "handshake" a tres vías.

- Verdadero
- Falso

**4. Indique la opción correcta**

TELNET actualmente está implementado en dos módulos: Usuario TELNET y Servidor TELNET.

- Verdadero
- Falso

**5. Indique la opción correcta**

¿Qué tipo de servicio provee el protocolo IP?

- El protocolo IP provee un servicio seguro orientado a conexión.
- El protocolo IP provee un servicio seguro no orientado a conexión.
- El protocolo IP provee un servicio inseguro orientado a conexión.
- El protocolo IP provee un servicio inseguro no orientado a conexión.

**6. Indique la opción correcta**

¿Cuál es la utilidad del protocolo FTP?

- FTP se usa para la transferencia de archivos.
- Compartir archivos por varios host en la red.
- Se usa en aplicaciones Web.
- Se utiliza para distribuir correo electrónico.

**7. Indique la opción correcta**

Los siguientes protocolos: FTP, SMTP, TELNET y HTTP se encuentran en la capa:

- Acceso a Red.
- Interred o Internet.
- Transporte o Transmisión.
- Aplicación.

**8. Ordene relaciones**

En el modelo TCP/IP tenemos cuatro capas, en cada una de ellas operan los siguientes protocolos:

Capa de Acceso a la Red	FTP, SMTP, NFS, HTTP, TELNET, DNS
Capa Internet	IP, ICMP, ARP
Capa de Transmisión	TCP, UDP
Capa de Aplicación	Ethernet, Token Ring, FFDDI, ATM

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

El protocolo ICMP (Internet Control Message Protocol) realiza los siguientes controles: Control de Flujo, Detección de Destinos Inalcanzables, Redirección de rutas y Chequeo de Host Remotos.

- Verdadero
- Falso

## 2. Indique la opción correcta

En el encapsulamiento, las aplicaciones TCP se refieren a los datos como un "flujo", y las aplicaciones que usan UDP lo llaman "mensajes".

- Verdadero
- Falso

## 3. Indique la opción correcta

TCP utiliza un protocolo de establecimiento de conexión llamado "handshake" a tres vías.

- Verdadero
- Falso

## 4. Indique la opción correcta

TELNET actualmente está implementado en dos módulos: Usuario TELNET y Servidor TELNET.

- Verdadero
- Falso

## 5. Indique la opción correcta

¿Qué tipo de servicio provee el protocolo IP?

- El protocolo IP provee un servicio seguro orientado a conexión.
- El protocolo IP provee un servicio seguro no orientado a conexión.
- El protocolo IP provee un servicio inseguro orientado a conexión.
- El protocolo IP provee un servicio inseguro no orientado a conexión.

## 6. Indique la opción correcta

¿Cuál es la utilidad del protocolo FTP?

- FTP se usa para la transferencia de archivos.
- Compartir archivos por varios host en la red.
- Se usa en aplicaciones Web.
- Se utiliza para distribuir correo electrónico.

## 7. Indique la opción correcta

Los siguientes protocolos: FTP, SMTP, TELNET y HTTP se encuentran en la capa:

- Acceso a Red.
- Interred o Internet.
- Transporte o Transmisión.
- Aplicación.

## 8. Ordene relaciones

En el modelo TCP/IP tenemos cuatro capas, en cada una de ellas operan los siguientes protocolos:

Capa de Acceso a la Red	Ehternet, Token Ring, FFDDI, ATM
Capa Internet	FTP, SMTP, NFS, HTTP, TELNET, DNS
Capa de Transmisión	IP, ICMP, ARP
Capa de Aplicación	TCP, UDP

# Situación profesional 7: ¿Cómo diseñar nuestra red LAN?

## Diseño de la red

Ya ha realizado el relevamiento, que le encargara su jefe sobre las necesidades de la empresa y, de acuerdo con el mismo, el grupo de administradores de red ha evaluado la necesidad de contar con una red LAN. Ha podido determinar que deberá conectar computadoras con distintos sistemas operativos, como Windows 9x, Windows NT y Linux. Dadas las características de la red Ethernet, se definió una topología física en estrella con hub o switch. Usará cable UTP categoría 5 o mejor. Deberá tener en cuenta las posiciones de los armarios de cableado y los accesos para la red WAN.

El trabajo de diseño consiste en realizar todos los pasos de documentación para delinear la nueva red de la empresa.

# SP7 / H1: Objetivos de diseño

En esta Situación Profesional se analizará una metodología para la elaboración del diseño de redes.

Inmediatamente nos surge la pregunta: ¿Qué pasos se deberán dar, y en qué orden, para llevar a cabo la tarea encomendada de la mejor forma posible?. Bien vale la pena conocer cuáles son esos pasos.

Podemos no saber nada de nuestro cliente, qué pretende, qué tiene instalado, cuánto está disponible a invertir, en qué marco se desempeña.

Parece una tarea de titanes, pero no desesperemos, la cuestión, si bien compleja, no es tan complicada. A continuación vamos a ver cuáles son esos pasos que debemos seguir para llegar a un buen resultado.

Hemos llamado los pasos a seguir de la siguiente manera:

1. **Objetivos del diseño:** la definición de con qué finalidad se realizará el diseño de la red. Surge del requerimiento del cliente y ser perfecciona con nuestro asesoramiento profesional.
2. **Descripción de la solicitud de red:** descripción de la red actual y de la red solicitada
3. **Metodología para el diseño de redes:** los pasos a seguir para diseñar la nueva red.
4. **Consideraciones antes de comenzar con el diseño:** definición de topologías y equipamiento necesario para operación de la red a distintos niveles (capas)

## Objetivos de diseño

En este primer paso deberemos contemplar tres cuestiones importantes:

- **Diseñar** una red que se ajuste a los requerimientos de rendimiento, seguridad, capacidad y escalabilidad del usuario.
- **Describir una metodología** de manera de simplificar las complejidades asociadas al análisis de la red del cliente y a crear soluciones escalables.
- **Documentar** las aplicaciones, protocolos y topologías actuales y las notas sobre la red actual que son importantes en un proyecto de diseño de red.

En base a estas cuestiones vamos a definir, junto con el cliente, cual es la finalidad de la nueva red, como vamos a hacerlo (cuales van a ser los pasos que vamos a seguir: descripción de la solicitud y metodología para el diseño) y volcar estas intenciones en un escrito (documentar) que nos permita mantener siempre los objetivos.

## Conocimientos previos

Como diseñador deberá analizar redes con diferentes problemas, requerimientos y necesidades y deberá tener las herramientas para enfrentar de la mejor manera el proceso de diseño. Un buen diseño es fundamental; si una red **no** está diseñada de forma adecuada, pueden surgir muchos problemas imprevistos y se puede poner en peligro su crecimiento.

Para llegar a buen puerto es necesario tener en cuenta los conocimientos previos necesarios para el diseño de la red.

- Conocimientos de ingeniería y análisis y diseño de sistemas.
- Conocimientos legales (Leyes, códigos, reglamentos, convenios y ordenanzas).

- Conocimientos técnicos (tecnologías actuales y disponibilidad del mercado).
- Conocimiento de servicios de redes (proveedores de servicios de comunicaciones).



¿Te animás a medir cuánto aprendiste?

**1. Indique la opción correcta**

En la metodología para el diseño de redes el primer paso es plantear los objetivos del diseño.

- Verdadero
- Falso

**2. Indique la opción correcta**

Los objetivos del diseño de red son: diseñar una red que se ajuste a los requerimientos del usuario, describir una metodología para simplificar las complejidades de la red y documentar las aplicaciones y notas sobre la red.

- Verdadero
- Falso

**3. Indique la opción correcta**

Los conocimientos previos necesarios para un buen diseño de red son referidos al diseño de sistemas, legales, técnicos y de servicios de Redes.

- Verdadero
- Falso

**4. Indique la opción correcta**

Para asegurar la consecución de los objetivos, es necesario:

- Definir con el cliente la finalidad de la red.
- Seguir los pasos para describir la solicitud en detalle.
- Seguir una metodología para el diseño.
- Todas las anteriores.

**5. Indique la opción correcta**

Para llegar a un buen diseño es necesario contar también con algunos conocimientos previos tales como:

- Conocimientos técnicos (tecnologías actuales y disponibles en el mercado).
- Conocimiento de servicios de redes (proveedores de servicios de comunicaciones).
- Conocimientos legales (Leyes, códigos, reglamentos, convenios y ordenanzas).
- Todas las anteriores.

#### 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Objetivos del diseño	describe la red actual y la solicitada
Descripción de la solicitud	define la finalidad de la red
Metodología para el diseño	define los pasos a seguir para diseñar la red
Consideraciones	define topologías y equipamiento necesario

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

En la metodología para el diseño de redes el primer paso es plantear los objetivos del diseño.

Verdadero

Falso

## 2. Indique la opción correcta

Los objetivos del diseño de red son: diseñar una red que se ajuste a los requerimientos del usuario, describir una metodología para simplificar las complejidades de la red y documentar las aplicaciones y notas sobre la red.

Verdadero

Falso

## 3. Indique la opción correcta

Los conocimientos previos necesarios para un buen diseño de red son referidos al diseño de sistemas, legales, técnicos y de servicios de Redes.

Verdadero

Falso

## 4. Indique la opción correcta

Para asegurar la consecución de los objetivos, es necesario:

Definir con el cliente la finalidad de la red.

Seguir los pasos para describir la solicitud en detalle.

Seguir una metodología para el diseño.

Todas las anteriores.

## 5. Indique la opción correcta

Para llegar a un buen diseño es necesario contar también con algunos conocimientos previos tales como:

Conocimientos técnicos (tecnologías actuales y disponibles en el mercado).

Conocimiento de servicios de redes (proveedores de servicios de comunicaciones).

Conocimientos legales (Leyes, códigos, reglamentos, convenios y ordenanzas).

Todas las anteriores.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Objetivos del diseño

define la finalidad de la red

Descripción de la solicitud

describe la red actual y la  
solicitada

Metodología para el  
diseño

define los pasos a seguir para  
diseñar la red

Consideraciones

define topologías y  
equipamiento necesario



## SP7 / H2: Descripción de la solicitud de red

A fin de completar el requerimiento del cliente, veremos a continuación una serie de pasos para definir más en detalle cuál es el requerimiento en concreto y el detalle de donde estamos parados y a donde queremos arribar y de qué forma.

Definimos como pasos los siguientes:

1. **Planteo del problema.**
2. **Investigación de la empresa solicitante.**
3. **Análisis de la red por instalar.**
4. **Definición de la red.**
5. **Instalación de la red.**

Posteriormente se detallan algunas reglas prácticas para el diseño de redes que le será muy útil en entornos donde ya existen redes con problemas

### 1. Planteo del Problema (causas por las cuales se solicita la red)

#### Informaciones necesarias

- a) Tareas que desarrolla la empresa.
- b) Planos de la planta o plantas y vistas de los edificios.
- c) Identificación de cada sector.
- d) Suministro y distribución de energía eléctrica.
- e) Red telefónica.
- f) Sistemas de seguridad y protecciones (pararrayos, puestas a tierra, instalación de grupos electrógenos, si los hubiera, etc.).
- g) Riesgos (inundaciones, incendios, etc.).

### 2. Investigación de la empresa solicitante (cliente)

#### Relevamiento

- a) Elaborar las planillas para el relevamiento.
- b) Detalles de equipos existentes.
- c) Instalaciones preexistentes (no sólo de computadoras previamente instaladas).
- d) Datos estadísticos.
  - Cantidad de transacciones, locales y remotas.
  - Cantidad de llamadas telefónicas por motivos operativos y administrativos entre los distintos sectores de la empresa.
  - Uso del correo electrónico.
  - Detalles de la secuencia de operaciones (órdenes de compra, fabricación, depósito, expedición,

etc.).

## Evaluación de los datos relevados

Deberá relacionar los datos relevados con el objetivo del diseño de la nueva red, para ver cómo afecta lo relevado al diseño.

## Proyecto base

- a) Interrelación de los servicios instalados con los existentes.
- b) Confección de los cuadros de tráfico, donde consten tipos de datos, volúmenes frecuencia, horarios, tolerancia a fallas, seguridad, etc.
- c) Tratamiento de los datos.
- d) Planificación de los nuevos servicios por incorporar.
- e) Graficación de los posibles circuitos lógicos.
- f) Relaciones y distancias a cubrir.
- g) Dimensionamiento (velocidad, medios de comunicación posible).
- h) Determinación de las topologías físicas y lógicas.
- i) Selección de los enlaces físicos.
- j) Determinación del tipo de administración de la red.
- k) Verificación.

## 3. Análisis de la red por instalar

### Estudios previos

- a) Determinación de la topología lógica y física.
- b) Determinación del tipo de administración de la red.
- c) Estudio de la carga de tráfico y horarios críticos.

### Cálculos

- a) Demandas tráfico.
- b) Dimensionamiento. (velocidad, medios de comunicación, distancias, etc.)

### Determinación de la red

- a) Selección de los enlaces físicos de acuerdo con las dimensiones obtenidas.
- b) Verificación del dimensionamiento de cada enlace.
- c) Pre-evaluación presupuestaria.

## 4. Definición de la red

### Proyecto

- a) Selección del equipamiento de usuario.
- b) Selección del equipamiento de conectividad necesario.
- c) Evaluación de la contratación de servicios de terceros.
- d) Determinación de alternativas.
- e) Relación costo/beneficio.
- f) Análisis de impacto y futuro crecimiento.

- **Estudio de factibilidad.**

- **Diseño definitivo: confección de planos definitivos**

- **Proyectos alternativos**

- **Presupuestos**

- **Aprobación y/o aceptación del solicitante**

## 5. Instalación de la red

### Pasos

- a. Planificación y programación de tareas
- b. Coordinación
- c. Determinación de los tiempos de instalación
- d. Planes de compra y contrataciones de los medios, equipos y servicios
- e. Instalación
  - Cableado
  - Equipos de conectividad
  - Equipos de usuario
- f. Puesta en marcha
- g. Pruebas de funcionamiento
- h. Entrenamiento al personal
- i. Aprobación
- j. Entrega de los sistemas funcionando.

## Marco de referencia para el diseño de redes pequeñas y medianas

Una vez obtenida cierta cantidad de información del usuario, estará en condiciones de mejorar el diseño de redes pequeñas y medianas, de acuerdo con las siguientes reglas:

- Si tiene problemas de acceso al medio, utilice commutación LAN (switch). Si usted tiene muchas estaciones en un medio compartido (como es Ethernet), tendrá una alta utilización de la red. Los dispositivos tendrán que competir para acceder al medio ocasionando colisiones y tiempos de

respuesta elevados. Introduciendo switches permitirá que se dividan los dominios de colisión, resultando en una menor cantidad de estaciones compitiendo por el medio.

- Si tiene problemas relacionados con los *broadcast*, utilice enrutamiento. Muchos protocolos de LAN utilizan *broadcast* continuamente y no son escalables (cuando se agrupan demasiadas estaciones se producen excesivos broadcasts). Para solucionar esto, puede utilizar routers para dividir su red en subredes y reducir los dominios de broadcast. Se pueden aplicar políticas de acceso y seguridad en los routers para ajustar el rendimiento de la red.
- Si se requiere mayor ancho de banda considere aplicar *Fast Ethernet* o *Gigabit Ethernet*. Una buena opción para las estaciones es aplicar *Switches Fast Ethernet* y realizar los backbones con *Gigabit Ethernet*.



¿Estás listo para un desafío?

**1. Indique la opción correcta**

Los pasos para definir más en detalle cuál es el requerimiento en concreto y el detalle de donde estamos parados y a donde queremos arribar y de que forma son: planteo del problema, investigación de la empresa solicitante, análisis de la red por instalar, definición de la red e instalación de la red.

- Verdadero
- Falso

**2. Indique la opción correcta**

Las reglas básicas en la solución ante problemas de redes son:

- Si tiene problemas de acceso al medio, utilice conmutación LAN (switch).
- Si tiene problemas relacionados con los broadcast, utilice routers.
- Si se requiere mayor ancho de banda, migrar a Fast Ethernet o Gigabit Ethernet.
- Todas las anteriores.

**3. Indique la opción correcta**

Las tareas que desarrolla la empresa, los planos, la identificación de cada sector, el suministro de la energía, los sistemas de seguridad y los riesgos (inundaciones, incendios, etc) forman parte de:

- El planteo del problema.
- La investigación de la empresa solicitante.
- El análisis de la red por instalar.
- La Definición de la red.

**4. Indique la opción correcta**

El relevamiento, la evaluación de los datos relevados y el proyecto base forman parte de:

- El planteo del problema.
- La investigación de la empresa solicitante.
- El análisis de la red por instalar.
- La Definición de la red.

**5. Indique la opción correcta**

Los estudios previos, los cálculos y la determinación de la red se realizan en:

- El planteo del problema.
- La investigación de la empresa solicitante.
- El análisis de la red por instalar.
- La Definición de la red.

**6. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Investigación de la empresa	cableado y equipos
Análisis de la red por instalar	estudios previos, cálculos y determinación de la red
Definición de la red	Relevamiento, evaluación de los datos y proyecto base
Instalación de la red	análisis de impacto y futuro crecimiento

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Los pasos para definir más en detalle cuál es el requerimiento en concreto y el detalle de donde estamos parados y a donde queremos arribar y de que forma son: planteo del problema, investigación de la empresa solicitante, análisis de la red por instalar, definición de la red e instalación de la red.

Verdadero

Falso

## 2. Indique la opción correcta

Las reglas básicas en la solución ante problemas de redes son:

- Si tiene problemas de acceso al medio, utilice conmutación LAN (switch).
- Si tiene problemas relacionados con los broadcast, utilice routers.
- Si se requiere mayor ancho de banda, migrar a Fast Ethernet o Gigabit Ethernet.

Todas las anteriores.

## 3. Indique la opción correcta

Las tareas que desarrolla la empresa, los planos, la identificación de cada sector, el suministro de la energía, los sistemas de seguridad y los riesgos (inundaciones, incendios, etc) forman parte de:

El planteo del problema.

La investigación de la empresa solicitante.

El análisis de la red por instalar.

La Definición de la red.

## 4. Indique la opción correcta

El relevamiento, la evaluación de los datos relevados y el proyecto base forman parte de:

El planteo del problema.

La investigación de la empresa solicitante.

El análisis de la red por instalar.

La Definición de la red.

## 5. Indique la opción correcta

Los estudios previos, los cálculos y la determinación de la red se realizan en:

El planteo del problema.

La investigación de la empresa solicitante.

El análisis de la red por instalar.

La Definición de la red.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Investigación de la  
empresa

Análisis de la red por  
instalar

Relevamiento, evaluación de los  
datos y proyecto base  
estudios previos, cálculos y  
determinación de la red

Definición de la red  
Instalación de la red

análisis de impacto y futuro  
crecimiento  
cableado y equipos

# SP7 / H3: Metodología para el diseño de redes

En las siguientes secciones estudiaremos una metodología para realizar el diseño de una red. La metodología consiste en los siguientes pasos:

1. Relevamiento de información.
2. Evaluación de la red existente.
3. Consideración de los protocolos.
4. Diseño de la LAN.
5. Diseño de la WAN.
6. Generación de la documentación de diseño.
7. Selección de las aplicaciones de administración.
8. Prueba del diseño.

## 1. Relevamiento de información

### Aspectos a tener en cuenta

Los aspectos a tener en cuenta son:

- a. Necesidades de negocios del Usuario.
- b. Requerimientos técnicos del Usuario.
- c. Limitaciones impuestas por el Usuario.

## 2. Evaluación de la red existente

En este paso se debe recolectar toda la información perteneciente a la red actual del usuario. Esta información debe incluir datos de la red física, lógica, las características del tráfico y el sistema de administración de red (NMS: Network Management System) utilizado.

### Evaluación física de la red

El relevamiento físico implica documentar la topología física (cableado y dispositivos de *networking*) de la red. También es necesario documentar las diferentes tecnologías LAN y tecnologías WAN que están en uso.

### Evaluación lógica de la red

La evaluación lógica de la red se utiliza para determinar lo siguiente:

- a. Tipos de protocolos utilizados.
- b. El esquema de direccionamiento.
- c. Mecanismos de seguridad.

### Evaluación del Tráfico:

Para realizar la evaluación del tráfico, debe analizar las siguientes características:

- a. Documente los flujos de tráfico en la red.
- b. Ubique dónde se encuentran los servidores.

## Evaluación de la administración

Determine las herramientas que se utilizan para realizar la administración de la red.

- a. Determine las herramientas de administración.
- b. Ubique la estación de administración.

## 3. Consideración de los protocolos implicados

La razón de existencia de la red es proveer acceso a las aplicaciones de forma remota; por esta razón es muy importante considerar las aplicaciones soportadas por la red.

### Redes Microsoft

Las redes Microsoft utilizan el protocolo de capa de sesión NetBIOS para compartir sus recursos (archivos e impresoras). Cuando NetBIOS corre sobre NetBEUI implica que todas las estaciones que quieran participar en el mismo grupo de trabajo deben pertenecer a la misma red o subred. Por esta razón, las estaciones que utilicen NetBIOS sobre NetBEUI dentro del mismo grupo de trabajo comparten el mismo dominio de broadcast.

### Redes Novell

Novell utiliza el protocolo SAP (Service Advertising Protocol) para permitir que los dispositivos anuncien sus servicios a la red. Los broadcast SAP son generados por los servidores de archivo, servidores de impresión, etc. En redes muy grandes, estos broadcast pueden llegar a saturar la red y se debe considerar la utilización de filtros.

### Redes IBM

Las redes SNA tradicionales implican el uso de SDLC para la conectividad de WAN y Token Ring para las LAN. Las comunicaciones entre hosts y terminales se encuentran puenteadas.

### Servicios Multimedios

Al momento de estudiar una red, debe prestar especial atención a los requisitos para soportar servicios multimedia como voz y video. Se deben utilizar técnicas como *multicasting* para reducir el ancho de banda consumido por estas aplicaciones. La utilización de enrutamiento *multicast* permite transmitir video a estaciones preseleccionadas y reducir al ancho de banda comparado con la utilización de broadcast.

## 4. Diseño de la LAN

El diseño de la red LAN debe comprender requisitos de performance y crecimiento. Para lograr estos requisitos y permitir una escalabilidad futura, se presentan los modelos que se indican a continuación. Como veremos, sólo los modelos jerárquico y modular permitirán escalabilidad y crecimiento. Al momento de realizar el diseño,

se debe tener en cuenta la utilización de hub, switch y routers.

## Modelos de diseño:

### a. Diseños Planos

Las redes planas pueden ser una solución temporal para redes muy pequeñas sin requerimientos de crecimiento ni rendimiento. El crecimiento de las redes planas puede ser caótico y no asegurar una continuidad del servicio. Una característica de los diseños planos es que resulta muy difícil controlar la utilización de la red, teniendo como consecuencia la imposibilidad de asignar niveles de servicios adecuados.

### b. El modelo jerárquico

Para facilitar el diseño de redes escalables y controlables, se presenta un modelo jerárquico de tres capas.

- Capa de Núcleo: Provee commutación de alta velocidad y redundancia de enlaces. Interconecta sitios distantes.
- Capa de Distribución: Provee seguridad y control a través de listas de acceso. Provee también summarización de direcciones y traducción de medios.
- Capa de Acceso: Consiste en la red LAN corporativa y en los diferentes puntos remotos que se conectan a través de enlaces WAN.

### c. El modelo de bloques constructivos

En el modelo de bloques constructivos se representa toda la red como un conjunto de bloques independientes, interconectados donde cada bloque tiene una función específica.

Estos bloques pueden ser:

- Bloques de acceso
- Bloque de Acceso WAN
- Bloque de Servidores
- Bloque de núcleo (interconecta los demás bloques)

La ventaja clave de este modelo es su modularidad. En una red pequeña se puede comenzar con un diseño sencillo; cuando la red crece, el diseño crecerá, manteniendo escalabilidad y cohesión en todos sus puntos.

## Protocolos LAN

Se deben tener en cuenta las características de las diferentes tecnologías LAN, incluyendo la forma de acceso al medio, distancias y tipos de cables: Ethernet (10Base2, 10Base5 y 10BaseT), Fast Ethernet (100BaseT, 100BaseFX), Gigabit Ethernet, Wireless Ethernet, Token Ring, y FDDI. Dependiendo los requerimientos de accesibilidad, rendimiento, distancia y tipos de tráfico, se seleccionará la tecnología que resulte más apropiada.

## Diseño LAN Físico

En este paso se deben seleccionar los dispositivos a utilizar, de acuerdo con la tecnología seleccionada y la cantidad de puertos necesarios.

Las soluciones para LAN pueden incluir las siguientes líneas de dispositivos:

- *Switches.*
- *Routers.*
- *Access Point.*

## 5. Diseño de la WAN

Si bien el diseño de la [WAN](#) \* 11.1 está fuera del alcance de este libro, se dan algunas sugerencias para tener en cuenta en el caso de interconexión de redes de distintas sucursales. En este paso determine el tipo de tecnología WAN por utilizar. Es necesario que estudie los requerimientos del usuario para seleccionar entre las diferentes alternativas. Esta sección contiene un resumen de las actividades involucradas en este paso.

### Selección del transporte

Al tomar la decisión de la tecnología WAN que va a usar, tenga en cuenta lo siguiente:

- \* Utilice líneas dedicadas donde hay tráfico constante entre ambos extremos.
- \* Utilice Frame Relay como transporte económico. Esta tecnología es muy popular y ofrece la posibilidad de realizar numerosos circuitos virtuales permanentes sobre un mismo enlace físico.
- \* Utilice X.25 cuando necesite una alta confiabilidad en los enlaces WAN. X.25 es una tecnología WAN antigua, que aún se aplica, sobre todo cuando se envía poco tráfico y se necesita alta confiabilidad.
- \* Utilice ATM cuando requiera altos anchos de banda (155 Mbps) y calidad de servicios.
- \* Utilice VPN (Red Privadas Virtuales) cuando requiera seguridad, confidencialidad y autenticación en sus comunicaciones.

### Planificación del Ancho de Banda

Es necesario conocer las aplicaciones que se utilizarán en los extremos, para conocer cuánto y qué tipo de ancho de banda se requiere. Utilice la información recopilada en el estudio de la red existente, y tenga en cuenta qué nuevas aplicaciones correrán por la red. Si un vínculo tiene una utilización mayor al 70%, significa que se encuentra saturado y deberá incrementarlo.

### Diseño WAN Físico

En este paso, seleccione los dispositivos que va a utilizar. Tenga en cuenta las tecnologías y la cantidad de puertos necesarias.

## 6. Generación de la documentación de diseño

Luego de trabajar en diseño de LAN, WAN y protocolos, en este paso incorpore todas las soluciones en un diseño global. Verifique que la solución final concuerde con los objetivos del usuario en rendimiento, escalabilidad y costo.

La documentación de diseño ayuda al diseñador a explicar y verificar cómo la solución planteada resuelve los requisitos del proyecto.

Las principales secciones de la documentación son:

- Requerimientos del diseño
- Solución del diseño
- Resumen
- Apéndices
- Costos del diseño propuesto

## 7. Selección de las aplicaciones de administración

Antes de realizar una prueba del diseño, incorpore una solución de administración de red activa que satisfaga las metas del servicio de red que necesita el cliente.

El objetivo básico del management es monitorear la red para localizar problemas antes que ocurran. Se deben recopilar datos estadísticos de la red y documentar el estado actual de la red para utilizarlo como un punto de referencia. Esta documentación actual debería incluir:

- Utilización de la red
- Utilización de los dispositivos de conectividad
- Medición de los tiempos de respuestas

Una vez documentados estos puntos, debe definir cuáles son las metas para un servicio de red aceptable.

## 8. Prueba del diseño

Después de haber propuesto un diseño, el paso siguiente es verificar que ese diseño funcione. Para redes extensas, se puede construir un prototipo; para redes pequeñas se puede realizar una prueba piloto.

### Prueba piloto

- Usado en el diseño de redes pequeñas, con un número pequeño de segmentos o redes WAN simples.
- Usado para demostrar funcionalidad básica, como conectividad.
- Bajo costo por la simplicidad.
- Usado cuando el cliente necesita una pequeña prueba de diseño.

### Prototipo

- Usado en el diseño de redes extensas que pueden expandirse.
- Usado para evaluar funcionalidad compleja.
- Más costoso por el equipamiento y recursos necesarios.
- Usado cuando el cliente necesita una verificación completa de la red.

# REFERENCIAS 11

## 11.1 : WAN

El estudio de las redes WAN, es muy complejo y escapa al alcance de este curso. Los servicios de redes WAN, son provistos generalmente por terceros, que son empresas que tienen capacidades para ofrecer comunicaciones a grandes distancias. En esta Situación profesional, se ha incluido este punto porque forma parte del conjunto de ítems a tener en cuenta en el diseño de las redes de la empresa. En nuestro diseño solo se solicitará que el alumno averigüe las posibilidades de servicios de los proveedores locales.

---



¡Vamos a comprobar cuánto aprendiste!

**1. Indique la opción correcta**

Los primeros pasos para la metodología en el diseño de redes son: el relevamiento de información, la evaluación de la red existente, consideraciones de los protocolos implicados y diseño de la LAN.

- Verdadero
- Falso

**2. Indique la opción correcta**

Los últimos pasos para la metodología en el diseño de redes son: el diseño de la WAN, la generación de la documentación de diseño, la selección de las aplicaciones de administración y la prueba del diseño.

- Verdadero
- Falso

**3. Indique la opción correcta**

Para el relevamiento de información los aspectos a tener en cuenta son:

- Necesidades de negocios del Usuario.
- Requerimientos técnicos del Usuario.
- Limitaciones impuestas por el Usuario.
- Todas las anteriores.

**4. Indique la opción correcta**

El modelo de diseño de red conocido es:

- El modelo plano.
- El modelo jerárquico.
- El modelo de bloques constructivos.
- Todos los anteriores.

**5. Indique la opción correcta**

El modelo jerárquico contiene la siguiente capa:

- Núcleo.
- Acceso WAN.
- Servidores.
- Todas las anteriores.

#### 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Diseño LAN	Modelos, protocolos y diseño físico
Documentación	Utilización de la red, de los dispositivos de conectividad y medición de tiempos
Aplicaciones de administración	Resumen ejecutivo, requerimientos del diseño, solución del diseño
Prueba del diseño	Piloto y Prototipo

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Los primeros pasos para la metodología en el diseño de redes son: el relevamiento de información, la evaluación de la red existente, consideraciones de los protocolos implicados y diseño de la LAN.

- Verdadero
- Falso

## 2. Indique la opción correcta

Los últimos pasos para la metodología en el diseño de redes son: el diseño de la WAN, la generación de la documentación de diseño, la selección de las aplicaciones de administración y la prueba del diseño.

- Verdadero
- Falso

## 3. Indique la opción correcta

Para el relevamiento de información los aspectos a tener en cuenta son:

- Necesidades de negocios del Usuario.
- Requerimientos técnicos del Usuario.
- Limitaciones impuestas por el Usuario.
- Todas las anteriores.

## 4. Indique la opción correcta

El modelo de diseño de red conocido es:

- El modelo plano.
- El modelo jerárquico.
- El modelo de bloques constructivos.
- Todos los anteriores.

## 5. Indique la opción correcta

El modelo jerárquico contiene la siguiente capa:

- Núcleo.
- Acceso WAN.
- Servidores.
- Todas las anteriores.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Diseño LAN

Modelos, protocolos y diseño físico

Documentación

Resumen ejecutivo,  
requerimientos del diseño,  
solución del diseño

Aplicaciones de  
administración  
Prueba del diseño

Utilización de la red, de los  
dispositivos de conectividad y  
medición de tiempos  
Piloto y Prototipo

# SP7 / H4: Consideraciones antes de comenzar con el diseño

Antes de realizar el diseño definitivo de una red LAN (que corresponde con el paso 4 de la metodología para el diseño ya vista en la herramienta anterior) seguir con el método, recordemos algunos conocimientos ya vistos y que debemos tener en cuenta al momento de diseñar definitivamente la topología de la LAN:

## Diseño de Capa 1

En una topología en estrella simple con un solo armario para el cableado, el "Armario Principal" incluye uno o más paneles de conexión cruzada horizontal (HCC). Los cables de conexión HCC se utilizan para conectar el cableado horizontal de Capa 1 con los puertos del switch.

## Topología de Estrella Extendida

Cuando los host de las redes de mayor tamaño están ubicados fuera del límite de 100 metros para el UTP Categoría 5, no es inusual que haya más de un armario para centro de cableado. Al crear múltiples centros de cableado, se crean múltiples áreas de captación. Los armarios secundarios para el cableado se denominan ICC (o IDF). Los estándares TIA/EIA 568-A especifican que los ICC se deben conectar al MCC utilizando cableado vertical, también denominado cableado backbone. Como las longitudes del cableado vertical normalmente superan el límite de 100 metros para el cable UTP Categoría 5, normalmente se utiliza cableado de fibra óptica.

## Los Dispositivos de Capa 2

El propósito de los dispositivos de Capa 2 en la red es suministrar control de flujo, detección de errores, corrección de errores y reducir la congestión en la red. Los dos dispositivos más comunes de Capa 2 (además de la NIC, que todos los host deben tener) son los puentes y los switches de LAN. Los dispositivos de esta capa determinan el tamaño de los dominios de colisión de broadcast.

## Los Dispositivos de Capa 3 - Router

Los dispositivos de Capa 3 (la capa de red) tales como los router, se pueden utilizar para crear segmentos de LAN exclusivos y permitir la comunicación entre segmentos basándose en el direccionamiento de Capa 3 como, por ejemplo, el direccionamiento IP.

Los dispositivos de Capa 3 permiten la segmentación de la LAN en redes lógicas y físicas exclusivas. También permiten la conectividad a redes de área amplia (WAN) como, por ejemplo, Internet.

El enrutamiento determina el flujo de tráfico entre segmentos de red físicos exclusivos basándose en el direccionamiento de Capa 3 como, por ejemplo, red y subred IP. El router es uno de los dispositivos más poderosos en la topología de red.

Como ha aprendido, el router envía paquetes de datos basándose en las direcciones destino. Un router no envía broadcasts basados en LAN, como, por ejemplo, peticiones ARP. Por lo tanto, la interfaz del router se considera como el punto de entrada y salida de un dominio de broadcast y evita que los broadcast lleguen hasta los otros segmentos de LAN:

## Comunicación de VLAN (Virtual LAN)

Un tema importante en la red es la cantidad total de broadcast, tal como las peticiones ARP. Al utilizar las

VLAN, se puede limitar el tráfico de broadcast dentro de una VLAN y, de este modo, crear dominios de broadcast más pequeños. Las VLAN también se pueden utilizar para suministrar seguridad al crear grupos funcionales.

Se utiliza una asociación de puertos para implementar la asignación de VLAN. La comunicación entre las VLAN se puede producir solamente a través del router. Esto limita el tamaño de los dominios de broadcast y utiliza el router para determinar si las VLAN pueden comunicarse. Esto significa que se puede crear un esquema de seguridad basado en la asignación de VLAN.

Se utiliza una asociación de puerto físico para implementar la asignación de VLAN. La comunicación entre las VLAN se puede producir solamente a través del router. Esto limita el tamaño de los dominios de broadcast y utiliza el router para determinar si las VLAN pueden comunicarse. Esto significa que se puede crear un esquema de seguridad basado en la asignación de VLAN.



¿Te animás a medir cuánto aprendiste?

**1. Indique la opción correcta**

El propósito de los dispositivos de Capa 2 en la red es suministrar control de flujo, detección de errores, corrección de errores y reducción de la congestión.

- Verdadero
- Falso

**2. Indique la opción correcta**

Los dispositivos de capa 2 determinan el tamaño de los dominios de colisión del broadcast.

- Verdadero
- Falso

**3. Indique la opción correcta**

Los dispositivos de Capa 3, tales como los router, se pueden utilizar para crear segmentos de LAN exclusivos y permitir la comunicación entre segmentos basándose en el direccionamiento de Capa 3 como, el IP.

- Verdadero
- Falso

**4. Indique la opción correcta**

Los dispositivos de Capa 3 permiten la segmentación de la LAN en redes lógicas y físicas exclusivas. También permiten la conectividad a redes WAN.

- Verdadero
- Falso

**5. Indique la opción correcta**

Los dispositivos más comunes de capa dos son:

- Hubs.
- Switches.

- o Routers.
- o Gateways.

#### 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Topología estrella extendida

suministra control de flujo, detección y corrección de errores

Dispositivo de capa 2

limita el tráfico de broadcast dentro de la VLAN

Dispositivo capa 3

utiliza ICC conectados al MCC mediante cableado vertical o backbone

VLAN

enruta el tráfico en base a direcciones IP evitando broadcasts

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

El propósito de los dispositivos de Capa 2 en la red es suministrar control de flujo, detección de errores, corrección de errores y reducción de la congestión.

- Verdadero
- Falso

## 2. Indique la opción correcta

Los dispositivos de capa 2 determinan el tamaño de los dominios de colisión del broadcast.

- Verdadero
- Falso

## 3. Indique la opción correcta

Los dispositivos de Capa 3, tales como los router, se pueden utilizar para crear segmentos de LAN exclusivos y permitir la comunicación entre segmentos basándose en el direccionamiento de Capa 3 como, el IP.

- Verdadero
- Falso

## 4. Indique la opción correcta

Los dispositivos de Capa 3 permiten la segmentación de la LAN en redes lógicas y físicas exclusivas. También permiten la conectividad a redes WAN.

- Verdadero
- Falso

## 5. Indique la opción correcta

Los dispositivos más comunes de capa dos son:

- Hubs.
- Switches.
- Routers.
- Gateways.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Topología estrella extendida

utiliza ICC conectados al MCC mediante cableado vertical o backbone

Dispositivo de capa 2

suministra control de flujo, detección y corrección de errores

Dispositivo capa 3

enruta el tráfico en base a direcciones IP evitando broadcasts

VLAN

limita el tráfico de broadcast dentro de la VLAN



# SP7 / Ejercicio resuelto: cómo diseñar nuestra red LAN?

## Diseño de la red

Para poder cumplir con las necesidades de expansión de la empresa e integrar las computadoras existentes y también las nuevas que se van a adquirir, realizamos el relevamiento y de acuerdo con el mismo, realizaremos todos los pasos de documentación para delinejar la nueva red de la empresa.

Dadas las características de la red Ethernet, se definió una topología física en estrella con switches en cada piso. Usaremos cable UTP categoría 5e o mejor. Tendremos en cuenta las posiciones de los armarios de cableado y los accesos para la red WAN.

## Diseño de la Red

Los siguientes son todos los pasos para llegar a buen puerto, si bien algunos parecen más relevantes que otros, el hecho de tenerlos a todos nos garantiza que no nos olvidamos de contemplar nada importante

### Conocimientos previos

El primer paso nos indica "conocimientos previos", con lo que hemos visto hasta aquí, tenemos la mayoría de los conocimientos necesarios. Probablemente nos pueda faltar algún conocimiento en cuanto a la reglamentación vigente particular para el lugar de residencia de la empresa. Pero ello no siempre es necesario. Por ejemplo, si tuviera que hacer un cableado fuera de la empresa, debería saber si es posible hacerlo aéreo o deberá hacerlo subterráneo (obviamente, los costos no son los mismos), o si tenemos que realizar un radioenlace, deberíamos saber que se deberá tener los permisos de los organismos que regulan la actividad. Todos los demás conocimientos los hemos visto en las Situaciones Profesionales anteriores.

### Descripción de la solicitud

El siguiente paso nos pide que veamos la descripción de la solicitud. Sabemos que lo que se pretende es la mejora del funcionamiento de la empresa por vinculación electrónica de todos los sectores. Como no tenemos mayor información, ampliaremos con el relevamiento.

### Relevamiento

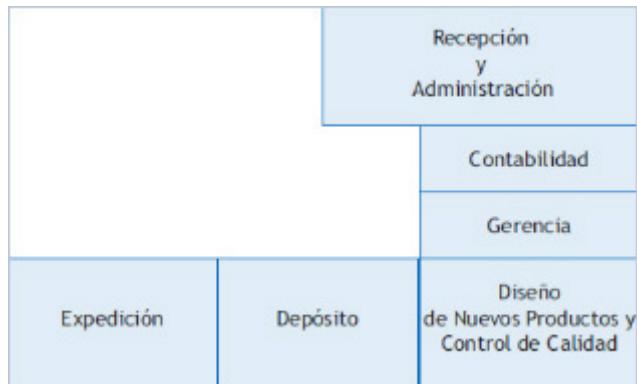
Y ahora sí, no nos queda más que recorrer el lugar y solicitar toda la información necesaria, además de hacer una inspección visual de todos los sectores, sin olvidarnos de ninguno.

Todo comienza con un buen relevamiento.

Comenzamos con una charla con los niveles gerenciales para conocer los detalles de las necesidades de esa empresa.

De esta charla, nos enteramos que debido al crecimiento de la misma se han adquirido equipos de distintas épocas y de distintas características.

Cuando les pedimos los planos de la empresa con la indicación de cada sector y la tarea que allí se realiza, nos entregan un plano, cuyo croquis se indica en el dibujo siguiente. .



El predio tiene una dimensión de 150 metros de frente y 200 metros de fondo.

Además, existe un anexo, en un predio colindante en su costado izquierdo, sobre la misma vereda, en donde funcionarán las oficinas de marketing y ventas y también un salón de venta al público (esta construcción tiene 20 metros de frente por 12 de fondo).

De la información obtenida, nos encontramos con que no había ninguna red instalada. Los equipos funcionaban aislados unos de otros y se intercambia información por medio de pen drives.

Al profundizar la investigación, y de las respuestas que se nos proveyeron, fuimos construyendo nuestra planilla de relevamiento para obtener lo siguiente.

LUGAR	EQUIPO	CANT	SIS. OPER.
Administración	PC Pentium 300 MHz. 64 MB RAM. 6Gb en disco	3	Windows 98
	PC Pentium 166 MHz. 12 MB RAM. 2Gb en disco	2	Windows 95
	PC 486 8 MB RAM. 1Gb en disco	4	Windows 3.11
	Impresora Láser de 4 ppm	1	
	Impresora chorro de tinta color	2	
	Impresora Matriz de puntos	3	
Contabilidad	PC Pentium 300 MHz. 64 MB RAM. 6Gb en disco	2	Windows 98
	PC Pentium 166 MHz. 12 MB RAM. 2Gb en disco	1	Windows 95
	Impresora Láser de 4 ppm	1	
Diseño de Nuevos Productos	PC Pentium 300 MHz. 64 MB RAM. 6Gb en disco	1	Windows 98
	Impresora Láser de 4 ppm	1	
Expedición	PC 486 8 MB RAM. 1Gb en disco	1	Windows 3.11
	Impresora Matriz de puntos	1	
Depósitos	PC 486 8 MB RAM. 1Gb en disco	2	Windows 3.11
	Impresora Matriz de puntos	1	
Venta al Público	PC Pentium 166 MHz. 12 MB RAM. 2Gb en disco	1	Windows 95
	Caja registradora con capacidad de conexión de red	1	
Marketing	PC Pentium 166 MHz. 12 MB RAM. 2Gb en disco	1	Windows 95
	Impresora chorro de tinta color	1	
Gerencia de Ventas	PC Pentium 166 MHz. 12 MB RAM. 2Gb en disco	1	Windows 95
	Impresora Matriz de puntos	1	
Producción	PC Pentium 300 MHz. 64 MB RAM. 4Gb en disco	4	Windows NT
			Workstation
	Placa de red Ethernet 100 Mbps (in board)	4	

Total equipamiento instalado		
PC	23	
Impresoras	12	

Como podemos verificar muy fácilmente, no existe equipamiento ni instalaciones de conectividad. Sí existe una instalación eléctrica, con toma a tierra adecuada.

También hay instalación telefónica interna, mediante una PABX (Central Telefónica Automática, Private Automatic Branch Exchange), de reciente generación, con salida para datos.

Obviamente, al no haber una red, no existen datos en cuanto a las transacciones ni tampoco existe correo electrónico.

### La secuencia de operaciones de la empresa es la siguiente:

A partir de los pedidos de los clientes, provenientes de la gerencia de ventas y de las políticas de la empresa, se generan los pedidos de fabricación (modelos, cantidades, colores, etc.). Estos pedidos son pasados manualmente mediante formularios en papel, desde la Gerencia de Ventas a la Gerencia General. Una vez aprobados por ésta, se pasa una copia a contabilidad, que la envía el depósito que se encarga de las compras

de las materias primas y otra copia a Producción para ejecutar el proceso de fabricación.

Por otra parte, la oficina de administración lleva a cabo las tareas propias de administración, como ser ingresos, egresos, liquidación de sueldos, etc.; para ello se vale de la información proveniente de los sectores de ventas, de expedición y de control de personal.

El sector de marketing diseña las políticas de inserción en el mercado y trabaja en conjunción con la Gerencia de Ventas y de diseño de nuevos Productos.

Dado el crecimiento sostenido de la empresa, deberá asignarse la siguiente cantidad de computadoras adicionales en cada oficina:

Nuevas necesidades de equipamiento

LUGAR	EQUIPO	CANT
Administración	PC	8
	Impresoras	4
Contabilidad	PC	5
	Impresora	2
Gerencia Gral	PC	4
	Impresora	2
Diseño de Nuevos Productos	PC	3
	Impresora	1
	Scanner	1
	Plotter	1
Expedición	PC	2
	Impresora	2
Depósitos	PC	3
	Impresora	2
Venta al Público	PC	3
	Impresora	1
Marketing	PC	3
	Impresora	2
	Scanner	1
Gerencia de Ventas	PC	5
	Impresora	2
Producción	PC	4

En conclusión, debemos agregar el siguiente equipamiento:

Total equipamiento nuevo

PC	36
Impresoras	16
Scanner	2
Plotter	1

Con lo cual la cantidad de equipos a instalar es la siguiente:

Total equipamiento a instalar	
PC	63
Impresoras	30
Scanner	2
Plotter	1
<b>TOTAL</b>	<b>96</b>

Con los datos que hemos relevado y de su evaluación, ya estamos en condiciones de realizar el primer proyecto base.

## Aplicando el método de diseño

A los fines de uniformar, decidimos que el nuevo equipamiento estará constituido por computadoras de escritorio estándar (Código ETAP PC-002)

En la República Argentina existen las normas ETAP (Estándares Tecnológicos para la Administración Pública) que si bien están pensados para que en la administración pública nacional tenga una herramienta para definir con precisión las características técnicas de los equipamientos a adquirir, son estándares de carácter público y son muy útiles como herramienta para utilizar como guía para avanzar en la estandarización y homogeneización de las adquisiciones.

Usted puede bajar las especificaciones técnicas del siguiente [sitio web: Estandares ETAP](#)  
<https://www.argentina.gob.ar/onti/estandares-tecnologicos/guia-de-uso-general-de-los-etap>

Allí, en Especificaciones Técnicas, se detallan las características técnicas de los equipos, identificados por una codificación que permite individualizar únicamente a cada uno de los mismos.

Puede bajar un archivo (haga click en Descargar.zip) con todas las especificaciones técnicas actualizadas.

Le adjunto a continuación uno de esos archivos ([Computadoras Personales ETAP V18.1](#)) \* 12.1 Archivo donde podrá ver el nivel de detalle con que se define cada equipamiento.

De las características principales de la Computadoras de Escritorio Estándar (Código ETAP PC-002) seleccionamos las siguientes:

- Unidad de procesamiento Intel Core I3, AMD Phenom II X4 B95 o rendimiento superior
- Memoria tipo DDR3-1066 o superior capacidad mínima 4 GB
- Disco duro capacidad mínima 250 GB
- Placa de red con características PQR-010 mínimo (100/1000 Mbps auto sensitiva 802.3 con drivers para Windows 7)
- Monitor MN-005 (LCD 17")
- Sistema Operativo Windows 7 Professional o superior, edición 64 bits en español con licencia original.

Las impresoras por adquirir serán todas Láser de escritorio (Impresora electrofotográfica estándar código ETAP PR-015) no siendo necesario, por las características de la tarea a desarrollar, otros equipos más sofisticados.

Hasta ahora no hemos hablado nada de la red, pero todo lo que hicimos es necesario para poder, ahora sí, ver cómo vamos a conectar todo esas máquinas.

Para ello, con el plano en la mano, y las necesidades de cada oficina podemos comenzar a trabajar en la red. Podemos deducir que necesitamos agregar otros equipos, entre ellos servidores y dispositivos de conectividad.

En cuanto a los servidores, tenemos dos opciones: que sean dedicados o no dedicados. En nuestro caso, y por razones de performance y de seguridad decidimos instalar un equipo servidor de red dedicado (Servidor de Red Genérico Código ETAP SR-001). También instalaremos un servidor de impresión (Servidor de Impresión Código ETAP PR-022).

En conclusión, ya sabemos que debemos agregar al presupuesto 2 servidores.

Decidimos instalar el Sistema Operativo de Red *Windows 2008 Server* por dos razones: la primera porque el ambiente existente es *Windows*, por lo que los usuarios ya están acostumbrados a él; además el software de aplicación instalado es de plataforma *Windows*. Con esto salvamos la inversión existente.

Podríamos haber elegido *Windows 2012 Server*, que es la última generación de estos productos, con una serie de supuestas ventajas, pero aquí entra en juego el segundo argumento, que es la confiabilidad de *Windows 2008 Server*, dado que se trata de un producto con probadas características de seguridad y de gran estabilidad. Podríamos haber elegido otras plataformas, tales como *Linux* o algunas versiones de *Unix*, pero nos hemos decidido por ésta de acuerdo con lo explicado más arriba.

Todos los servidores estarán aislados en una "Sala de Servidores", a las que les proveerán todas las medidas de seguridad.

En cuanto al software de las estaciones, instalaremos *Windows 7* en todas las máquinas.

#### Características de la Red

La topología por utilizar será siempre en estrella, con centro en el rack o armario principal. Indicado con un círculo rojo en el plano.

El vínculo entre los nodos se realizará con cable UTP.

### Cableado Horizontal

El cableado será realizado según el concepto de cableado estructurado y cumplirá con las especificaciones de las normas descriptas en las normativas vigentes indicadas en las Características Generales del Cableado.

Se emplearán conductores UTP de 4 pares categoría 5e de 100 ohm de impedancia nominal, Fast Et-hernet (de 100 Mb/s), en virtud de las ventajas comparativas que ofrece este tipo de instalaciones.

Los patchpanels con jacks RJ45 categoría 5 a instalar en los racks de cada nodo, serán de la misma marca que el cable, con capacidad para atender los puestos del nodo correspondiente más un 20% adicional para futuros puestos.

Se proveerán un patchcord para el usuario y uno para el patchpanel por cada puesto de trabajo instalado y serán de idéntica marca al cable instalado.

Los patchcords, desde la electrónica hacia el patch-panel, tendrán una longitud acorde a la ubicación de los elementos dentro del Rack.

Se proveerán patchcord de 2,40 metros para alimentar a los puestos de PC's.

Los patchcord serán categoría 5e armados y certificados en fábrica.

Todos los puestos de datos serán certificados a 100 Mbps bajo las normativas vigentes.

Se contemplará la posibilidad de que el 10% de los puestos de trabajos sean reubicados al momento de su instalación, así como la posibilidad de agregar hasta 10 puestos adicionales.

Se dejarán 5 cables UTP de reserva por cada nodo (nodos secundarios y rack principal) con un extremo rizado

en la patchera y el otro en lugar definido previamente.

## Backbone de Cable UTP

Desde el Rack principal parten cables UTP, a cada nodo secundario. Se instalarán en los Racks patchpanels exclusivos para este fin.

Todos los cables estarán instalados bajo las normativas vigentes citadas en las Características Generales del Cableado. Todos los conductores serán testeados con instrumentos de medición adecuados, que cumplimenten con las normativas de prueba vigentes y los resultados de las mismas serán presentados en informes.

## Características Generales de Cableado Estructurado

La presente arquitectura se basa en una topología de Cableado Estructurado Categoría 5. La capacidad de transmisión del cable es 100 Mhz en una distancia de 90 metros. El cableado está concebido para soportar adecuadamente todos los protocolos destinados a funcionar sobre cableado estructurado en cobre.

El sistema de cableado estructurado, debe satisfacer los requerimientos de sistemas categoría 5, en todos sus componentes, técnicas de interconexión y diseño general, en un todo conforme a las siguientes normas internacionales:

- EIA/TIA-568
- EIA/TIA-569
- TIA/EIA-606

## Racks y Gabinetes

Los Racks serán de 19", de 20U de alto y 800 mm de profundidad, con laterales desmontables, en dos partes por lado, perfil multiperforado 19", puerta delantera de vidrio templado, puerta trasera metálica en dos cuerpos, ambas con cerradura de seguridad, zócalo eléctrico con 10 tomas polarizadas (los Rack contarán con un zócalo extra de 11 tomas polarizadas conectado a la línea de UPS), 4 ventiladores de 4" y luz interior. Se proveerá también organizadores horizontales y verticales en cantidad necesaria para la correcta terminación estética del mismo, soportes horizontales posteriores para todas los patchpanels de datos.

Se proveerán elementos de fijación y tornillos en cantidad igual a 4 unidades por cada U del rack, para la fijación de todas las patcheras y los equipos.

## Canalización

Toda canalización realizada será dimensionada para una capacidad 50% mayor a la necesaria, correctamente fijada y con cajas de inspección de medidas y cantidad adecuadas que permita instalar los cables UTP sin sufrir ningún tipo de fatiga o daño en la protección exterior.

Las canalizaciones, realizadas con elementos del tipo metálicos, tendrán una correcta puesta a tierra vinculadas a la tierra de todo el sistema de Datos; dicha canalización será con separación adecuada y el cable de tensión viajara por un caño corrugado flexible.

- Canalización con bandeja metálica

Serán bandejas metálicas con todos los elementos de fijación que correspondan, con separador central de capacidad necesaria para alojar los cables del Backbone y los cables de energía y datos para los puestos de trabajo que comparten el recorrido de la misma.

Se instalarán dentro de caños metálicos rígidos y/o flexibles con separador central para evitar interferencias.

La derivación de la bandeja a cada uno de los puestos de trabajo se realizará mediante caño metálico con conectores de medidas adecuadas o caño corrugado flexible; para todos los casos, con una capacidad 50% mayor a la necesaria, correctamente fijado y con cajas de inspección de medidas y cantidad adecuadas que permitan instalar los cables UTP sin sufrir ningún tipo de fatiga o daño en la protección exterior.

- Canalizaciones mediante Cable Canal

Se realizará con cable canal de PVC de alto impacto de 63mm, de color similar al tono de las paredes, y estarán provistos de todos los accesorios necesarios para la fijación de tomas de energía y de datos, cuando fuera necesario, como así también para la correcta terminación estética del trabajo.

## Plan de Distribución

La norma de Documentación utilizada en este trabajo es la EIA/TIA-606, que especifica que se debe otorgar un identificador exclusivo a cada unidad de hardware de terminación o en su rótulo. Las Terminaciones de las estaciones deben rotularse en la placa frontal, en el alojamiento o en el conector mismo.

Los rótulos utilizados, según especificaciones UL969, cumplen con los requisitos de legibilidad, resistencia y adhesión. La identificación se realizará con un número de habitación más una letra a cada cable que se tiende a cada terminal de hardware.

En el cableado horizontal, se utilizará un rótulo de color azul en el armario para el cableado solamente, y un rótulo de color verde para el área de trabajo.

Las placas frontales en la pared también deben rotularse para corresponder con cada cable que se utiliza.

La instalación en el patch panel debe realizarse en orden ascendente para poder diagnosticar y detectar problemas fácilmente; además el cable debe estar rotulado en ambos lados o extremos.

Como sabemos que en las redes Ethernet baja la performance a medida que aumenta el tráfico, tenemos que tener mucho cuidado en cómo diseñamos nuestra red.

Es muy probable que debamos establecer más de una red. En este caso, también debemos tener en cuenta luego cómo conectamos esas redes, o subredes.

Para ver cómo vamos a establecer esas redes, nada mejor que tener el plano del edificio y la distribución de equipos por sectores.

Lo primero que haremos es buscar un lugar para los servidores y armarios de conectividad. Para ello, debemos tener en cuenta varias cosas a saber:

- Seguridad
- Accesibilidad
- Facilidad de administración
- Facilidad de cableado
- Distribución homogénea
- Equidistancia a los distintos puntos de la red

De acuerdo con esto, vemos que existen dos lugares con posibilidades. Uno es el de contabilidad y el otro es el de la Gerencia.

Optamos por el primero, ya que ofrece la misma seguridad que el segundo, y además no perturba el trabajo de la Gerencia General.

A partir de este punto, podemos ver que existen al menos cuatro posibles segmentos de red, a los cuales les asociaremos una VLAN cada segmento. \* 12.2

1. Administración - Contabilidad - Gerencia (VLAN 1)
2. Diseño de Nuevos productos - Depósitos - Expedición (VLAN 2)
3. Producción. (VLAN 3)
4. Venta al público - Marketing - Gerencia de Ventas (VLAN 4)

El por qué hemos elegido estos cuatro segmentos lo indicamos a continuación:

El primer segmento lo hemos elegido por sus características homogéneas y porque la cantidad de equipamiento instalado es bastante importante. Además, permite aislar las redes por razones de seguridad. En estos sectores se mueve información reservada de la empresa. Una forma de preservarla es aislar el segmento de red mediante un Switch y creando una VLAN.

El segundo segmento es una línea geográficamente diferenciada de la primera; la cantidad de tráfico en ella puede no ser importante, dado que existe una menor cantidad de equipos instalados, y dadas las características de las tareas que allí se realizan.

Podríamos haber constituido un único segmento de red con el área de producción, pero dado que este sector tendrá equipos dedicados a la producción, nos parece conveniente no mezclar el tráfico, de manera de que una congestión en otro lugar no nos perturbe en normal desarrollo de la actividad.

Por lo que hemos indicado más arriba, decidimos realizar ese tercer segmento hacia el área de producción.

El cuarto y último segmento, lo hemos decidido dado que las oficinas de Ventas y Marketing están físicamente separadas del edificio principal. Esta separación nos permite un mejor mantenimiento de la red. Además, las distancias a cubrir nos obligan a tener que tomar algunas medidas extras, tales como poner repetidores, o algún otro dispositivo que nos permita alcanzar esas distancias.

Una vez que hemos decidido los segmentos necesarios, podemos dibujar el cableado, pero antes que nada, vamos a decidir cómo saldremos del servidor y cómo podemos establecer los cuatro segmentos de red.

Si recuerda, decidimos instalar los servidores, agrupados en una sala de servidores. Con un cable UTP5 llegaremos hasta el sector y con un **switch de 12 puertos** \* 12.3 cubrimos las necesidades del mismo.

Para poder hacer los tres segmentos, colocaremos un Switch (dispositivo de interconexión de redes, en la SP11 definiremos con precisión cómo funciona).

Para ello lo instalaremos cerca de los servidores (armario principal) y de allí saldremos con los tres segmentos de red. Veamos cómo será el primer segmento, o sea, el que incluye la administración, contabilidad y gerencia.

Desde el Switch, salimos con los cables necesarios que irán hasta la Gerencia, hasta Contabilidad y hasta la Administración. En la Gerencia necesitamos instalar 4 PCs y 2 Impresoras. Para ello necesitamos 6 cables, pero tenderemos 10 para futuros crecimientos. Y de allí, con un pathcord, llegaremos a cada máquina.

Llegamos al sector de Contabilidad con otro de los canales para cables UTP5, donde instalaremos las bocas necesarias, quedando prácticamente cubierto desde otro switch instalado en el armario principal. En caso de necesidad, podremos agregar desde uno de los puertos otro switch, con lo que obtendremos bocas de conexión adicionales.

Con el tercer canal llegaremos al área de Administración. Aquí necesitamos 22 puestos de conexión, así que pondremos otro switch de 24 puertos. Si en el futuro necesitamos tener más puertos, agregamos otro switch, el cual lo conectaremos a uno de los puertos.

Otro segmento es el que va hacia los Depósitos, Expedición y Desarrollo de Nuevos Productos. Para ello necesitamos 18 puertos. Allí pondremos un hub de 24 puertos en la oficina de Diseño de Nuevos Productos, y de allí llegamos hasta los puestos con cable UTP5.

El otro segmento de red es hacia el edificio contiguo, o sea el de Ventas y Marketing. Para ello, y dado que son colindantes, extenderemos el cableado a través del muro de Depósitos y Expedición y luego por la medianera hasta llegar al otro edificio. Entraremos a éste y pondremos un switch en la Oficina de Marketing y de allí distribuiremos hacia el resto.

El cableado en el muro medianero debería ser protegido con caños flexibles metálicos para aislarlos de ruidos y descargas atmosféricas.

**Aquí, al verificar las distancias nos encontramos con dos problemas:**

1. En el tramo que va a la zona de producción, encontramos que el switch debe emplazarse sobre la pared del fondo, con lo cual la distancia hasta allí es de unos 150 metros; hay que tener en cuenta que el cable no va en línea recta, sino que debe seguir la estructura de muros o techos del edificio, por lo que a veces hay que subir o bajar, o dar vueltas para llegar a una ubicación determinada; esto hace que la distancia sea bastante mayor que si trazáramos una línea recta entre dos puntos. Como hemos elegido cable estructurado UTP5, los tramos deberán tener una longitud máxima de 300 pies, algo así como unos 100 metros aproximadamente. Por lo tanto, debemos proponer otra solución para este tramo.
2. En el tramo que va al edificio colindante (zona de venta y marketing) ocurre lo mismo que en el caso anterior, la distancia hasta allí es de más de 100 metros; por las mismas consideraciones de instalación explicadas en el punto 1.

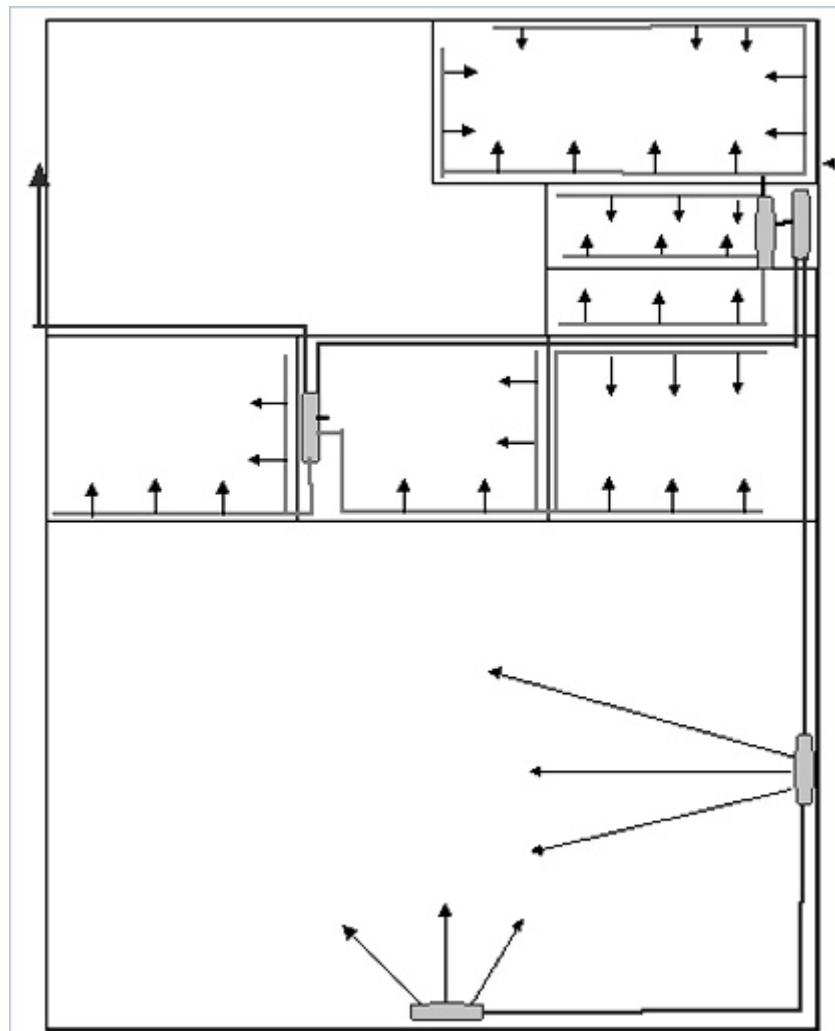
Veamos las posibles soluciones:

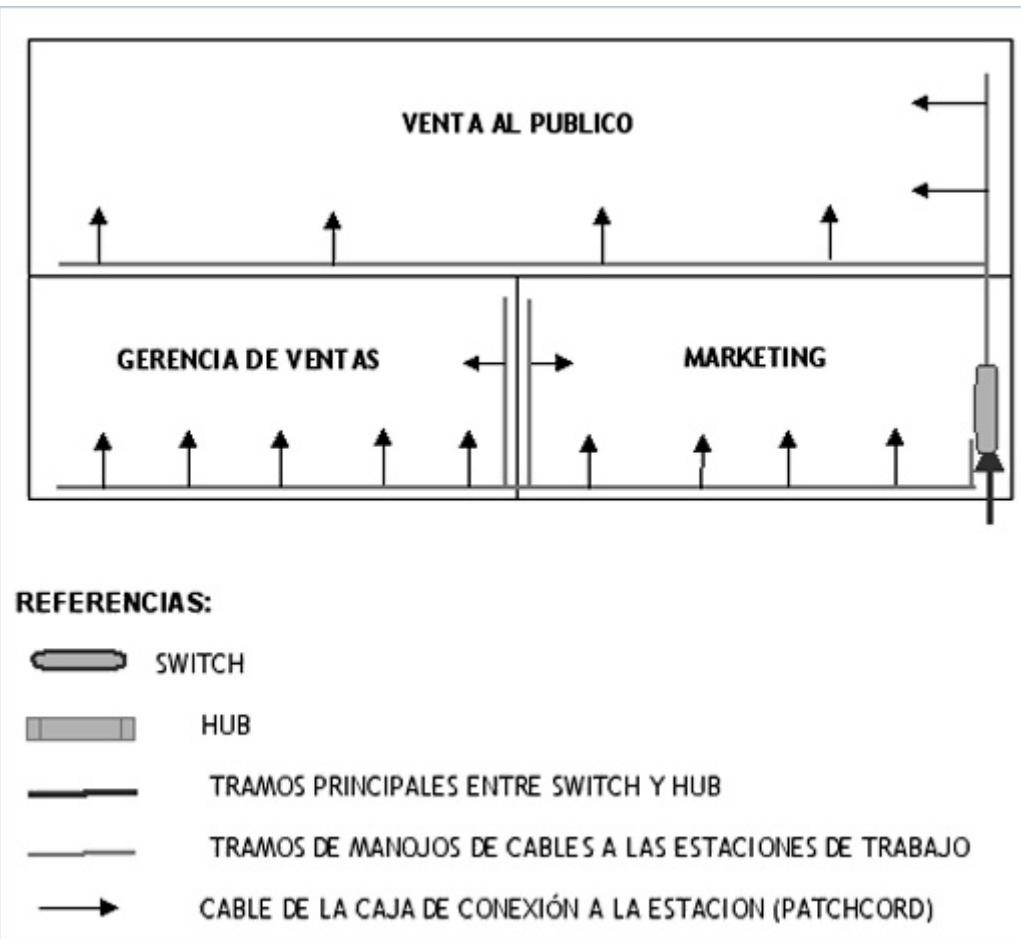
1. Una alternativa es hacer un backbone (cableado troncal) de cable coaxial o de fibra óptica. Con esta solución se pueden alcanzar distancias mayores, con el coaxial RG58 (10Base5) podemos alcanzar hasta 500 metros, mientras con la fibra óptica multimodo (que es más económica y de más fácil instalación), podemos alcanzar los 2000 metros.
2. La otra es encadenar switch, para alcanzar las distancias; dicho de otra manera, el tramo entre un switch y otro no puede superar los 100 metros, por lo cual podemos poner varios segmentos encadenados con switch. Esto -obviamente- tiene una limitación, ya que no podemos hacer más de 4 saltos. Pero en nuestro caso sería factible, ya que sólo necesitaríamos dos.

Vamos a optar por esta segunda alternativa, ya que la primera implica una instalación más sofisticada, con mayores costos, sobre todo la de fibra óptica, que requiere de personal especializado para realizarla.

Mientras que en el segundo caso, lo podemos hacer nosotros mismos, y sólo debemos adquirir un switch adicional. Esto nos provee de una ventaja extra ya que nos quedarán puertos de conexión libres para futuros crecimientos, (sólo tendremos que tender los cables entre el switch y los puestos de trabajo).

Para ello, veamos cómo quedará nuestra instalación:





En el tramo de Producción, colocaremos un armario con un switch aproximadamente a la mitad de la pared derecha, de allí alcanzaremos todas las máquinas que están cerca. Desde aquí tenderemos otro cable hasta la pared del fondo y ahí pondremos un segundo switch para alcanzar desde ese lugar al resto de las máquinas. Con esto queda solucionado el problema.

Al otro tramo, el que va a Ventas, lo solucionaremos de la siguiente manera: pondremos un Switch en el área de depósitos, conectado al switch principal, y desde este saldremos con un canal para la zona de Depósitos, Expedición y Diseño de Nuevos Productos. Por otro puerto del switch saldremos hacia el edificio colindante, y ahora sí, desde este switch alcanzaremos a las máquinas de esta área.

Podríamos habernos ahorrado un switch, instalando las máquinas del sector de Depósitos directamente al switch, pero el ahorro que podemos lograr no lo justifica. Además, es preferible dejar puertos libres para futuros crecimientos.

Otra cuestión a definir está referida a los tiempos de instalación. Se debe tener en cuenta que no podemos alterar el funcionamiento normal de la empresa. Debemos considerar los planes de compra, para asegurarnos de tener todo el material antes de iniciar la instalación. Luego de instalado, se deberán hacer las pruebas de funcionamiento y capacitación al personal que va a operar la red.

Ahora ya tenemos nuestro proyecto base. No resultó tan difícil como parecía a priori.

Por los conocimientos que tenemos y por el relevamiento realizado sabemos que es totalmente factible (totalmente realizable con la tecnología disponible).

Sólo nos resta verificar si el modelo propuesto es aceptable (es decir que, quien tome la decisión, acepte realizar el proyecto, asumiendo los costos del mismo).

Debemos hacer una planilla con los costos de la inversión. Haremos dos planillas, una para los equipos de computación (PCs, Impresoras, etc.). La otra para el cableado de la red y los dispositivos de conectividad (switches y otros).

#### Costo por equipos de computación

EQUIPOS	CANT	PRECIO UNIT	PRECIO TOTAL
PC	36	1.200,00	43.200,00
IMPRESORAS	16	800,00	12.800,00
SCANNER	2	200,00	400,00
PLOTTER	1	500,00	500,00
	TOTAL		56.900,00

#### Costo de la red

DISPOSITIVO	CANT	UNIDAD	PRECIO UNITARIO	PRECIO TOTAL
SWITCH	6		1.000,00	6.000,00
CABLE UTP	2400	Metros	0,30	720,00
ROSETAS P/CONEXIÓN RJ45	96		1,20	115,20
FICHAS RJ45	100		0,10	10,00
PATCHCORD	96		2,00	192,00
CABLE CANAL	350	Metros	0,20	70,00
SOFTWARE DE RED	1			5000,00
PRECINTOS P/FIJACIÓN	500	100Unid.	1,50	11.25
			TOTAL	12118,45

El costo total será, entonces, la suma de ambos conceptos, lo que nos da:

**COSTO TOTAL : u\$s 12118.45**

Ahora sólo nos resta presentar el proyecto a las autoridades de la empresa para confirmar si aceptan su realización.

Sólo nos queda hacer los planos definitivos, para que luego al llevar a cabo la instalación, se realice de acuerdo con lo planificado.

# REFERENCIAS 12

## 12.1 Archivo: ETAP 18.1

[ETAP 18.1.pdf \(198.14 KB\)](#)

---

## 12.2 : VLAN

Las VLAN (Virtual Local Aera Network) son redes lógicamente independientes dentro de una misma red física. Trataremos este tema en la SP11

---

## 12.3 : Elección del switch

Elegiremos, para uniformar switch de 12 ó 24 puertos, a los fines de poder intercambiarlos fácilmente, y además debemos prever el crecimiento futuro.

---

## SP7 / Ejercicio por resolver

El ejercicio será una actividad para desarrollar a lo largo de todo el semestre. Se realizará el diseño de una red que será propuesta por el docente y que deberá contener al menos las siguientes actividades:

1. Un edificio de cinco pisos mínimo como Casa Central, con algún piso con una superficie mínima de 1000 metros. El resto de los pisos no debe ser menor de 500 metros.
2. En esta Casa se instalarán 250 puestos de trabajo, más un 20 % para futuro crecimiento.
  - Los puestos de trabajo se identificarán como Tipo A y Tipo B. Los de tipo A tendrán dos bocas para señal y 3 tomacorrientes normalizados. Los del tipo B tendrán una boca para señal y dos tomacorrientes normalizados.
  - Los puestos tipo A serán el 80 % del total, mientras que los del tipo B serán el 20 % restante.
3. Una sucursal alejada como mínimo 200 metros de la Casa Central. Con una planta. Allí se instalarán 50 puestos de trabajo, con las mismas características anteriores, o sea 80 % tipo A y 20 % tipo B.
4. Una Sucursal en otra localidad distinta a la de la Casa Central. Allí se instalarán 20 puestos de trabajo, con las mismas características anteriores, o sea 80 % tipo A y 20 % tipo B.
5. Se deberá contratar un servicio de Internet de manera que todas las máquinas, tanto de la Casa Central como las Sucursales puedan tener acceso, a través de un servidor Web ubicado en la Casa Central.
6. Se deberán realizar todos los cómputos métricos y costos de toda la instalación, la que incluye instalación de:
  - Cableado estructurado UTP 5e o superior.
  - Instalación eléctrica adecuada para los puestos de trabajo.
  - Canalizaciones para la instalación del cableado estructurado y de energía eléctrica.
  - Costos de los armarios y manos de obra.

## SP7 / Evaluación de paso



¿Estás listo para un desafío?

**1. Indique la opción correcta**

Para redes extensas, se puede construir un prototipo; para redes pequeñas se puede realizar una prueba piloto.

- Verdadero
- Falso

**2. Indique la opción correcta**

El proyecto, el estudio de factibilidad, el diseño definitivo y los proyectos alternativos de la red se realizan en:

- El planteo del problema.
- La investigación de la empresa solicitante.
- El análisis de la red por instalar.
- La Definición de la red.

**3. Indique la opción correcta**

La planificación y programación de tareas, la coordinación, determinación de los tiempos de instalación y planes de compra e realizan en:

- La investigación de la empresa solicitante.
- El análisis de la red por instalar.
- La Definición de la red.
- La Instalación de la red.

**4. Indique la opción correcta**

Al utilizar tecnologías LAN se deben tener en cuenta la siguiente tecnología:

- Fast Ethernet.
- Gigabit Ethernet.
- FDDI.
- Todas las anteriores.

**5. Indique la opción correcta**

Cual de los siguientes son ejemplos de tecnologías WAN:

- Frame Relay.
- ATM.
- X.25.
- Todos los anteriores.

**6. Indique la opción correcta**

En el diseño de la WAN debe tenerse en cuenta:

- Selección del transporte.
- Planeamiento del Ancho de Banda.
- Diseño Físico.
- Todas las anteriores.

**7. Indique la opción correcta**

Para realizar la evaluación del tráfico, ¿cuáles de las siguientes son características por analizar?

- Documentar los flujos de tráfico en la red y ubicar los servidores.
- Determinar los tipo de protocolos utilizados y el esquema de direccionamiento.
- Determinar las herramientas de administración y ubicar la estación de administración.
- Documentar la topología física del cableado y los dispositivos de networking de la red.

**8. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Objetivos del diseño

Analizar sistemas, leyes,  
tecnologías y servicios de red

Conocimientos previos

Definir los pasos para realizar el  
diseño de una red

Descripción de la  
solicitud

Definir con precisión la red  
actual y la solicitada

Metodología para el  
diseño

Diseñar, describir y documentar  
los requerimientos

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Para redes extensas, se puede construir un prototipo; para redes pequeñas se puede realizar una prueba piloto.

- Verdadero
- Falso

## 2. Indique la opción correcta

El proyecto, el estudio de factibilidad, el diseño definitivo y los proyectos alternativos de la red se realizan en:

- El planteo del problema.
- La investigación de la empresa solicitante.
- El análisis de la red por instalar.
- La Definición de la red.

## 3. Indique la opción correcta

La planificación y programación de tareas, la coordinación, determinación de los tiempos de instalación y planes de compra e realizan en:

- La investigación de la empresa solicitante.
- El análisis de la red por instalar.
- La Definición de la red.
- La Instalación de la red.

## 4. Indique la opción correcta

Al utilizar tecnologías LAN se deben tener en cuenta la siguiente tecnología:

- Fast Ethernet.
- Gigabit Ethernet.
- FDDI.
- Todas las anteriores.

## 5. Indique la opción correcta

Cual de los siguientes son ejemplos de tecnologías WAN:

- Frame Relay.
- ATM.
- X.25.
- Todos los anteriores.

## 6. Indique la opción correcta

En el diseño de la WAN debe tenerse en cuenta:

- Selección del transporte.
- Planeamiento del Ancho de Banda.
- Diseño Físico.
- Todas las anteriores.

**7. Indique la opción correcta**

Para realizar la evaluación del tráfico, ¿cuáles de las siguientes son características por analizar?

- Documentar los flujos de tráfico en la red y ubicar los servidores.
- Determinar los tipo de protocolos utilizados y el esquema de direccionamiento.
- Determinar las herramientas de administración y ubicar la estación de administración.
- Documentar la topología física del cableado y los dispositivos de networking de la red.

**8. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Objetivos del diseño	Diseñar, describir y documentar los requerimientos
Conocimientos previos	Analizar sistemas, leyes, tecnologías y servicios de red
Descripción de la solicitud	Definir con precisión la red actual y la solicitada
Metodología para el diseño	Definir los pasos para realizar el diseño de una red

# **Situación profesional 8: ¿Cómo será el direccionamiento de nuestra red?**

## **La capa de red en el modelo TCP/IP**

Las computadoras necesitan una dirección para lógica que tiene que ver con el dominio asignado, y para ello debemos dar direcciones IP a las distintas redes. Es por ello imprescindible conocer cómo es la estructura de direccionamiento previsto en el modelo TCP/IP. Comprenderá también cómo se realiza la resolución de direcciones a través del protocolo ARP.

Esto le ayudará a monitorear la red y a resolver fallas. Podrá decidir sobre las distintas redes de información y también definir la MTU (Máxima Unidad de Transferencia) para optimizar el rendimiento.

## SP8 / H1: La entrega de datos

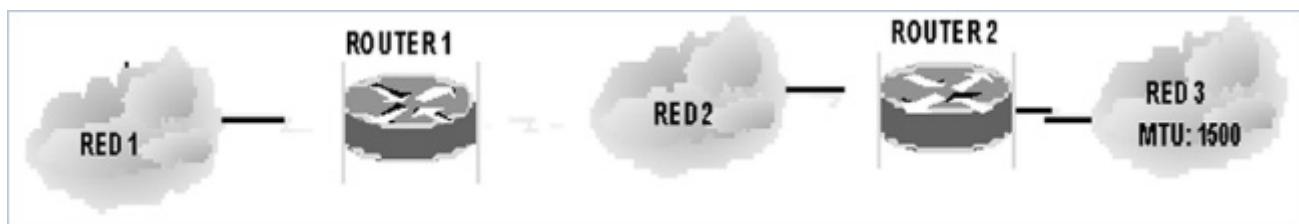
Hasta aquí hemos visto la arquitectura básica y diseño de los protocolos TCP/IP. De esta discusión, conocemos que TCP/IP es un modelo jerárquico de cuatro capas. Ahora veremos cómo se mueven los datos entre las capas de protocolos y el sistema de red. Para ellos necesitamos examinar la estructura de las direcciones Internet (IP addresses), incluyendo cómo se encaminan los datos hasta el destino final y cómo las reglas de enrutamiento son redefinidas localmente para crear subredes. Vamos a ver también los protocolos que comparten la capa IP.

El IP es usado por la capa Internet para proveer servicios de red a través de múltiples routers.

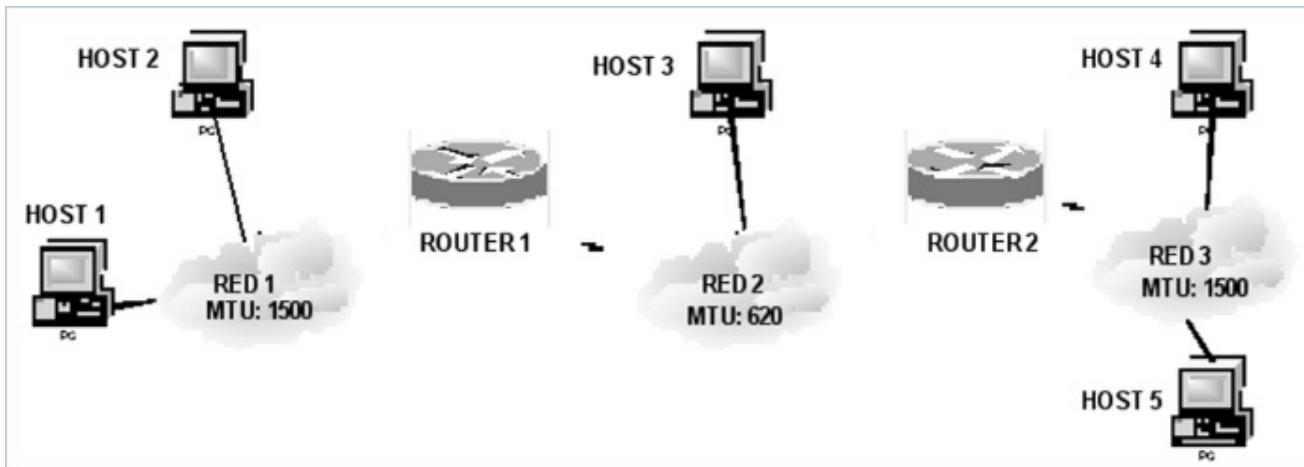
Para que dos redes puedan conectarse, deben estar vinculadas mediante una "computadora" que esté dispuesta a ofrecer servicios de transmisión de paquetes en ambos sentidos. Estas "computadoras" que comunican redes, se denominan "*routers o gateways*". En la actualidad se acepta denominar *router* (ruteador) al elemento que realiza las comunicaciones a nivel de capa de red, guardándose el término de Gateways para las comunicaciones a nivel de las capas superiores del modelo OSI.

Un "*router*" es un procesador de uso específico, que conecta dos o más redes, cuya función primaria es retransmitir datos de una red a otra, desde el host origen al destino.

Es importante tener en cuenta que las redes interconectadas por los Routers pueden ser de diversa índole: ethernet, Token Ring, redes troncales, o una simple conexión punto a punto. Tampoco influye si son redes basadas en servidor o *peer to peer*.



Obviamente que el objetivo principal de una red de redes, como Internet, es la de proveer servicios de interconexión a usuarios finales, es decir a computadoras individuales. Habitualmente a las computadoras individuales se las denomina *host* (anfitriones), y éstas son las que se encuentran conectadas a cada una de las redes, las cuales a su vez se encuentran interconectadas mediante los Router, como se muestra en la siguiente figura.



Los Routers son los encargados de direccionar los "mensajes", de tal forma que éstos lleguen a destino; no importa qué tan lejos se encuentren las computadoras que establecen la comunicación.

No debemos olvidar una cuestión fundamental en el diseño de Internet:

- **Los Router conectan redes, no hosts.**

Un "router" provee un camino de comunicación de modo que los datos puedan ser intercambiados entre las redes.

Para ello se vale de una unidad de datos (PDU) llamada datagrama o también paquete.

Un datagrama IP consta de una cabecera y un texto (datos). La cabecera tiene una parte fija de 20 bytes (5 palabras de 4 bytes cada una) y una opcional de longitud variable.

### Protocolo Internet (IP): entrega de datagramas sin conexión.

El Protocolo Internet (IP) provee el servicio básico de entrega de paquetes sobre la red. La capa "Internet" (capa "Red" del modelo OSI) está representada por el Protocolo Internet (RFC 791) y es el corazón del modelo TCP/IP. Todos los protocolos, superiores e inferiores a la capa Internet usan IP para la entrega de Datos. Todo el flujo de información pasa a través de la capa IP, tanto de entrada como de salida, sin considerar el destino final.

Técnicamente suele decirse que **el servicio IP es un servicio sin conexión y con el mejor esfuerzo (best effort)**. Este tipo de servicios se conoce también como **no confiable**, porque la entrega de los paquetes o datagramas **no está garantizada**.

Los paquetes se pueden:

- Perder
- Duplicar
- Retrasar
- Entregar sin orden

Pero el servicio IP no detectará estas condiciones ni informará al emisor o al receptor.

El servicio IP es llamado **sin conexión**, porque cada paquete es tratado de manera independiente de todos los demás; esto significa que una secuencia de paquetes, que se envían de una computadora a otra, pueden viajar por rutas diferentes; inclusive algunos de ellos pueden perderse mientras otros se entregan.

Se dice que el servicio IP trabaja con base en una **entrega con el mejor esfuerzo, porque el software de Internet hace un intento por entregar los paquetes**, es decir, que éstos no se descartan arbitrariamente.

## ¿Qué se pretende con el protocolo Internet?

Tres son las **ideas principales** que se pretenden del **protocolo IP** \* 13.1 :

- Primero: especificar el **formato exacto** de todos los datos que se transferirán a través de una red de redes TCP/IP.
- Segundo: el software IP debe realizar la **función de ruteo**, seleccionando la ruta por la que los datos serán enviados
- Tercero: debe definir la forma en que los *hosts* y los *routers* deben **procesar los paquetes**, cómo y cuándo se deben generar los **mensajes de error** y las condiciones bajo las cuales los paquetes pueden ser descartados.

## El Datagrama

TCP/IP fue construido para transmitir datos sobre una red de commutación de paquetes. Un paquete es un bloque de datos que transporta información necesaria para la entrega, en forma similar a la carta postal, la cual tiene direcciones, escritas en el sobre y un contenido.

Una red de commutación de paquetes usa el direccionamiento para commutar los paquetes de una red física a otra, moviéndolos en dirección al destino final. Cada paquete viaja por la red, independientemente de otro paquete.

La figura que se ve a continuación es una representación de un datagrama IP.



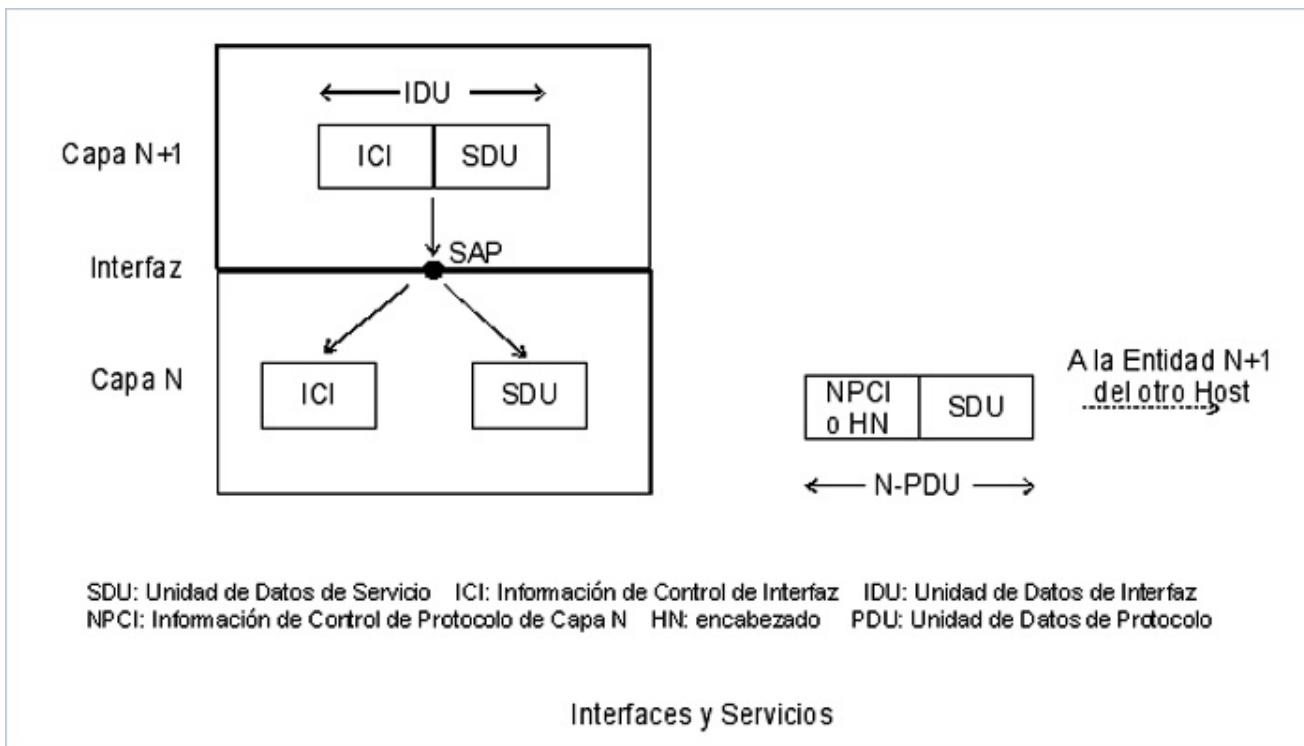
"El Datagrama" | *Elaboración autor*

El datagrama es un paquete de formato definido por el Protocolo Internet.

### Formato de un datagrama IP

Un datagrama IP, consta de un encabezado y un área de datos. En el encabezado, entre otras cosas, figuran las direcciones IP de origen y destino; en el área de datos se carga la información que, proveniente de las capas superiores, se desea transmitir.

Antes de que comencemos a ver con detalle cómo está conformado el datagrama IP, debemos relacionar lo mencionado anteriormente con respecto a las Interfaces y Servicios definidos en el modelo OSI, con nuestro caso real:

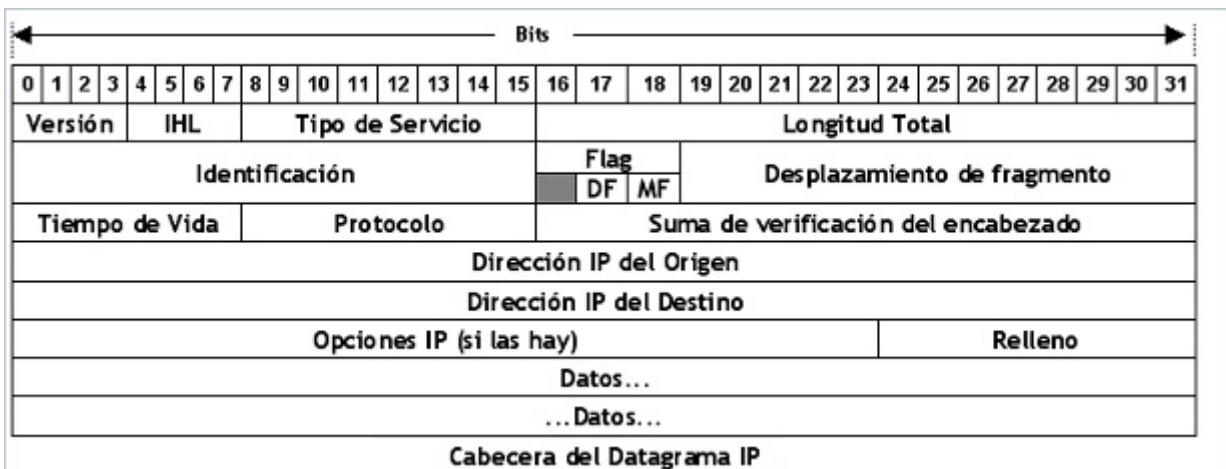


En este momento estamos analizando una situación similar en el caso específico del modelo TCP/IP.

La analogía es la siguiente:

- La capa N+1 es la que estamos estudiando en este capítulo, es decir la capa de red, donde "reside" IP.
- La capa N es la capa de acceso al medio.
- La SDU está conformada por el paquete IP (encabezado + área de datos)
- Una pequeña diferencia se da con respecto a la ICI, en el caso TCP/IP se incluye un campo de control, denominado ICMP (Protocolo de Mensajes de Control Internet) que se carga dentro del área de datos del paquete IP (luego lo analizaremos detalladamente).
- Por último, el HN consiste en la dirección de hardware (obtenido mediante el servicio ARP) del próximo destino del mensaje (que no tiene por qué ser el destino final, ya que puede ser la dirección de hardware correspondiente a un host que comenzará el ruteo).
- La SDU + la HN constituyen, por último, la PDU. (La trama)

Ahora sí, pasemos a analizar con más detalle, qué tiene un trama IP.



Las primeras cinco o seis palabras de 32 bit del datagrama son información de control llamada "encabezamiento" (header). Por defecto, la longitud del header es de cinco palabras, la sexta palabra es opcional. Debido a la longitud variable del encabezamiento, se incluye un campo llamado IHL (*Internet Header Length*), que indica la longitud en palabras del encabezamiento. El valor mínimo es 5.

El header contiene toda la información necesaria para la entrega del paquete.

El campo "Versión" indica a qué versión pertenece el datagrama (versión del protocolo IP, actualmente IPv4). La inclusión de la versión permite modificar los protocolos mientras la red está en operación.

El campo "Tipo de Servicio" le permite indicar a la subred el tipo de servicio que se desea. Es posible tener varias combinaciones con respecto a la seguridad y la velocidad. Por ejemplo, para voz digitalizada es más importante la entrega rápida que corregir errores de transmisión. En cambio, para la transferencia de archivos es a la inversa.

### Campo Tipo de Servicio (Type Of Service – TOS)

Este campo está subdividido en 4 subcampos:

8	9	10	11	12	13	14	15
Prioridad	D	T	R	Sin Uso			

"Campo Tipo de Servicio" | *Elaboración autor*

- Subcampo Prioridad: se pueden asignar 8 grados de prioridad, del valor 0 al valor 7, siendo el 0 el valor normal, subiendo la misma hasta el valor 7. Permite indicar a los Router la importancia de cada datagrama.

Los subcampos D, T y R, dan indicaciones con respecto a qué tipo de transporte se solicita a los Router. Cuando un router tiene más de una opción para direccionar el datagrama debe inspeccionar estos bits para decidir cuál debe ser el próximo salto.

- Subcampo D: cuando el bit D está activado (1), solicita un ruteo con retardos cortos.
- Subcampo T: cuando está activado solicita un alto desempeño (alta capacidad).

- Subcampo R: cuando está activado solicita confiabilidad.

La "Longitud Total" incluye la longitud total de todo el datagrama, tanto la cabecera como los datos. Obsérvese que éste es un campo de 16 bits, así que la longitud máxima de un datagrama IP (encabezado + datos) es de  $2^{16} = 65.536$  Bytes o sea 64KBytes.

El campo "Identificación" se necesita para permitir al destinatario saber a qué datagrama pertenece el fragmento que ha llegado. Todos los fragmentos de un datagrama tienen el mismo valor de identificación.

Luego viene un conjunto de tres bit, llamados "banderas" o "flag". El primer bit no se utiliza y después dos bit indicados como DF (Denial Fragment) que significa no fragmentar. Ésta es una orden para que los routers no fragmenten el datagrama.

El bit MF (More Fragment) significa más fragmentos. Todos los fragmentos con excepción del último deberán tener este bit en ON (1).

El "Desplazamiento del Fragmento" indica a qué parte del datagrama (número de fragmento) pertenece este fragmento. Esto en el caso de que se haya fragmentado un datagrama.

El campo "Tiempo de Vida" es un contador que se usa para limitar el tiempo de vida de los paquetes. En realidad no es un indicador de tiempo, sino de saltos. Cuando un paquete es enviado, se le agrega la cantidad de saltos para llegar a destino. Si el paquete, por razones de congestión o de caída de un enlace, comienza a viajar por la red, puede llegar a producirse un lazo (*loop*); para evitarlo, cuando este campo llega a cero, el paquete se descarta. Máximo 255 saltos.

El campo "Protocolo" indica a qué proceso de transporte pertenece el datagrama. Indica el tipo de Protocolo de Capa de Transporte utilizado. TCP es una posibilidad, pero existen otras.

El campo "Suma de verificación del encabezado" comprueba la exactitud de los datos sólo de la Cabecera.

Las Direcciones Fuente y destino indican el número de red y de Host, del origen y del destino respectivamente.

El Protocolo Internet entrega los paquetes chequeando la "Dirección Destino" (*Destinación Address*) indicado en la quinta palabra del encabezamiento. La Dirección destino es una dirección estándar de 32 bit, que identifica la red destino y el host específico dentro de la red. El formato de la dirección IP se explica más adelante.

Si la Dirección destino es una dirección de host sobre la red local, el paquete es entregado directamente al destino. Si la Dirección destino no está en la red local, el paquete es pasado al router para su entrega.

El router es un dispositivo que conmuta paquetes entre las diferentes redes físicas. La decisión de cual router usar es llamada "enrutamiento" (*routing*). IP toma la decisión de encaminamiento individualmente para cada paquete.

## Direccionamiento, Encaminamiento y Multiplexación

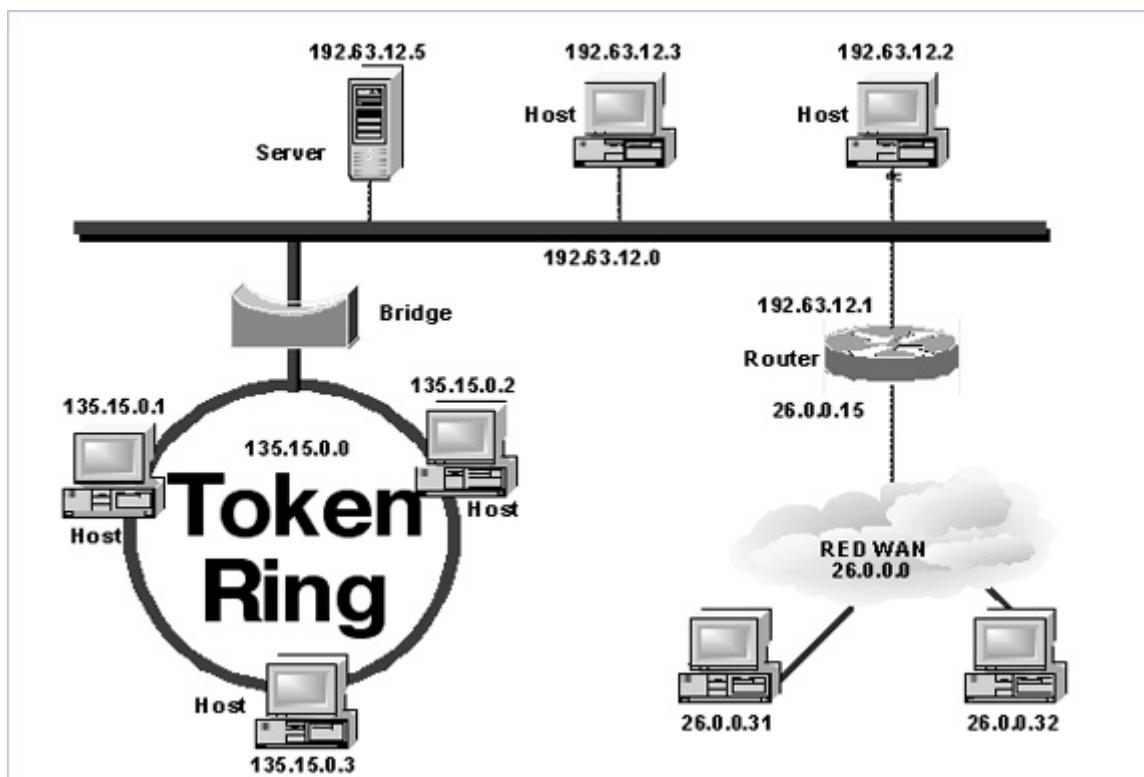
Para entregar datos entre dos host en Internet, es preciso mover esos datos a través de la red hacia el host destino y dentro de este host al proceso de usuario apropiado. TCP/IP usa tres esquemas para realizar esta tarea:

- Direccionamiento (*addressing*): las direcciones IP, las cuales identifican únicamente cada uno de los host en la Internet, entregan datos al host adecuado.
- Encaminamiento (*routing*): los router entregan datos a la red adecuada.
- Multiplexación (*multiplexing*): los protocolos y números de puertos entregan los datos al módulo de

software correcto dentro del host.

Cada una de estas funciones (direcciónamiento entre host, encaminamiento entre redes y multiplexación entre capas) son necesarias para enviar datos entre dos aplicaciones cooperativas a través de la Internet. Vamos a examinar cada una de estas funciones en detalles.

Para ilustrar estos conceptos y proveer un ejemplo consistente, vamos a usar una red corporativa. Una compañía imaginaria, que está formada por varias redes, en su planta de fabricación y oficina de ventas. La administración de la Ethernet es responsabilidad de un centro de computación. Esta estructura de red, o topología, se muestra en la siguiente figura:



Por supuesto que existen varios otros sistemas o redes, pero aquí apreciamos el uso de host únicos (workstation) y sistemas que sirven como router y bridges (puentes). La red Token Ring conecta varios host de la planta de producción. La nube representa una red WAN como la Internet. Qué indican los números, cómo son usados y cómo son entregados los datagramas es lo que vamos a ver a continuación.

# REFERENCIAS 13

## 13.1 : Protocolo IP

Una buena lectura sobre este tema la constituyen las siguientes RFC:

RFC 791  
RFC 1112  
RFC 894  
RFC 815

---



¡Vamos a comprobar cuánto aprendiste!

**1. Indique la opción correcta**

Una cuestión fundamental en el diseño de Internet es que los routers interconectan redes, no hosts.

- Verdadero
- Falso

**2. Indique la opción correcta**

Los paquetes se pueden:

- Perder.
- Retrasar.
- Entregar sin orden.
- Todas las anteriores.

**3. Indique la opción correcta**

El servicio IP es un servicio:

- Sin conexión.
- Con el mejor esfuerzo.
- No confiable.
- Todas las anteriores.

**4. Indique la opción correcta**

La idea principal del protocolo IP es:

- Especificar el formato exacto de todos los datos que se transferirán a través de una red de redes TCP/IP.
- El software IP debe realizar la función de ruteo, seleccionando la ruta por la que los datos serán enviados.
- Definir la forma en que los Host y los Routers deben procesar los paquetes, cómo y cuándo se deben generar los mensajes de error y las condiciones bajo las cuales los paquetes pueden ser descartados.
- Todas las anteriores.

**5. Indique la opción correcta**

Para entregar los datos en Internet, es preciso mover esos datos a través de la red hacia el host destino y dentro de este host al proceso de usuario apropiado. Para realizar esta tareas TCP/IP usa el siguiente esquema:

- Direcciónamiento (Addressing).
- Encaminamiento (Routing).
- Multiplexación (Multiplexing).
- Todas las anteriores.

**6. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Encabezamiento	Define Velocidad y Seguridad
Versión	Contiene cinco o seis palabras de 32 bits del datagrama
Tipo de servicio	Incluye todo el datagrama, tanto la cabecera como los datos
Longitud total	Define si es IPV4 O IPV6

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Una cuestión fundamental en el diseño de Internet es que los routers interconectan redes, no hosts.

Verdadero

Falso

## 2. Indique la opción correcta

Los paquetes se pueden:

Perder.

Retrasar.

Entregar sin orden.

Todas las anteriores.

## 3. Indique la opción correcta

El servicio IP es un servicio:

Sin conexión.

Con el mejor esfuerzo.

No confiable.

Todas las anteriores.

## 4. Indique la opción correcta

La idea principal del protocolo IP es:

Especificar el formato exacto de todos los datos que se transferirán a través de una red de redes TCP/IP.

El software IP debe realizar la función de ruteo, seleccionando la ruta por la que los datos serán enviados.

Definir la forma en que los Host y los Routers deben procesar los paquetes, cómo y cuándo se deben generar los mensajes de error y las condiciones bajo las cuales los paquetes pueden ser descartados.

Todas las anteriores.

## 5. Indique la opción correcta

Para entregar los datos en Internet, es preciso mover esos datos a través de la red hacia el host destino y dentro de este host al proceso de usuario apropiado. Para realizar esta tarea TCP/IP usa el siguiente esquema:

Direccionamiento (Addressing).

Encaminamiento (Routing).

Multiplexación (Multiplexing).

Todas las anteriores.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Encabezamiento	Contiene cinco o seis palabras de 32 bits del datagrama
Versión	Define si es IPV4 O IPV6
Tipo de servicio	Define Velocidad y Seguridad
Longitud total	Incluye todo el datagrama, tanto la cabecera como los datos

## SP8 / H2: Direcciones IP

Uno de los objetivos principales de TCP/IP es hacer transparente, a los usuarios de la capa física de conexión entre redes; un elemento fundamental para poder conseguirlo es la asignación de direcciones IP.

El punto principal a entender con respecto a las direcciones de IP es que las mismas no se otorgan a los dispositivos, como por ejemplo host, sino que se asignan a las conexiones que tienen los mismos. Esto provoca que un mismo dispositivo pueda tener más de una dirección de IP.

Considere por caso un *router*: por lo menos tiene dos conexiones, así que por lo menos tiene dos direcciones de IP, de la misma forma que una computadora que esté conectada a dos redes tendrá también dos direcciones de IP.

*En Internet existe una dirección IP por cada conexión. Cada dispositivo (host, router) tendrá tantas direcciones IP como cantidad de redes a las que se encuentre conectado* \* 14.1.

### Esquema general de las direcciones IP

El Protocolo Internet (IP) mueve datos entre host en la forma de datagramas. Cada datagrama es entregado a la dirección contenida en la "Dirección Destino" (palabra 5) del encabezado del Datagrama. La Dirección Destino es un estándar de 32 bit que contiene suficiente información que identifica una red y un host específico dentro de la red.

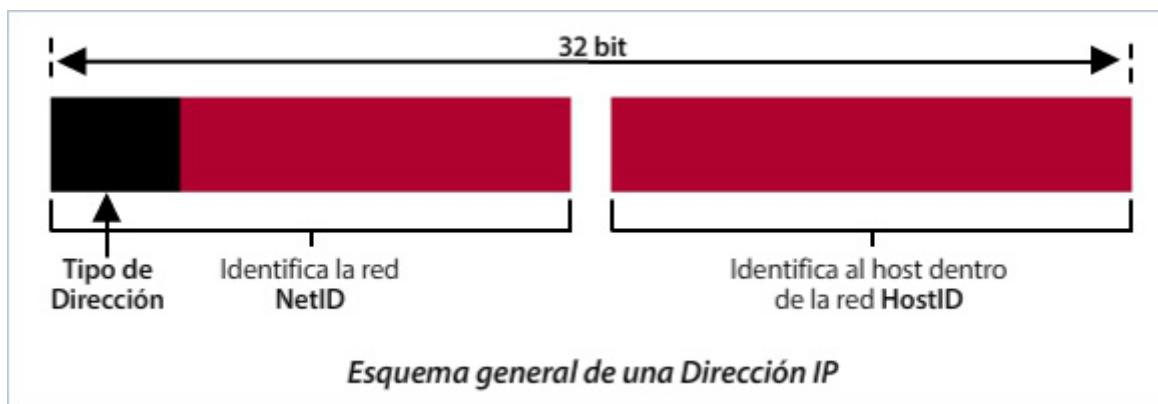
Una dirección IP contiene una "parte de red", (Net-ID) y una "parte de host", (Host-ID), pero el formato de esas partes no es el mismo en cada dirección IP. El número de bits usado para identificar el host, varía de acuerdo a la "clase" de dirección.

Examinando los primeros bits de la dirección, el software IP puede determinar fácilmente la "clase", por lo tanto, su estructura.

Existen cinco tipos distintos de direcciones IP; sin embargo, todas ellas comparten algunas características:

- Todas están compuestas de 32 bits
- Están compuestas por tres partes:
  - Identificador del tipo de dirección
  - Identificador de la red (NetID)
  - Identificador del Host dentro de la red (HostID)

La siguiente figura esquematiza lo dicho:



"Esquema general de una dirección IP" | *Esquema general de las direcciones IP*

Como puede verse, haciendo abstracción del hecho de que la primera parte de la dirección corresponde al tipo de dirección, los 32 bits se utilizan en una parte para identificar la red, y el resto para identificar el Host dentro de esa red. Esto justifica el hecho de que las direcciones IP identifican direcciones de enlaces o conexiones de host a redes.

¿Por qué será así, y no, por ejemplo, utilizar los 32 bits para identificar a cada uno de los host en el mundo?

Si fuera así tendríamos la cantidad de:

$$2^{32} = 4.294.967.296 \text{ Direcciones distintas}$$

La respuesta es bastante obvia si se tiene en cuenta la forma en que se envían los datos de un host a otro: la palabra clave es "enrutamiento".

Al estar dividida la dirección IP correspondiente a un host en dos partes: la primera correspondiente a la red y la segunda correspondiente a él dentro de la red, hace posible que para el enrutamiento no sea necesario utilizar todos los bits, ya que sólo será fundamental utilizar los bits correspondientes a la identificación de la red (compuesto por el tipo de dirección y el NetID); al usar menos bits la cuestión se simplifica y se puede hacer más velozmente.

Tenga en cuenta también que si un host (computadora), está conectado a más una red, tendrá necesariamente más de una dirección IP, y al enviarse los paquetes con datos a través de direcciones distintas, serán enrutados de distinta forma.

## Las 5 Clases de Direcciones IP

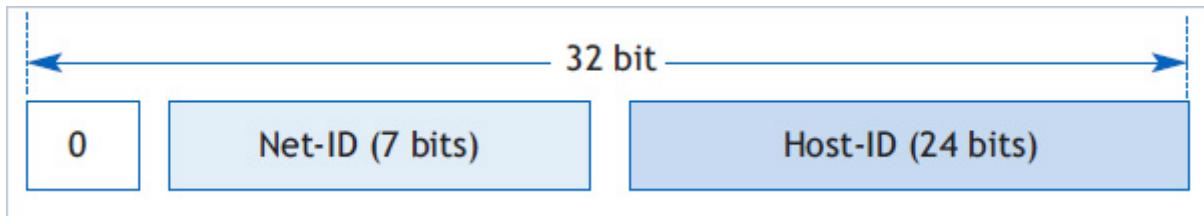
Existen cinco tipos de direcciones IP, cada una denotada con una letra: A, B, C, D, E. Las tres primeras se denominan primarias, y son las utilizadas actualmente para dar direcciones.

Las direcciones tipo D sirven para lo que se denomina multidifusión, y las tipo E están reservadas para uso futuro.

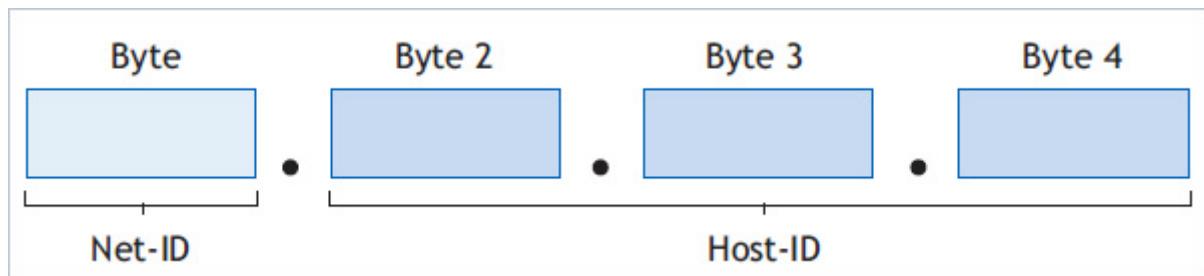
Las siguientes reglas determinan la clase de dirección:

- **CLASE A**

Si el primer bit de la dirección IP es 0 (cero), ésta identifica una "Red clase A". Los próximos 7 bits identifican el número de red y los últimos 24 bits identifican el Host. Hay menos de 128 números de redes Clase A, pero cada red Clase A puede estar compuesta de millones de host.

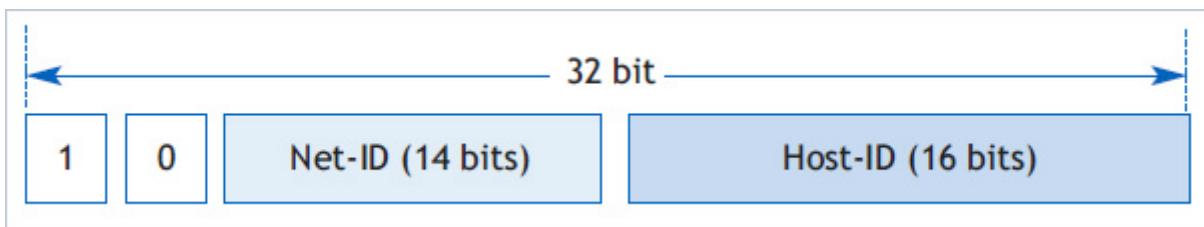


La clase A se divide en 1 byte u octeto para la red y 3 bytes u octetos para el host.

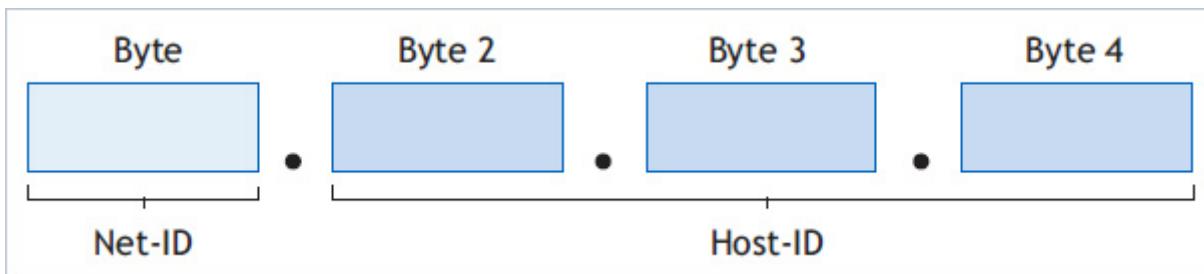


- **CLASE B**

Si los dos primeros bit de la dirección son **10**, esta es una "Red clase B". Los primeros dos bit identifican la clase, los próximos 14 bit identifican el número de red y los últimos 16 bits identifican el host. Hay miles de números de redes y cada red clase B puede contener miles de host.

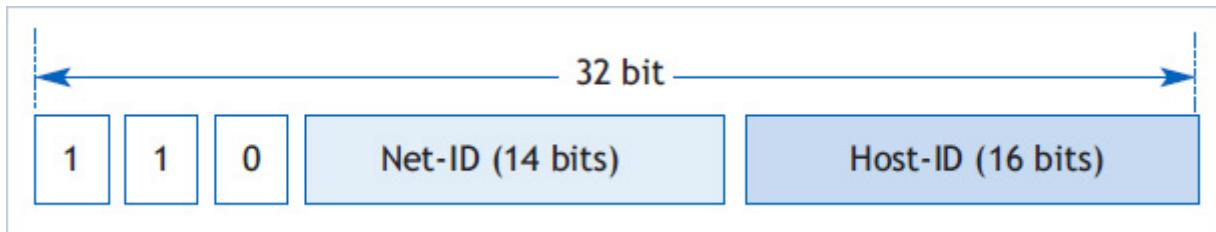


La clase B se divide en 2 bytes para la red y 2 bytes para el host.

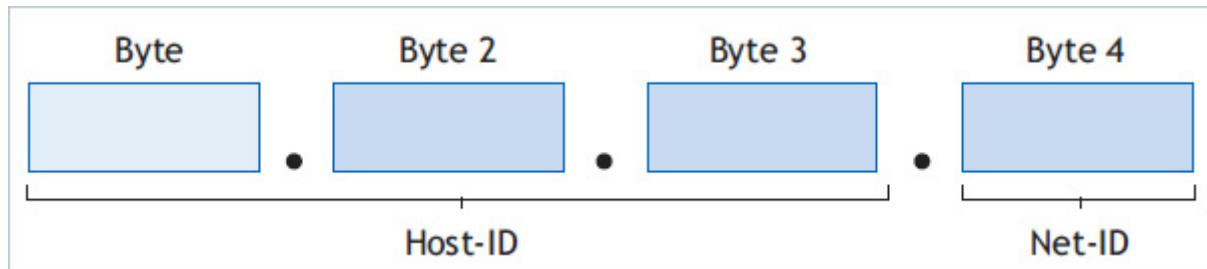


- **CLASE C**

Si los tres primeros bits de la dirección son **110**, es una dirección de "Red clase C". Los primeros tres bits identifican la clase, los próximos 21 bits identifican el número de red y los últimos 8 bits identifican el host. Hay millones de redes clase C, pero cada red está compuesta por menos de 254 host.

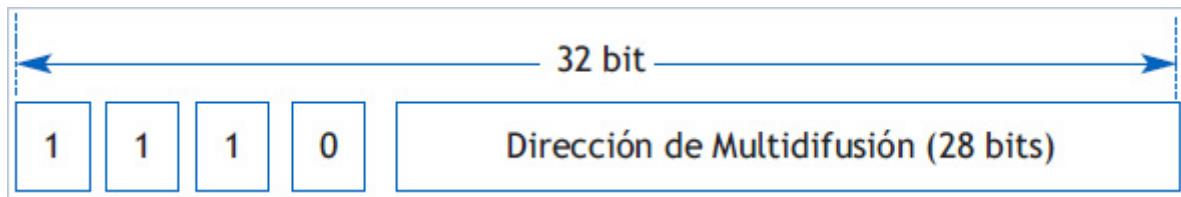


La clase C se divide en 3 bytes para la red y 1 bytes para el host.



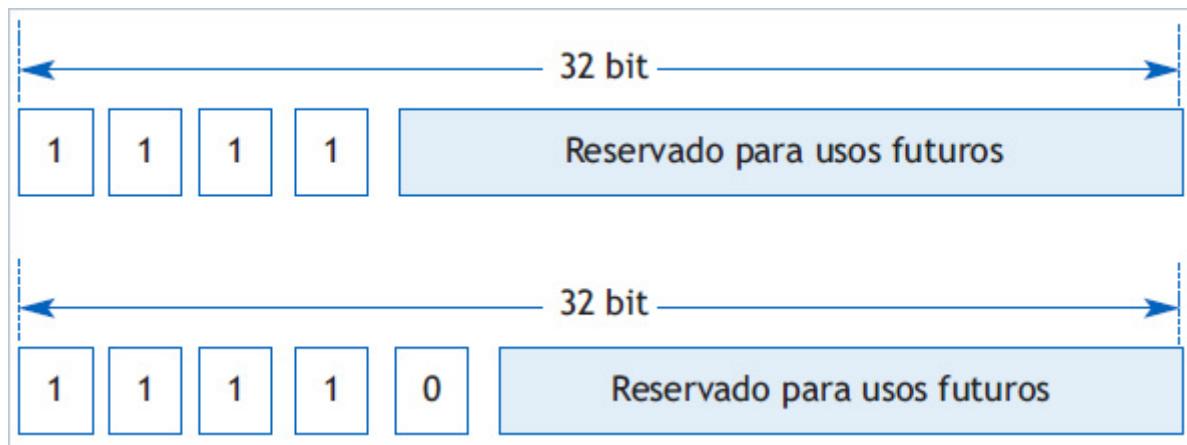
#### • CLASE D

Si los cuatro primeros bits de la dirección son **1 1 1 0**, es una dirección de "Red clase D". Los primeros cuatro bits identifican la clase. No existe separación de Red-ID ni de Host-ID. Cuando un router, al leer la dirección IP, se encuentre con los tres primeros bit en **1 1 1**, sabe que es una dirección especial. Éstas son direcciones, no están referidas específicamente a una red, sino que indican una dirección múltiple. Las **direcciones múltiples** \*14.2 son usadas para direccionar un grupo de computadoras al mismo tiempo (multicast o broadcast limitado).



#### • CLASE E

Si los cuatro primeros bits de la dirección son **1 1 1 1**, o si los cinco primeros bits son **1 1 1 1 0** es una dirección de "**Red clase E**" \*14.3 Los primeros tres bits identifican la clase, los próximos 21 bits identifican el número de red y los últimos 8 bits identifican el host. Hay millones de redes clase C, pero cada red está compuesta por menos de 254 host.



## Las direcciones IP primarias

Como ya dijimos antes, las tres primeras Clases A, B y C, se denominan primarias, y son las utilizadas en la actualidad para dar direcciones a host.

Obsérvese que las direcciones tipo A están pensadas para esas pocas redes que pueden albergar hasta unos 16 millones de host; las tipo B -en cambio- son un tanto más masivas: están pensadas para aquellas redes que pueden tener que entre 256 y 65.536 hosts; por último, las tipo C están pensadas para aquellas redes pequeñas de hasta 256 computadoras conectadas.

Clase	Cantidad de host	Cantidad de redes
A	De $2^{16}$ (65.536) a $2^{24}$ (16,7 millones)	$2^7$ (128)
B	Entre $2^8$ (256) y $2^{14}$ (65.536)	$2^{14}$ (16.384 )
C	Menos de (256)	$2^{21}$ (2.097.152)

Tabla 1

## Cómputo de la clase o tipo de una dirección IP

Cuando un router recibe un paquete, debe identificar la dirección destino, para así poder remitirlo correctamente; a partir de la figura anterior se puede confeccionar la siguiente tabla para diferenciar a qué clase corresponde la dirección especificada.

Para distinguir la clase a la que pertenece una dirección, se utilizan los 4 primeros bits, con los cuales es posible configurar una Tabla indexada como la siguiente:

Índice	Primeros 4 bits de la dirección	Clase
0	0000	A
1	0001	A
2	0010	A
3	0011	A
4	0100	A
5	0101	A
6	0110	A
7	0111	A
8	1000	B
9	1001	B
10	1010	B
11	1011	B
12	1100	C
13	1101	C
14	1110	D
15	1111	E

Tabla 2

## Notación decimal con puntos

Las direcciones IP están constituidas por 32 bits, lo cual las hace bastante incómodas para ser manejadas por los seres humanos; es por eso que se instrumentó una notación más sencilla, la denominada notación decimal con puntos.

Afortunadamente, esto no es tan complicado como parece. La dirección [\\* 14.4](#) IP es usualmente escrita como cuatro números decimales separados por un "punto".

En este caso, se dividen los 32 bits en 4 grupos de 1 Byte, a cada uno de ellos se le calcula su equivalente en notación decimal, y cada uno se separa con un punto.

Cada uno de los cuatro números está en el rango de 0 - [\\* 14.5](#). El máximo valor que puede tener cada uno de los números decimales es 255, que corresponde al Byte **11111111**, es decir, que por ejemplo: **123.345.112.8** no es una dirección IP, ya que el 345 es imposible en este contexto.

A causa de que el bit que identifica la clase es contiguo con los bits de dirección de red, se puede reunir los trozos y ver cómo están compuestos todos los bytes de la dirección de red y de host.

## Extensión de las direcciones para las clases D y E

La Clase D se extiende desde **224.0.0.0** hasta **239.255.255.255**.

La clase E depende de cómo tomemos los bits.

Si consideramos 5 bit **1 1 1 1 0**, se extiende desde la **240.0.0.0** hasta **247.255.255.255**.

Si consideramos 4 bit **1 1 1 1**, se extiende desde la **240.0.0.0** hasta **255.255.255.255**.

Para facilitar la visualización y memorización puede valerse de la Tabla 3:

Gama de valores para el primer número decimal	Clase
De 0 a 127	A
De 128 a 191	B
De 192 a 223	C
De 224 a 239	D
De 240 a 255	E

Tabla 3

## Direcciones especiales o reservadas

Sin embargo algunas direcciones están reservadas para propósitos especiales, con lo cual en la realidad la asignación es la siguiente:

Tipo de dirección	desde	hasta
A	0.1.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.1.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

Tabla 4

## Los casos especiales:

Existen algunos casos de direcciones IP que se consideran a continuación:

- Dirección IP de una red,
- Difusión dirigida,
- Difusión limitada,
- Dirección de "este host"
- *Loopback*
- **Dirección IP de una red**

Como ya dijimos, no todas las direcciones de red o de host están disponibles para usar. En la clase A existen dos direcciones reservadas para usos especiales. La red 0 designa la "*default route*" y la 127 "*loopback address*". La "*default route*" es usada para simplificar la información de "*routing*" (enrutamiento) que puede manejar el IP.

La *loopback address* simplifica la aplicación de red para permitir direccionar al host local de la misma manera que el host remoto. Se usa esta dirección de red especial cuando configuramos un host.

También en las direcciones de todas las clases de red, los números de host 0 y 255 están reservados. Una dirección IP con todos los bits de host en cero identifica la red.

La dirección de Host con todos los bits en uno corresponde a una dirección de "broadcast". La dirección broadcast es usada como dirección simultánea de todos los host de la red. Por ejemplo, la dirección de broadcast para la red Clase B "128.66" es "128.66.255.255". Un datagrama enviado a esta dirección es entregado a todos los host de la red "128.66".

Las direcciones IP son a menudo llamadas direcciones de host. Mientras esto es de uso común, es un poco engañoso. Las direcciones IP son asignadas a las interfaces de red, no a los sistemas de computación. Un router, tiene diferentes direcciones para cada red a la cual está conectado. El router es conocido para otros dispositivos por la dirección asociada con la red que este comparte con aquellos dispositivos.

IP usa la porción de red para encaminar los paquetes entre las redes. La dirección completa, incluyendo la información del host, es usada para hacer la entrega definitiva cuando el datagrama alcanza la red destino.

Por regla general nunca se asigna el campo HostID igual a 0 (todos los bits del HostID iguales a 0) a un host determinado, sino que se guarda dicha alternativa para referirse a la red en sí, esto permite que mediante las direcciones IP no sólo sea posible direccionar hosts dentro de redes, sino que también es posible asignar direcciones a las redes mismas.

Por ejemplo:

**123.0.0.0** es la dirección IP de una red de tipo A y

**123.42.0.72** se refiere a un host conectado a dicha red

de la misma forma:

**201.123.47.0**

es la dirección de una red tipo C.

Observe que en este caso los 3 primeros decimales se utilizan para determinar el tipo de dirección y el NetID, quedando sólo el último decimal para el HostID

**201.123.47.111** es la dirección de un host dentro de dicha red.

- **Difusión dirigida**

Otro caso especial de direcciones IP está pensado para poder difundir un mismo mensaje a todos los hosts de una misma red. En este caso se utiliza la asignación de valores todos 1 en el campo HostID (es decir todos los bits del campo HostID valen 1; tenga cuidado de no confundir la frase "que todos los bits valgan 1" con el decimal **111**. Para aclarar más: todos los bits iguales a 1 se corresponden en notación decimal con el 255).

Por ejemplo:

**180.43.0.0** se refiere a una red clase B (ya que los dos últimos Bytes que son los que corresponden al HostID son todos 0),

**180.43.111.111** se refiere a un host conectado a dicha red y

**180.43.255.255** hace referencia a todos los hosts conectados a dicha red. (Broadcast)

Es de notar que una dirección de este tipo nunca será tomada como una **dirección válida de origen**. \* 14.6

- **Difusión limitada**

Se refiere a un mensaje que se debe difundir sólo en la red a la cual pertenece el Host que lo emite, es decir no saldrá de la red local.

Esta dirección está asignada con todos sus bits en 1 (es decir 32 unos, o lo que es lo mismo en la notación

decimal con puntos: **255.255.255.255**).

Este tipo de difusión es utilizado habitualmente por un host en el momento del arranque, cuando aún no "sabe" cuál es su dirección de red, luego veremos cómo.

Al igual que la anterior, esta dirección nunca es válida como dirección de origen.

- **Dirección "este host"**

Es habitual que cuando arranca una computadora no conozca su dirección IP, en ese caso puede utilizar temporalmente la dirección asignada por todos los bits iguales a 0.

Esta dirección sólo es válida en la situación antes descripta, es decir en el arranque de la computadora y nunca es válida como dirección de destino.

- **Loopback (retrociclo)**

Como ya vimos anteriormente, la dirección 127 está reservada como dirección de "**loopback**" \*14.7. Si bien la dirección de loopback permite cualquier valor para los tres bytes de host, se suele utilizar el valor:

#### **127.0.0.1 como dirección de "loopback"**

La "**loopack address**" simplifica la aplicación de red para permitir direccionar al host local de la misma manera que el host remoto. Se usa esta dirección de red especial cuando configuramos un host.

NetID	HostID	Tipo	Objetivo	Notas
Todos los bits en 0	Todos los bits en 0	"esta computadora"	Se usa durante el arranque	
Dirección de red	Todos los bits en 0	red	Identificar una red	
Dirección de red	Todos los bits en 1	Difusión dirigida	Difusión dirigida a todos los hosts de otra red	No es válida como dirección de origen
Todos los bits en 1	Todos los bits en 1	Difusión limitada	Difusión en la red local	No es válida como dirección de origen
Primer Byte = 127	Cualquier cadena (habitualmente 127.0.0.1)	Loopback	pruebas	Nunca debe ser asignada en una red.

## **Direcciones IP privadas**

Otro enfoque de la conservación del espacio de direcciones IP se describe en el RFC 1597 - Distribución de direcciones para redes privadas. En pocas palabras, relaja la regla de que las direcciones IP han de ser únicas globalmente al reservar parte del espacio de direcciones para redes que se usan exclusivamente dentro de una sola organización y que no requieren conectividad IP con Internet. Hay tres rangos de direcciones que IANA ha reservado con este propósito:

Red	Rango	
	DESDE	HASTA
CLASE A	10.0.0.0	10.255.255.255
CLASE B	172.16.0.0	172.31.255.255
CLASE C	192.168.0.0	192.168.255.255

**10.255.255.255** \* 14.8

Cualquier organización puede usar estas direcciones en su red interna. Debido a que estas direcciones no son únicas a nivel global, no pueden ser direccionadas a host de otras organizaciones y por consiguiente no están definidas para los "router" externos.

Se supone que los "router" de una red que no usa direcciones privadas, particularmente aquellos operados por proveedores de servicios de Internet, han de desechar toda información de encaminamiento relativa a estas direcciones. Los "router" de una organización que utiliza direcciones privadas deberían limitar todas las referencias a direcciones privadas a los enlaces internos; no deberían hacer públicas las rutas a direcciones privadas ni enviar datagramas IP con estar direcciones a los "router" externos.

Los host que tienen una dirección IP privada carecen de conexión a Internet en forma directa. Esto, a veces es deseable por razones de seguridad. Toda la conectividad con host externos de Internet la deben proporcionar gateways o proxys.

## Resolución de direcciones lógicas IP en direcciones físicas

El protocolo IP brinda una gran transparencia a las aplicaciones de la capa superior: mientras la aplicación conozca su propia dirección IP, y la dirección IP del destino, sabe que puede establecer una comunicación. También brinda una gran capacidad de enrutamiento: conociendo el NetID del destino, cualquier Router puede determinar hacia dónde debe enviar el mensaje, de tal forma que en una cantidad finita de saltos, el mismo llegue a la red a la cual pertenece el host destino.

Sin embargo, a nivel de capas inferiores, de capas de hardware, las direcciones IP no tienen sentido: a nivel físico, cada host tiene una dirección de hardware, también conocida como dirección **MAC** \* 14.9 (MAC address) la cual depende de la tecnología y los protocolos de la red LAN a la que se encuentre conectado (Ethernet, Token Ring, etc.), y es mediante estas direcciones de hardware que se produce la comunicación real.

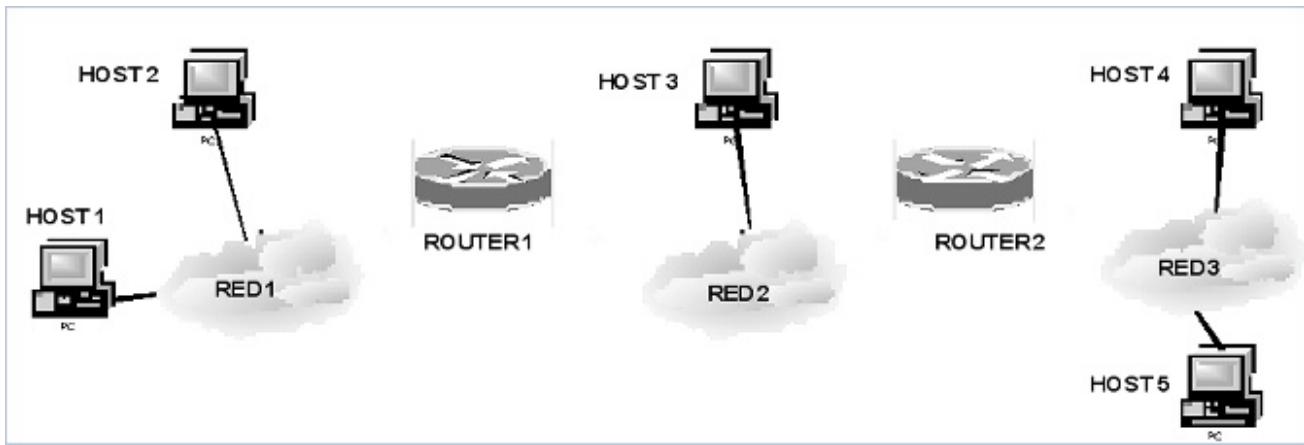
Como puede imaginar, esto trae un problema: en algún lugar "alguien" debe traducir las direcciones IP en direcciones de *hardware*, o direcciones MAC.

Con respecto a la terminología diremos que al proceso de traducir la dirección IP en una dirección de hardware se lo denomina "Resolución de Dirección".

### Resolución de direcciones

La resolución de direcciones sólo se produce dentro de una red local.

Un *host* puede resolver la dirección de otro sólo si ambos se encuentran conectados a la misma red; un host nunca resuelve la dirección de otro ubicado en una red remota. Quien resuelve una dirección MAC a partir de una IP en una red remota es el router, a través de un mecanismo conocido como Proxy ARP.



"Conexión a la misma red física" | Un host solamente puede resolver la dirección de otro sólo si ambos se encuentran conectados a la misma red física.

**Tomemos como ejemplo la configuración de la figura.** Supongamos que el host 1 desea enviar un mensaje al host 2, del cual conoce su dirección IP. Lo primero que hace es observar mediante el NetID, que el host 2 pertenece a la misma red, entonces pregunta a todos los host de esa red (*broadcast*) para que el que tenga la NetID en cuestión, responda cuál es su dirección física o MAC. De esta manera resuelve la dirección (es decir, encuentra la dirección de hardware de la máquina cuya dirección IP se conoció), y envía el mensaje.

Ahora supongamos que el host 1 desea enviar un mensaje al host 5, del cual conoce su dirección IP. Ningún host de la red 1 responde a la pregunta, ya que ninguno tiene esa dirección IP, dado que ésta no pertenece a la red 1 sino a la red 5. En este caso, el router es quien responde con su propia dirección MAC; entonces el Host 1 le envía la trama al router, el cual se encarga de enviarlo (luego de averiguar la NetID de destino) a la red 3. El router sabe que la red 3 es accesible a través de la red 2 y del router 2. De esta forma se resuelve la dirección física a partir de la dirección lógica o NetID. Este procedimiento se conoce como Proxy ARP.

Observe que no resuelve la dirección del Host 5, en su lugar resuelve la dirección del Router 1, que inspecciona la dirección IP de destino, y decide reenviar ese paquete hacia el Router 2. Éste se da cuenta de que el mensaje va dirigido a un host de la red 3 (ya que observa su NetID), entonces sí resuelve la dirección de hardware del host 5 y envía el mensaje.

### ¿Qué es una dirección de hardware?

Con lo visto en las herramientas anteriores, tenemos una idea de qué es una dirección IP, pero ¿qué es una dirección de hardware?

La dirección de hardware reside físicamente en la interfaz de red (es decir, en la placa de red o NIC); en algunos casos, esta dirección no se puede modificar; en otros casos, el administrador de red puede decidir cuál es la dirección de cada placa, como ya vimos en la situación profesional 4.

Existen tres tipos de resolución de direcciones:

- Resolución directa
- Resolución mediante búsqueda en tabla
- Resolución mediante enlace dinámico
- **Resolución directa.**

Ejemplificaremos este tipo de resolución con el caso más sencillo: el de las redes tipo Token Ring.

Como mencionamos antes, en este caso, el administrador de red puede asignar los números correspondientes a la dirección de cada una de las placas de red, ya que cuenta con la posibilidad de hacerlo sobre la misma placa.

No olvidemos que también es prerrogativa del administrador de red asignar el HostID de la dirección IP de cada host (lo que no puede cambiar es el NetID, que lo designa una autoridad competente, la InterNic). Obviamente, si puede decidir tanto el valor del HostID como el de la dirección de hardware de cada placa de red, lo más lógico es que designe el mismo valor en ambos.

Supongamos, por ejemplo, un administrador de una red LAN tipo C, cuya dirección es 200.80.44.0.

Al primer host podría asignarle la dirección IP 200.80.44.1, y asignar como dirección de hardware en la placa simplemente el 1. Al siguiente host le asignaría la dirección IP 200.80.44.2, y, obviamente, la dirección de hardware sería el 2.

Observe que de esta forma ni siquiera sería necesario armar una tabla o base de datos con la correspondencia entre ambas, ya que una simple operación de producto lógico resolvería problema; por ejemplo ¿cómo encontraría la dirección de hardware del segundo host mediante la operación de producto lógico?

La dirección IP 200.80.44.2, escrita en bits es la siguiente:

	1er Byte	2do Byte	3er Byte	4to Byte
Notación decimal	200	80	44	2
Notación en bits	xxxxxxxx	xxxxxxxx	xxxxxxxx	00000010

Se han indicado con x los bits correspondientes a los 3 primeros Bytes, ya que en realidad su valor es irrelevante, sólo nos interesarán los bits del último Byte.

Efectuamos la operación AND o producto lógico de la dirección IP con una cadena de 32 bits, donde los primeros 24 bits son ceros y los últimos 8 son unos:

Dirección IP	xxxxxxxx	xxxxxxxx	xxxxxxxx	00000010
Operando	00000000	00000000	00000000	11111111
Resultado de AND	00000000	00000000	00000000	00000010

Observe que el resultado de la operación es sencillamente el número 2, el cual se corresponde con la dirección de hardware asignada.

Nótese que es más rápido realizar una operación AND de este tipo que una búsqueda en una Tabla indexada, por lo cual no se implementa dicha tabla (las operaciones lógicas a nivel bit son de las más veloces en los procesadores actuales). Dado que en este tipo de **resolución de direcciones** se utilizan operaciones, también suelen llamarse: "Resolución de dirección con cálculo de forma cerrada".

Note, por último, que nada impediría al administrador de red utilizar operaciones más complejas, como por ejemplo realizar un producto lógico y luego una suma lógica con un valor determinado, por ejemplo el uno; claro que en ese caso el resultado del ejemplo habría sido 3, valor que se debería haber asignado inicialmente a la dirección de hardware.

Lamentablemente, el caso general no es una resolución en forma directa ya que en general las redes más utilizadas son las de tipo Ethernet, las cuales -como mencionamos anteriormente- tienen un número identificatorio de 48 bits para cada placa que se fabrique en el mundo y el administrador de red no puede cambiar esta secuencia a su gusto.

- **Resolución de direcciones con búsqueda en tabla**

En este caso, la idea es establecer una relación entre las direcciones IP de cada host y su dirección de *hardware*, por ejemplo, utilizando dos campos o columnas: uno correspondiente a la dirección de IP y el otro, a la dirección de hardware. Quizá la mejor solución es usar el HostID de la dirección de IP como índice de la tabla.

Antes de ver un ejemplo, no nos olvidemos que en este caso la dirección de hardware no es modificable, pero siempre es prerrogativa del administrador de red asignar a la dirección del HostID. Tomemos por caso una red Ethernet, de la cual ya hemos comentado que sus direcciones consisten en 48 bits. La norma correspondiente indica que es preferible escribir las direcciones Ethernet en nomenclatura hexadecimal.

Tomemos por ejemplo, la misma red del caso anterior, pero ahora dispuesta en red Ethernet:

**Red Tipo C**

**IP de la red: 200.80.44.0**

Supongamos que las siguientes son las direcciones Ethernet de los hosts de esta red:

Dirección de hardware Ethernet (en hexadecimal)
0A : 02 : 3B : 1C: 85 : A4
0A : 9B : C8 : CB : 01 : 1F
0A : 00 : 8D : 97 : 14 : A0

Estas direcciones de hardware podrían relacionarse con las direcciones IP asignadas por el administrador de red de la siguiente forma:

Dirección IP	Dirección de hardware Ethernet
200.80.44.2	0A : 02 : 3B : 1C: 85 : A4
200.80.44.3	0A : 9B : C8 : CB : 01 : 1F
200.80.44.4	0A : 00 : 8D : 97 : 14 : A0

Obsérvese que el NetID de cada una de las direcciones IP necesariamente debe ser el mismo, y por lo tanto ofrece información redundante para la tabla. Podría utilizarse para indexar la misma sólo el HostID, en cuyo caso la tabla quedaría:

índice	Dirección de hardware Ethernet
2	0A : 02 : 3B : 1C : 85 : A4
3	0A : 9B : C8 : CB : 01 : 1F
4	0A : 00 : 8D : 97 : 14 : A0

¿Cómo relacionamos la dirección IP con el índice de la Tabla para poder ingresar en ella para encontrar la dirección de hardware?

Siguiendo el mismo procedimiento que en el caso de la Resolución Directa: haciendo una operación lógica AND con los bits de los 3 primeros Bytes todos 0 y los del último todos 1. Ya habíamos observado que esto daba como resultado la repetición de la secuencia de bits correspondiente al HostID. Luego, con este valor, es posible ingresar a la tabla, usándolo como índice de la misma.

- **Resolución mediante enlace dinámico**

En los dos casos de resolución de direcciones comentados anteriormente es necesario que exista uno u varios servidores que provean la resolución de la dirección.

Supongamos que el *host 1* desea enviar un mensaje al *host 2*, del cual conoce su dirección IP. Primero observa el NetID de la dirección IP del *host 2*, una vez que ha determinado que pertenece a la misma red se da cuenta que está en condiciones de establecer la comunicación, para lo cual necesita conocer la dirección de hardware del *host 2*.

En los casos hasta ahora estudiados es preciso que haya una autoridad centralizada que realice los cálculos correspondientes en la resolución directa, o mantenga actualizada la tabla en el caso de resolución por tabla. Esta tarea habitualmente recae en uno o varios servidores. Entonces, continuando con el ejemplo, el *host 1* solicita al servidor que le dé la dirección de hardware del *host 2*, éste se la envía y, a partir de allí, está en condiciones de enviarle mensajes al *host 2*.

En redes grandes, con muchas computadoras conectadas, esta tarea puede ser bastante pesada, siendo quizás los servidores un elemento que haga más lenta la transmisión en la red. Por otro lado, no es de extrañar que muchas veces se produzcan errores en las tablas de asignación, por ejemplo, cuando se rompe una placa de red de un *host* y hay que cambiarla por otra que obviamente tendrá otra dirección de hardware.

Una alternativa a todo esto es la resolución mediante enlace dinámico. Cuando el *host 1* necesita conocer la dirección de hardware del *host 2*, difunde un mensaje en toda la red, que puede ser como el siguiente:

"Si IP 2 es tu dirección de IP, envíame tu dirección de hardware H2, te envío mi dirección de hardware H1".

Si bien el mensaje es difundido en toda la red local, lo cual significa que es recibido y procesado por todas las computadoras, solamente el *host 2* responderá. A partir de este momento, como el *host 1* ya conocerá la dirección de hardware del *host 2*, podrá enviarle el mensaje original.

En este momento deberíamos plantearnos una pregunta: ¿por qué el *host 1* no difunde un mensaje como el siguiente?:

"Si tu dirección IP es IP 2, este mensaje es para vos"

Y le envía directamente el mensaje.

Observe que con este esquema de difusión del mensaje sería innecesario realizar los intercambios previos para que el host 1 conozca la dirección de hardware del host 2, es más, sería también innecesario que alguien mantuviera una tabla donde se relacionen las direcciones IP con las de hardware.

El problema radica en la difusión: éste es un proceso muy "caro" para la red, ya que todas las computadoras deben procesar parte del mensaje para determinar si le corresponde a ella, y con el procedimiento propuesto, cada mensaje sería difundido, ya que no se llevarían tablas.

Este problema obliga a que cada host mantenga en memoria intermedia (memoria caché) una pequeña tabla donde consten las asociaciones de las direcciones IP y las direcciones de hardware que ha ido averiguando en los últimos tiempos.

## ARP -Protocolo de Resolución de Direcciones \* 14.10

TCP/IP puede utilizar cualquiera de los tres métodos de resolución de direcciones explicados anteriormente; en realidad el uso de cada uno de ellos depende del esquema de direccionamiento del *hardware* de red; en general, la búsqueda en tabla se utiliza para resolver direcciones IP en una WAN, el cálculo en forma cerrada en las redes que son configurables y el intercambio dinámico se utiliza en aquellas redes que no permiten un direccionamiento configurable (direcciones estáticas de hardware).

Dado que en cualquiera de los casos hay un flujo de mensajes a través de la red, es necesario establecer un protocolo que permita reconocer exactamente qué tipo de resolución se está empleando y de gestionar dichos mensajes. En el caso del protocolo TCP/IP, éste incluye ARP (aunque ARP podría utilizarse también en redes que no sean TCP/IP, ya que está definido en forma amplia).

En esencia, ARP define dos tipos básicos de mensajes:

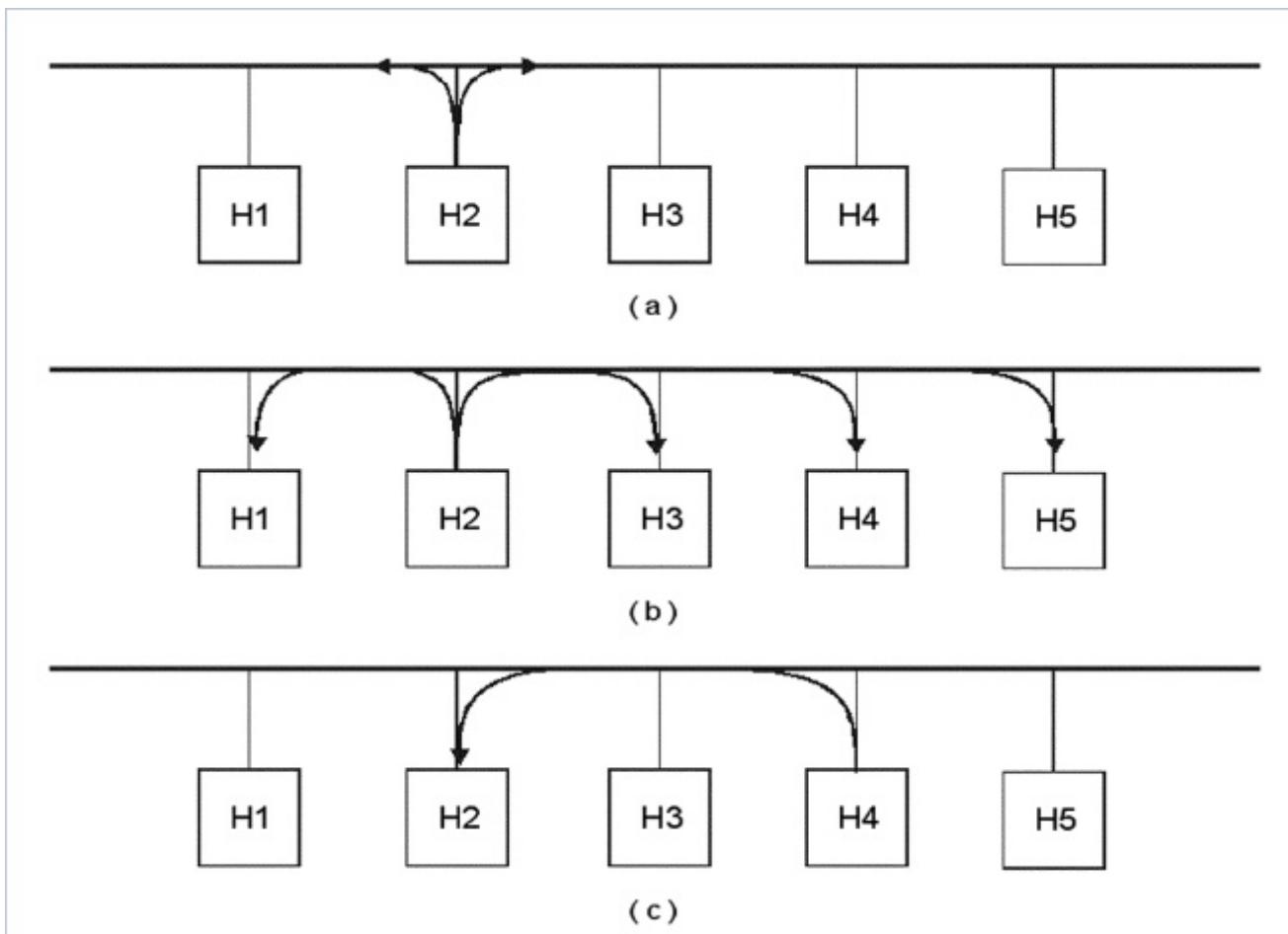
- Mensaje de solicitud
- Mensaje de respuesta

Esencialmente, un mensaje de solicitud incluye la dirección IP del host con el que se desea establecer conexión y solicita la dirección de *hardware* correspondiente.

También en forma general, podemos decir que un mensaje de respuesta incluye la dirección IP enviada con la solicitud junto con la de *hardware* asociada.

### Entrega de mensajes ARP

La forma de gestionar los mensajes ARP se encuentran especificados en la norma ARP. De una manera simplificada podemos decir que los mismos se gestionan de la siguiente manera:



"Intercambios de mensajes ARP" | (a) el Host 2 difunde una solicitud ARP para averiguar la dirección de hardware del Host 4. (b) todas las computadoras reciben el mensaje y lo procesan. (c) sólo el Host 4 responde al Host 2 en forma directa, sin utilizar la difusión.

- El host transmisor coloca un mensaje ARP de solicitud en un cuadro de nivel hardware y lo difunde a todos los demás hosts de la red.
- Cada una de las computadoras recibe dicha solicitud, y la procesa: inspecciona la dirección IP de destino.
- Sólo el host al que pertenece dicha dirección IP responde el mensaje, pero en la respuesta no se utiliza difusión, sino que se lo remite directamente al host que realizó la solicitud.

## ¿Cómo son los mensajes ARP? El formato de los mensajes ARP

Nosotros veremos un ejemplo de formato de mensaje ARP pensado para el caso de que el nivel lógico de la red está basado en TCP/IP (es decir, las direcciones de alto nivel serán IP) y el nivel físico de red es tecnología Ethernet, por qué éste es el caso más habitual. Sin embargo, ARP es lo suficientemente flexible como para brindar el servicio de resolución de direcciones a cualquier sistema de direcciones de alto nivel que necesite relacionar las mismas con cualquier tipo de direcciones de hardware. El porqué de esta flexibilidad quedará claro al ver el formato de los mensajes ARP. El Protocolo ARP se define en el RFC 826.

Un mensaje ARP es una larga secuencia de bits, distribuida como se muestra en la siguiente figura \* 14.11; no perdamos de vista que las direcciones de protocolo IP constan de 32 bits (4 Bytes) y las direcciones de hardware Ethernet de 48 bits (6 Bytes).

32 bits	
Tipo de Dirección de hardware (Ethernet)	Tipo de Dirección de Protocolo (IP)
Long. Dirección Hard.	Operación
Long. Dir. Protocolo	Dirección de Hardware del Transmisor (primeros 4 Bytes)
	Direcc. Hard. Transmisor (últimos 2 Bytes)
	Direcc. P Transmisor (últimos 2 Bytes)
	Dirección de hardware del Objetivo (últimos 4 Bytes)
	Dirección de Protocolo del Objetivo ( 4 Bytes)

En esta Tabla se ha utilizado la letra P para indicar Protocolo, en referencia al IP.

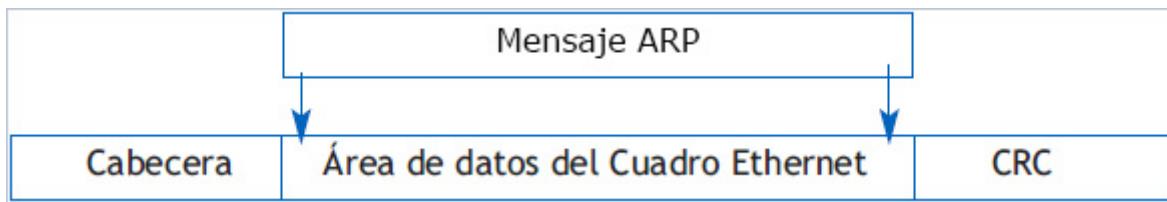
- El primer campo es de diecisés bits, indica el tipo de dirección de hardware. En el caso de que sea Ethernet debe ser 1.
- El segundo campo, también de 16 bits indica el tipo de dirección de protocolo. En nuestro caso es el IP. Para indicar IP en este campo se debe incluir el valor 0800 en hexadecimal.
- Los siguientes dos campos son de 8 bits cada uno, que indican las longitudes de las direcciones de hardware, en nuestro caso, Ethernet (48 bits), y de protocolo, en nuestro caso, IP (32 bits).
- El siguiente campo es de diecisés bits y está pensado para indicar el tipo de operación que se desea realizar, por ejemplo, una solicitud o una respuesta. En el caso de ser solicitud debe ir el valor 1, en el caso de ser una respuesta debe ir el valor 2.
- Los siguientes 48 bits son para transcribir la dirección de hardware del equipo que transmite (en este caso, son 48 bits porque hemos supuesto tecnología de red Ethernet; si fuera otra tecnología, irían los valores correspondientes).
- A continuación se disponen los dos primeros Bytes de la dirección IP del equipo objetivo.
- Luego, los dos primeros Bytes de la dirección IP del equipo transmisor.
- A continuación, 2 Bytes que sirven para indicar la dirección de hardware del equipo objetivo.
- Si ha venido leyendo con atención seguramente habrá esbozado una sonrisa: obviamente este campo no tiene sentido ya que la dirección de hardware del objetivo es lo que se pretendía averiguar; por ende, se completa con ceros, luego veremos que en otro contexto sí tiene sentido.
- A continuación cuatro Bytes correspondientes a la dirección de hardware del objetivo que tampoco tienen sentido.
- Por último, los primeros cuatro Bytes correspondientes a la dirección IP del objetivo los cuales si son conocidos al emitir la solicitud.

## Transmisión de un mensaje ARP

Cuando un *host* envía un mensaje ARP a otro, éste viaja dentro de un cuadro de *hardware* (en nuestro caso, Ethernet); este mensaje ARP no es examinado por el hardware de red.

Técnicamente hablando, este proceso se denomina encapsulamiento, y a grandes rasgos consiste en la colocación de una cabecera de cuadro y de una trama al final del mismo (CRC).

La siguiente figura ilustra el concepto.



### Identificación de los cuadros ARP

De la misma forma que se transmiten encapsulados los mensajes ARP a nivel físico, se transmiten todos los otros mensajes entre computadoras a nivel físico; la pregunta que surge es entonces: ¿Cómo sabe la computadora que recibe el mensaje, que éste se trata de un mensaje ARP?

La respuesta viene dada por el proceso de encapsulamiento, en la cabecera se reserva una parte para un campo denominado tipo de cuadro, en el que se puede indicar qué tipo de mensaje es, en el caso de la norma Ethernet en ese cuadro debe figurar del número 0806 en hexadecimal. Ese valor indica que es un mensaje ARP.

### Manejo en memoria caché de las respuestas ARP

Supongamos la siguiente situación: el host 1 debe enviar un mensaje al host 2, como no conoce la dirección de hardware del host 2 difunde un mensaje ARP en la red para buscar la respuesta. El host 2 recibe el mensaje, lo procesa y remite la respuesta al host 1. En este momento el host 1 ya conoce la dirección de hardware del host 2, lo cual significa que está en condición de enviar el mensaje original, y entonces lo manda.

Tres mensajes han viajado por la red cuando, en el mejor de los casos, lo debería haber hecho sólo uno.

Pensemos -además- que es muy raro que un proceso de comunicación necesite intercambiar un solo mensaje, habitualmente son muchos. Si por cada mensaje que debe enviarse deben utilizarse tres mensajes ARP, el método no es muy eficiente.

Una forma de mejorarlo es permitir que el software ARP extraiga y guarde las relaciones entre las direcciones IP y las de hardware de cada mensaje de respuesta que recibe. De esta manera, si dos computadoras deben intercambiar cien mensajes, sólo se triplicará el tráfico de red en el primero de ellos.

El software no intenta mantener una tabla de relaciones históricas, sino que las manejar como una pequeña caché: se reemplazan entradas a medida que llegan nuevas respuestas y las entradas más viejas se eliminan cada vez que se acaba el espacio de la memoria caché o cuando no se ha actualizado en un periodo prolongado de tiempo (suele ser veinte minutos).

De esta manera cuando se solicita al software ARP que resuelva una dirección, primero se fija en su tabla en memoria caché y sólo si la relación no se encuentra en ella entonces difundirá el mensaje; si no utilizará la dirección que tiene almacenada.

Dado que cuando se envía una solicitud ARP, el mensaje se difunde a todas las computadoras de la red, y que todas ellas deben procesar si la dirección IP de destino es la de ellas, se presenta una buena oportunidad para que todas las computadoras de la red agreguen la relación entre la dirección IP y la de hardware de la máquina que inicia la transmisión. De esta forma se manejaban los primeros software de ARP. Sin embargo, en la actualidad se omite esta opción, ya que agregar esos datos a cada una de las cachés de las computadoras las hace perder tiempo y es poco probable que todas las computadoras necesiten comunicarse con todas las otras.

A menudo se ha criticado ARP aduciendo que es inseguro.

# REFERENCIAS 14

## 14.1 : Conectado

Cuando decimos que un dispositivo está conectado a una red queremos decir que está físicamente conectado, el elemento utilizado puede ser una placa de red (a menudo también llamadas interfaz de red, tarjetas adaptadoras de red o también NIC Network Interface Card), un módem o cualquier otro dispositivo que cumpla la función (puertos infrarrojos, inclusive conexiones seriales simples). Por ende cuando decimos que un Router está conectado a por lo menos dos redes significa que tiene por lo menos dos interfaces de red.

---

## 14.2 : Direcciones múltiples

Identifican a un grupo de host que comparten un protocolo común, en oposición al grupo de host que comparten una red común.

---

## 14.3 : Red clase E

No existe consenso con respecto a los bit que identifican a la Clase E. Algunos autores dicen que son cinco bit, dando la secuencia 11110, mientras que otros aseguran que no son necesarios cinco bit, que con cuatro es suficiente, ya que si los cuatro bit (1111) son uno, ya no puede ser ninguna de las otras clases, y por lo tanto son Clase E.

Si se toman cuatro o cinco bit para identificar la Clase E, cambiará la cantidad de redes posibles, pero como estas direcciones no están en uso, no es de importancia el comentario, sólo se efectúa como una curiosidad.

---

## 14.4 : Dirección

Las direcciones también pueden estar escritas en Hexadecimal, pero la notación con puntos es la más ampliamente usada.

---

## 14.5 : 255

El mayor valor decimal posible para un byte.

---

## 14.6 : Casos especiales

Obviamente los dos casos especiales anteriores implican que el administrador de red no debe asignar nunca a un host un HostID con todos sus bits iguales a 0 ni con todos sus bits iguales a 1, a no ser que desee generar un conflicto de software.

Para agregar un poco de confusión al tema, debemos hacer notar que aún persiste una antigua versión de TCP/IP (que se distribuía junto al UNIX de Berkeley) que utilizaba para la difusión la norma de "todos 0". Debido a este desliz el software TCP/IP actual a menudo reserva también la posibilidad de utilizar esta opción.

---

## 14.7 : Loopback

Es una dirección especial que permite verificar la propia placa de red, ya que cuando se envía un paquete, por ejemplo ICMP (ping), este paquete sale por el puerto de transmisión (Tx) e ingresa por el de recepción (Rx), verificando de esta manera el funcionamiento de la NIC.

---

## 14.8 : 10.255.255.255

Sólo se reserva una red Clase A.

---

## **14.9 : MAC**

Media Access Control o Control de Acceso al Medio. Esta es la subcapa inferior en la cual la IEEE divide a la capa de Enlace de Datos de OSI. Ver situaciones profesionales 3 y 4.

---

## **14.10 : Resolución de Direcciones**

Este tema es un mix de lo desarrollado en: capítulo 15 de "Redes de Computadoras, Internet e Interredes" de Comer; capítulo 5 de "Redes Globales de Información con Internety TCP/IP" de Comer; y capítulo 5 "La capa de red" (página 420) y "Redes de Computadoras" de Tanenbaum, en ese orden de importancia.

---

## **14.11 : Fuente del esquema**

Este esquema se ha tomado de Comer, "Redes Globales de Información con Internet" y TCP/IP, ya que está mejor que en el otro libro de Comer. Concretamente están distintos los órdenes de los Bytes.

---



¿Te animás a medir cuánto aprendiste?

**1. Indique la opción correcta**

Habitualmente cuando un host en el momento de arranque aún no sabe cuál es su dirección de red, utiliza Difusión Dirigida.

- Verdadero
- Falso

**2. Indique la opción correcta**

Si el primer bit de una dirección IP es 0 (cero) esta identifica una red clase:

- A
- B
- C
- E

**3. Indique la opción correcta**

Indique cuál de los siguientes NO es un método de resolución de direcciones:

- Resolución Directa.
- Resolución Indirecta.
- Búsqueda en Tabla.
- Enlace Dinámico.

**4. Indique la opción correcta**

Indique cuál de las siguientes NO es una dirección IP Privada:

- 10.17.25.41
- 172.16.46.58
- 172.32.26.89
- 192.168.65.89

**5. Ordene relaciones**

Las siguientes direcciones IP pertenecen a las siguientes clases:

14.27.3.45	es una dirección clase B
136.12.67.21	es una dirección clase D
200.10.12.98	es una dirección clase A
225.15.168.1	es una dirección clase C

## 6. Ordene relaciones

El uso de cada uno de los métodos depende del esquema de direccionamiento de hardware de la red; en general se utiliza:

Búsqueda en Tabla	para redes con direcciones estáticas de hardware.
Cálculo en forma cerrada	para redes que son configurables.
Intercambio dinámico	para resolver direcciones IP en una WAN.

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Habitualmente cuando un host en el momento de arranque aún no sabe cuál es su dirección de red, utiliza Difusión Dirigida.

- Verdadero
- Falso

## 2. Indique la opción correcta

Si el primer bit de una dirección IP es 0 (cero) esta identifica una red clase:

- A
- B
- C
- E

## 3. Indique la opción correcta

Indique cuál de los siguientes NO es un método de resolución de direcciones:

- Resolución Directa.
- Resolución Indirecta.
- Búsqueda en Tabla.
- Enlace Dinámico.

## 4. Indique la opción correcta

Indique cuál de las siguientes NO es una dirección IP Privada:

- 10.17.25.41
- 172.16.46.58
- 172.32.26.89
- 192.168.65.89

## 5. Ordene relaciones

Las siguientes direcciones IP pertenecen a las siguientes clases:

- |              |                          |
|--------------|--------------------------|
| 14.27.3.45   | es una dirección clase A |
| 136.12.67.21 | es una dirección clase B |
| 200.10.12.98 | es una dirección clase C |
| 225.15.168.1 | es una dirección clase D |

## 6. Ordene relaciones

El uso de cada uno de los métodos depende del esquema de direccionamiento de hardware de la red; en general se utiliza:

- |                          |  |
|--------------------------|--|
| Búsqueda en Tabla        | para resolver direcciones IP en una WAN. |
| Cálculo en forma cerrada | para redes que son configurables.        |

Intercambio dinámico

para redes con direcciones  
estáticas de hardware.

# SP8 / H3: Introducción al Ruteo IP

Suele hacerse una distinción entre dos tipos de ruteo IP:

- Ruteo directo
- Ruteo indirecto

## Ruteo directo

Con ruteo directo se pretende distinguir aquellos casos en los cuales el envío de información se realiza a través de la misma red física; es decir, cuando el emisor y el receptor forman parte de la misma red, por ejemplo, una red Ethernet.

## Ruteo indirecto

El ruteo indirecto, en cambio, hace referencia al caso en el cual el emisor y el receptor forman parte de redes distintas; éste es el caso en el cual participan los Routers.

### Ruteo IP controlado por tabla

El elemento principal en el ruteo indirecto es la denominada tabla de ruteo IP o tabla de ruteo Internet que existe en cada host y cada Router que participen de la red de redes.

¿Qué información está almacenada en esta tabla?

Afortunadamente, no es necesario almacenar todas las rutas posibles que comuniquen a un host determinado con cualquier otro host (o su dirección de IP) del mundo. Esto es así por dos razones:

- La primera, para direccionar un datagrama no es necesario usar el campo HostID de la dirección IP del destino, solamente es necesario conocer el NetID de esa dirección de IP.
- La segunda razón es que se utiliza el ruteo con salto al siguiente, lo cual evita que cada host deba conocer por completo la ruta a seguir hasta el destino.

### Ruteo con salto al siguiente

En general, una tabla de ruteo IP contiene pares, donde uno de los elementos es la dirección IP de una red de destino, y el segundo elemento es la dirección IP del siguiente Router en el camino hacia dicha red. Este Router es conocido como el salto siguiente; de esta forma sólo es necesario almacenar la información correspondiente al próximo salto, y no la información de una ruta completa. Esto hace que las tablas sean mucho más reducidas.

Ni el host de origen ni los Routers intermedios, conocen de antemano por dónde llegar al host destino (excepción hecha del caso en el cual la ruta se especifica en el datagrama IP analizado en un apartado anterior).

La siguiente figura ejemplifica cómo es una tabla de ruteo IP.

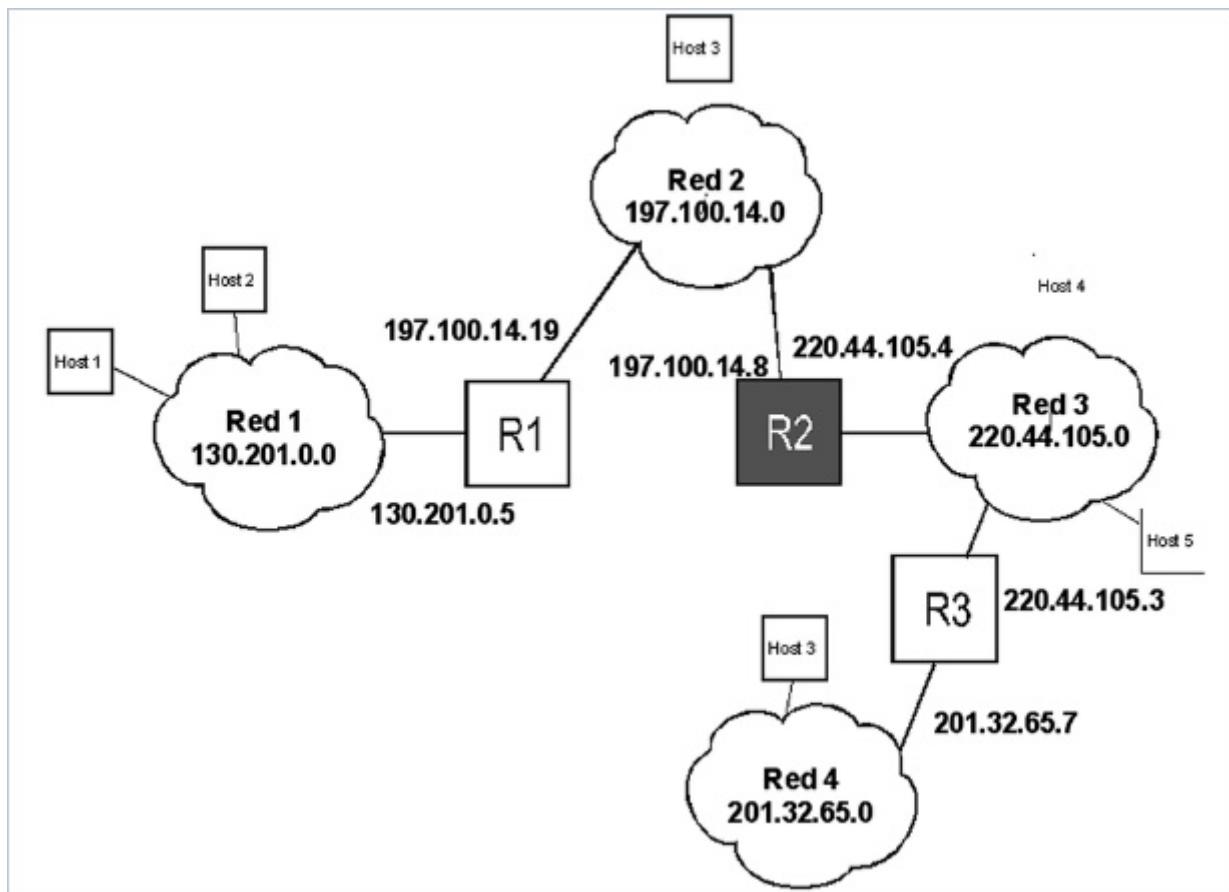


Tabla de Ruteo de R2

Red Destino	Rutear a
130.201.0.0	197.100.14.19
197.100.14.0	entrega directa
220.44.105.0	entrega directa
201.32.65.0	220.44.105.3

## Los casos especiales

### Rutas asignadas por omisión

¿Qué pasa cuando una red destino no figura en una tabla de ruteo IP? El truco es asignar la dirección de un Router por omisión, al cual se enviarán todos aquellos datagramas para los cuales no se tienen cargados en la tabla los datos correspondientes al próximo salto.

Obviamente, que un ruteo por omisión, funciona muy bien en aquellas redes que tienen un solo Router, ya que los hosts no tienen que "pensar" mucho a cuál de los Routers disponibles deben enviar un mensaje que se dirige fuera de la red.

## Ruteo por host específico

Si bien el proceso de ruteo está basado en redes y no en hosts, es decir, se identifican las redes a las cuales deben llegar los mensajes, es posible asignar una ruta específica hacia un host determinado. Éste es un caso muy especial que suele utilizarse más que nada, para testear las conexiones de una red.

Seguramente, usted estará pensando lo siguiente: hasta aquí todo muy bien, el ruteo se entiende, pero, ¿cómo hace el software IP residente en los hosts y los Routers para armar las tablas, cómo hace para mantenerlas actualizadas?

## ICMP: mensajes de error y control del protocolo Internet (IP)

### El manejo de los errores con IP

Ya hemos mencionado un elemento de control de errores que forma parte del protocolo IP, la suma de verificación de su encabezado. Como usted recordará, la suma de verificación del encabezado se hace sobre todos los bits que forman parte del encabezado del datagrama IP; el host emisor calcula dicha suma y la agrega al campo suma de verificación; cuando un Router o el host destino recibe el mensaje, chequea que el resultado del campo de verificación realmente corresponda a la suma de todos los otros bits del encabezado. Si esto no es así, el host destino o el Router, eliminan el datagrama completo.

Obsérvese, que el datagrama debe ser eliminado y que el Router o el host destino es incapaz de remitirle un mensaje a la fuente, por ejemplo, indicando que el datagrama se perdió. Esto es así porque dado que se sabe que se ha dañado por lo menos un bit del encabezado, no se puede confiar en ninguna de las direcciones IP e incluidas en él. Esto determina que en el caso de un error en la suma de verificación, el datagrama completo debe ser eliminado.

Claro que también hay otro tipo de errores en la entrega de datagramas, los cuales no involucran la destrucción de las direcciones IP de origen o destino; en esos casos es posible realizar un reporte de errores; y el encargado de hacerlo es el protocolo ICMP.

Errores de entrega de Datagramas de esta categoría pueden ocurrir cuando el host destino está desconectado, cuando el contador del tiempo de vida expira, o cuando los Routers intermedios se congestionan tanto que no pueden procesar el tráfico entrante. En todos estos casos es posible utilizar ICMP para reportar el error de la entrega del datagrama al host fuente.

Si bien tanto IP como ICMP son protocolos separados, y ambos conviven en la misma capa de interred, son fuertemente interdependientes.

*Toda implementación IP obligatoriamente debe incluir el protocolo ICMP; por otro lado los mensajes ICMP son simplemente datagramas IP. En resumen IP, utiliza ICMP para reportar errores, e ICMP utiliza IP para enviar sus mensajes.*

Los mensajes de reporte de errores ICMP viajan por la red en la parte de datos de un datagrama IP; sin embargo, el destino final de mensajes ICMP no es un programa de aplicación ni un usuario en el host de destino, sino el software de protocolo internet (IP) en dicha máquina. Esto significa que cuando llega un mensaje de error ICMP, el módulo de software ICMP lo maneja; claro que si ICMP determina que un protocolo de un nivel más alto o un programa de aplicación causaron el problema, notificará a dicho módulo.

Un detalle importante: si bien es cierto que ICMP ha sido diseñado para permitir que los Routers reporten a los hosts las causas de los errores en la entrega, el ICMP no se restringe sólo a los Routers. Aunque las reglas y normas limitan el uso de algunos mensajes ICMP, en realidad cualquier máquina puede enviar un mensaje

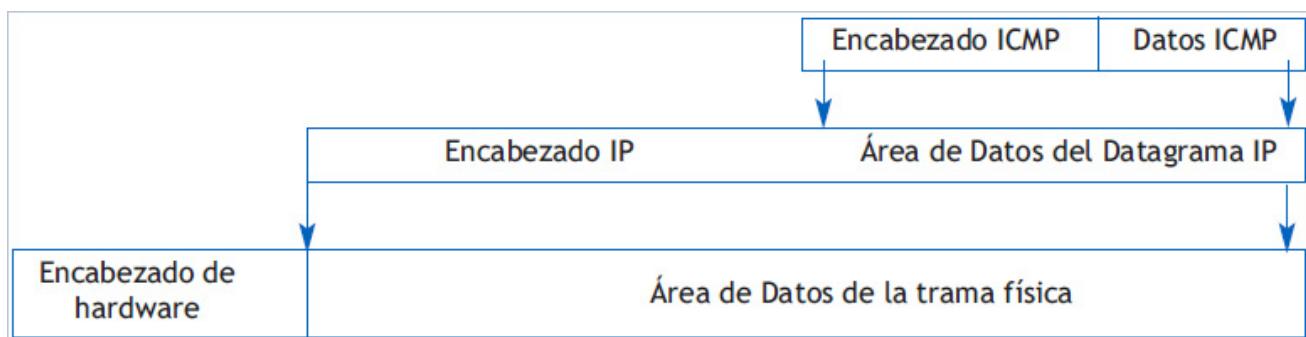
ICMP a cualquiera otra . Por lo tanto, un host puede utilizar ICMP para comunicarse con un Router o con otro Host. La mayor ventaja de permitir que los hosts utilicen ICMP es que proporciona un solo mecanismo que se utiliza para todos los mensajes de información y control.

## Reporte de errores y corrección de errores

No olvidemos que técnicamente ICMP es un protocolo que brinda un mecanismo para reportar errores, no para corregirlos; toda acción de corrección debe llevarse a cabo en el host que originó el datagrama. Esto es así porque los Routers envían el mensaje de error al host fuente, y ni siquiera remiten mensajes de error a otros Routers. ¿Por qué no remitir mensajes de error a otros Routers? La respuesta es sencilla: no olvidemos que en el encabezado del datagrama IP sólo figuran las direcciones IP del host origen y el host destino; no figuran las direcciones IP de los Routers por los cuales ha transitado el datagrama, excepto en el excepcional caso de que esté habilitada la opción que guarda las direcciones de cada uno de los Routers por los que ha transitado el datagrama. Como puede apreciarse, esta limitación es un elemento negativo de ICMP pero, por otro lado, hace que los mensajes sean más cortos y por lo tanto la transmisión sea más veloz.

## La entrega de los mensajes ICMP

Como comentábamos anteriormente, un mensaje ICMP se envía en la porción de datos reservada de un simple datagrama IP. A su vez, este datagrama se encapsula en una trama de hardware donde viaja en la porción de datos de la misma. Es decir que tiene un doble proceso de encapsulamiento.



Como se puede presumir, los datagramas que llevan mensajes de reporte de errores ICMP se rutean exactamente igual que cualquier datagrama IP; no existe ni una confiabilidad ni una prioridad adicionales, es decir que los mensajes de error se pueden perder o descartar. Hay que tener en cuenta que estos mensajes de error también causan congestionamientos adicionales en la red.

Sin embargo, existe una diferencia fundamental entre el manejo de un datagrama IP común y uno que lleva un mensaje ICMP: **si un datagrama IP que lleva un mensaje ICMP genera un error, éste no se reporta con otro mensaje ICMP**; de esta forma se evita aumentar el congestionamiento de la red con mensajes de error que reportan errores en el envío de mensajes de error indefinidamente.

Usted puede preguntarse cómo hace un Router para determinar que no debe dar respuesta a un error generado por un datagrama IP que lleva un mensaje ICMP; la pregunta que subyace es ¿cómo hace un Router para distinguir un datagrama IP común de uno que lleva un mensaje de error ICMP?

La respuesta es sencilla: si usted recuerda, en el encabezado de todo datagrama IP hay un campo denominado protocolo; según el valor ubicado en ese campo, se puede saber si el mensaje que lleva es uno común o uno que lleva un mensaje ICMP \* 15.1 .

## Formato de los mensajes ICMP

Si bien, cada mensaje ICMP tiene su propio formato, todos comparten los tres primeros campos:

- Campo tipo de mensaje: 8 bits que identifican el mensaje.
- Campo código: 8 bits que proporcionan más información sobre el tipo de mensaje.
- Campo suma de verificación: de 16 bits. Esta suma de verificación se realiza solamente sobre el mensaje ICMP.

Además, todos los mensajes ICMP que reportan errores siempre reenvían el encabezado del datagrama que generó el error y los primeros 64 bits de datos del mismo. Esto es útil para que el host origen determine con precisión cuál fue el datagrama que generó el mensaje de error. Esto es así porque los protocolos de nivel más alto del grupo TCP/IP están diseñados para incluir información trascendental en los primeros 64 bits de datos.

### Campo Tipo de Mensaje

Valor del campo	Descripción del Tipo de Mensaje
0	Respuesta de Eco
3	Destino Inaccesible
4	Disminución de Origen
5	Redireccionar
8	Solicitud de Eco
11	Tiempo Excedido para un datagrama
12	Problemas de parámetros en un datagrama
13	Solicitud de Timestamp
14	Respuesta de Timestamp
15	Solicitud de información (fuera de uso)
16	Respuesta de solicitud de información (fuera de uso)
17	Solicitud de máscara de dirección
18	Respuesta de máscara de dirección

### Solicitud de Eco (Echo Request o Ping)

Una de las herramientas de depuración más utilizada incluye los mensajes ICMP de solicitud de eco y respuesta de eco.

Un host o un Router envía un mensaje ICMP de solicitud de eco hacia un destino específico; cuando la máquina recibe la solicitud de eco, formula una respuesta y la regresa al transmisor original.

La solicitud contiene un área opcional, un área donde el emisor puede ubicar una cierta cantidad de datos, cotejada en la respuesta de eco para ver si son iguales.

En el caso que coincidan, significa que el destino es accesible y que la transmisión ha sido confiable.

En la mayoría de los sistemas, el comando que llama el usuario para enviar solicitudes de eco ICMP se denomina ping. Las versiones más sofisticadas de ping envían una serie de solicitudes de eco ICMP, capturan

las respuestas, y proporcionan estadísticas sobre la pérdida de datagramas. Además, miden el tiempo que tarda en ser devuelto el mensaje.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31								
Tipo (8 o 0)								Código (0)								Suma de Verificación																							
Identificador																Número de Secuencia																							
Datos Opcionales																																							
***																																							

- **Campo Tipo:** identifica si es una solicitud de Eco ( 8 ) o una respuesta de Eco ( 0 ).
- **Campos de Identificación y secuencia:** se utilizan para responder las solicitudes.
- **Campo de datos opcionales:** el transmisor puede agregar datosopcionales para controlar la respuesta. El receptor de una solicitud de eco, siempre trata de devolver los datosopcionales exactamente iguales a los recibidos.

## Reporte de destinos no accesibles

Cuando un Router no puede direccionar o entregar un datagrama, envía al host de origen un mensaje ICMP de destino no accesible.

Son muchas las razones por las cuales un mensaje puede no ser entregado: entre otras, que no se pueda acceder a la red a la que pertenece el host destino, o que el host sea inaccesible porque, por ejemplo, está desconectado, o puede ser que el puerto al que va dirigido el mensaje original no se encuentre habilitado en el host destino.

El listado completo, junto con sus códigos de Tipo se muestran en la siguiente tabla:

Código de tipo	Descripción
0	Red inaccesible
1	Host inaccesible
2	Protocolo inaccesible
3	Puerto inaccesible
4	Se necesita fragmentación y configuración DF (se utiliza en el caso que el datagrama original tenga seteado el valor de no fragmentación)
5	Falla en la ruta de origen
6	Red de destino desconocida
7	Host destino desconocido
8	Host de origen aislado
9	Comunicación con la red destino prohibida
10	Comunicación con el host destino prohibida
11	Red inaccesible por el tipo de servicio (TOS)
12	Host inaccesible por el tipo de servicio (TOS)

### Formato de los mensajes de destino inaccesible

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31								
Tipo ( 3 )				Código (0-12)										Suma de Verificación																									
No utilizable (debe ser 0)																																							
Encabezado IP - primeros 64 bits del datagrama																																							
...																																							

# REFERENCIAS 15

## 15.1 : ICMP

Hay que tener en cuenta que aunque un mensaje ICMP se introduce en la porción reservada para los datos de un mensaje IP común, no debe verse a ICMP como un protocolo superior a IP. Es más, ya habíamos indicado que ICMP esté en la misma capa que IP. Además todo programa IP debe incorporar el protocolo ICMP.

---



¿Estás listo para un desafío?

**1. Indique la opción correcta**

Cuando un router recibe un mensaje, debe direccionarlo en la "dirección correcta"; esto implica que cada router debe conocer el camino (o ruta) completo hasta el host de destino.

- Verdadero
- Falso

**2. Indique la opción correcta**

ICMP es un protocolo que resuelve problemas de comunicación.

- Verdadero
- Falso

**3. Indique la opción correcta**

Dado que ICMP es un protocolo que reside en la capa de red, es una alternativa al servicio brindado por IP.

- Verdadero
- Falso

**4. Indique la opción correcta**

Indique ¿Cuál de las siguientes afirmaciones NO es correcta: ICMP es un protocolo que:

- Reporta errores.
- Utiliza datagramas IP.
- Resuelve problemas de comunicación.
- No ofrece servicio a las capas superiores.

**5. Indique la opción correcta**

IP e ICMP son:

- El mismo protocolo que tiene el mismo destino final.
- Protocolos separados fuertemente interdependientes.

- o Protocolos de distintas capas del modelo TCP/IP.
- o Protocolos alternativos que cumplen el mismo fin.

#### 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

ICMP

es un mensaje ICMP enviado por un router cuando no puede direccionar o entregar

Ping

es un comando que una solicitud de eco para verificar entre otras cosas si un destino es accesible

Reporte de destino no accesible

es un protocolo que brinda un mecanismo para reportar errores, no para corregirlos

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Cuando un router recibe un mensaje, debe direccionarlo en la "dirección correcta"; esto implica que cada router debe conocer el camino (o ruta) completo hasta el host de destino.

- Verdadero
- Falso

## 2. Indique la opción correcta

ICMP es un protocolo que resuelve problemas de comunicación.

- Verdadero
- Falso

## 3. Indique la opción correcta

Dado que ICMP es un protocolo que reside en la capa de red, es una alternativa al servicio brindado por IP.

- Verdadero
- Falso

## 4. Indique la opción correcta

Indique ¿Cuál de las siguientes afirmaciones NO es correcta: ICMP es un protocolo que:

- Reporta errores.
- Utiliza datagramas IP.
- Resuelve problemas de comunicación.
- No ofrece servicio a las capas superiores.

## 5. Indique la opción correcta

IP e ICMP son:

- El mismo protocolo que tiene el mismo destino final.
- Protocolos separados fuertemente interdependientes.
- Protocolos de distintas capas del modelo TCP/IP.
- Protocolos alternativos que cumplen el mismo fin.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

ICMP	es un protocolo que brinda un mecanismo para reportar errores, no para corregirlos
Ping	es un comando que una solicitud de eco para verificar entre otras cosas si un destino es accesible
Reporte de destino no accesible	es un mensaje ICMP enviado por un router cuando no puede direccionar o entregar



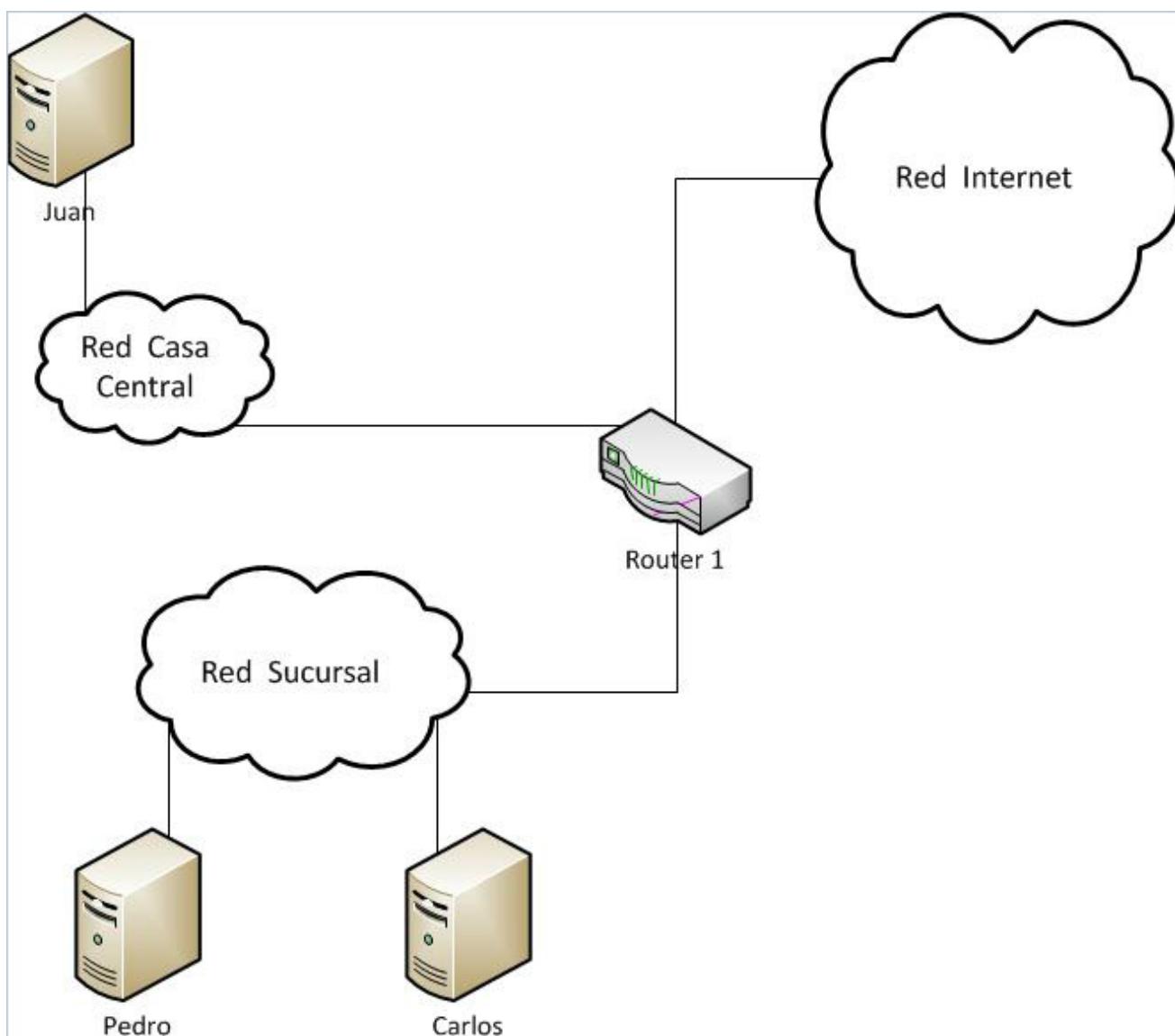
## SP8 / Ejercicio resuelto

Para contratar un servicio de acceso a Internet que permita alcanzar los objetivos de la empresa, de la oferta disponible en nuestra ciudad, aconsejamos la contratación de una empresa proveedora de servicios de internet por cable que tenga la capacidad de asignar direcciones IP fijas.

A fin de resolver este ejercicio con las herramientas vistas, no tendremos en cuenta otro tipo de soluciones como la utilización de NAT, Subredes o Superredes que se verán mas adelante en la SP9 y nos dedicaremos a encontrar una solución sencilla, asignando direcciones IP a las distintas redes como si pudiéramos disponer de ellas libremente y a los Routers que las conectan.

Sabiendo que ya tenemos enlazadas la Red Casa Central con la Red Sucursal mediante una conexión propia utilizando switches, no es necesario que cada una de ellas salga por si misma a Internet

Resolvemos entonces la situación planteada con el siguiente esquema de direccionamiento:



"SP8 Ej Resuelto" | Elaboración propia Autor

En la figura se brinda un esquema de conexión de dos redes, la Red Casa Central y la Red Sucursal que, como estaban previamente enlazadas mediante switches, es posible realizar la conexión de ambas al Router.

Se muestran tambien a manera de ejemplo algunos host conectados a las redes. Como ya habíamos definido anteriormente estas redes son tipo estrella en el caso de la Casa Central y tipo estrella de estrellas para el caso de la Sucursal, ambas con un concentrador principal del tipo Switch.

Sabiendo que:

La Red Casa Central está compuesta por 30 Hosts,

La Red Sucursal es posible que llegue a tener 300 Hosts

**Asignamos direcciones IP en formato decimal con puntos a cada red** de la siguiente forma:

Red Casa Central: utilizamos una dirección IP de clase C: 210.21.2.0

Red Sucursal: utilizamos una dirección IP de clase B: 130.13.0.0

**Asignamos direcciones IP en formato decimal con puntos a cada host** de la siguiente forma:

Red Casa Central: utilizamos direcciones IP de clase C que van desde: 210.21.2.1 hasta 210.21.2.30

Red Sucursal: utilizaremos direcciones IP de clase B que van desde: 130.13.0.1 hasta 130.13.1.46

A manera de ejemplo algunos host tendrán las siguientes direcciones IP:

Juan tiene asignada la dirección IP: 210.21.2.1

Pedro tiene asignada la dirección IP: 130.13.0.1

Carlos tiene asignada la dirección IP: 130.13.0.2

**Asignamos las direcciones correspondientes al Router:**

Router 1: 200.20.2.128 (asignado por nuestro proveedor para la conexión a Internet)

Router 1: 210.21.2.251 (asignado para conectarse a la red Casa Central)

Router 1: 130.13.1.251 (asignado para conectarse a la red Sucursal)

A continuación damos **algunos ejemplos de direcciones origen y destino** para los siguientes casos:

Juan le envía un mensaje a Pedro: IP Origen: 210.21.2.1 IP Destino: 130.13.0.1

Pedro responde a Juan; IP Origen: 130.13.0.1 IP Destino: 210.21.2.1

Juan envía un mensaje a todos los host de la red Casa Central: IP Origen: 210.21.2.1 IP Destino: 255.255.255.255

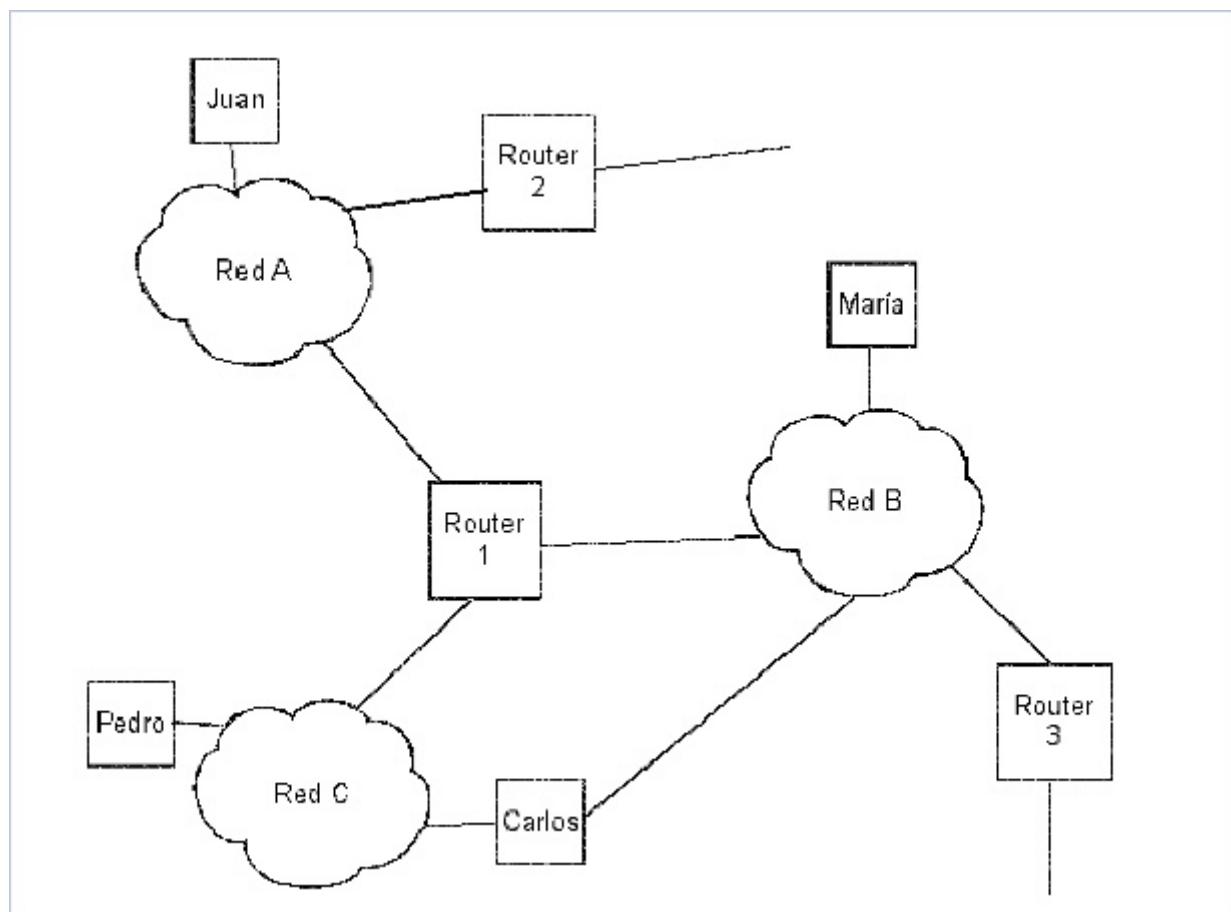
Juan envía un mensaje a todos los host de la red Sucursal: IP Origen: 210.21.2.1 IP Destino: 130.13.255.255

Seguramente tendrá muchas dudas acerca de los porque en las asignaciones de estas direcciones IP y no otras, repase los conceptos contenidos en las herramientas vistas en esta SP (SP8 / H1: La Entrega de Datos) y luego coméntelas a su profesor, la charla será muy fructífera pues podrá integrar todos los conceptos. Con lo que aprenda en las SP siguientes seguramente estará en capacidad de poder plantear otras soluciones.

## SP8 / Ejercicio por resolver

Los siguientes ejercicios deberán ser presentados resueltos y por escrito la siguiente clase.

En la figura siguiente se brinda un esquema de conexión de varias redes, Red A, Red B, Red C. Se muestran también algunos *routers* y algunos de los *hosts* conectados a las redes.



Se pide:

1. Asigne las direcciones IP en formato decimal con puntos a cada red, sabiendo que:

- La red A se piensa estará compuesta por 30 hosts,
- La red B es posible que llegue a tener hasta 500 hosts y
- La red C, se plantea como una que en el futuro pueda albergar unos 100 mil hosts.

Elemento	Dirección IP
Red A	
Red B	
Red C	

2. Asigne direcciones IP en formato decimal con puntos a cada host:

Host	Dirección IP
Juan	
Pedro	
María	
Carlos	
Carlos	

3. Asigne las direcciones correspondientes a los Routers:

Router	Dirección IP
Router 1	
Router 1	
Router 1	
Router 2	
Router 3	

4. Determine las direcciones de origen y de destino para cada uno de los casos planteados:

Caso	IP Origen	IP Destino
Juan envía un mensaje a María		
María responde a Juan		
Pedro envía un mensaje a Carlos		
Pedro envía un mensaje a Carlos		
Carlos responde a Pedro		
Juan envía un mensaje a todos los hosts de la red B		
Pedro envía un mensaje a todos los hosts de la red C		

## SP8 / Evaluación de paso



¡Vamos a comprobar cuánto aprendiste!

### 1. Indique la opción correcta

Si un router no tiene información correspondiente a la red de destino de un mensaje, es decir si no tiene información sobre a qué router debe redireccionar el mensaje, debe enviar el mensaje a un router predefinido denominado "router por omisión" (en algunos casos también llamado default gateway). Habitualmente el router por omisión es un router que pertenece a la red troncal (backbone) o por lo menos más cercano a ella, es decir un router "más grande", que posee tablas de ruteo más extensas.

- Verdadero
- Falso

### 2. Indique la opción correcta

Para distinguir un datagrama IP "común" de uno que transporta un reporte de error ICMP el router lee el campo Protocolo del encabezado del datagrama IP, según su valor podrá distinguir si el datagrama contiene datos de las entidades de las capas superiores (como UDP o TCP) o de ICMP.

- Verdadero
- Falso

### 3. Indique la opción correcta

Si un host recibe un mensaje ICMP cuyo campo "Tipo de mensaje" contiene un valor 8, significa que ha recibido una solicitud de eco (o ping). En consecuencia deberá responder a la misma al host que originó la solicitud. Habitualmente esto significa cargar los datos enviados en el área de datos de la solicitud y reenviarlos al origen, en el campo Tipo del Mensaje deberá poner un valor 0(valor correspondiente a la Respuesta de Eco).

- Verdadero
- Falso

### 4. Indique la opción correcta

Un router es:

- Un dispositivo que proporciona conectividad a nivel de hosts.

- Un dispositivo que proporciona conectividad a nivel de redes.
- Un dispositivo que regenera la señal en todas direcciones.
- Un dispositivo que se utiliza para conectarse vía telefónica a internet.

**5. Indique la opción correcta**

El protocolo IP es un protocolo de comunicación de datos que trabaja en la capa:

- Física.
- Enlace de Datos.
- Red.
- Aplicación.

**6. Indique la opción correcta**

En los mensajes ICMP el campo tipo posee:

- 8bits.
- 16 bits.
- 24 bits.
- 32 bits.

**7. Ordene relaciones**

Para cada clase existen un rango de direcciones privadas:

Para la clase A	desde 172.16.0.0 hasta 172.31.255.255
Para la clase B	desde 192.168.0.0 hasta 192.168.255.255
Para la clase C	desde 10.0.0.0 hasta 10.255.255.255

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Si un router no tiene información correspondiente a la red de destino de un mensaje, es decir si no tiene información sobre a qué router debe redireccionar el mensaje, debe enviar el mensaje a un router predefinido denominado "router por omisión" (en algunos casos también llamado default gateway). Habitualmente el router por omisión es un router que pertenece a la red troncal (backbone) o por lo menos más cercano a ella, es decir un router "más grande", que posee tablas de ruteo más extensas.

- Verdadero
- Falso

## 2. Indique la opción correcta

Para distinguir un datagrama IP "común" de uno que transporta un reporte de error ICMP el router lee el campo Protocolo del encabezado del datagrama IP, según su valor podrá distinguir si el datagrama contiene datos de las entidades de las capas superiores (como UDP o TCP) o de ICMP.

- Verdadero
- Falso

## 3. Indique la opción correcta

Si un host recibe un mensaje ICMP cuyo campo "Tipo de mensaje" contiene un valor 8, significa que ha recibido una solicitud de eco (o ping). En consecuencia deberá responder a la misma al host que originó la solicitud. Habitualmente esto significa cargar los datos enviados en el área de datos de la solicitud y reenviarlos al origen, en el campo Tipo del Mensaje deberá poner un valor 0(valor correspondiente a la Respuesta de Eco).

- Verdadero
- Falso

## 4. Indique la opción correcta

Un router es:

- Un dispositivo que proporciona conectividad a nivel de hosts.
- Un dispositivo que proporciona conectividad a nivel de redes.
- Un dispositivo que regenera la señal en todas direcciones.
- Un dispositivo que se utiliza para conectarse vía telefónica a internet.

## 5. Indique la opción correcta

El protocolo IP es un protocolo de comunicación de datos que trabaja en la capa:

- Física.
- Enlace de Datos.
- Red.
- Aplicación.

## 6. Indique la opción correcta

En los mensajes ICMP el campo tipo posee:

- 8bits.

- 16 bits.
- 24 bits.
- 32 bits.

**7. Ordene relaciones**

Para cada clase existen un rango de direcciones privadas:

Para la clase A	desde 10.0.0.0 hasta 10.255.255.255
Para la clase B	desde 172.16.0.0 hasta 172.31.255.255
Para la clase C	desde 192.168.0.0 hasta 192.168.255.255

# Situación profesional 9: ¿Necesitaremos Subredes u Súper-redes?

## Extensiones de direcciones de subred

Ya habrá notado que la red que ayuda a administrar es demasiado grande y compleja: muchas computadoras, conectadas a la misma, la vuelven lenta y difícil de controlar. Entonces piensa: ¿será posible dividir esta red en redes más pequeñas?, ¿tendré que gestionar una dirección IP distinta para cada nueva red? La respuesta es que, afortunadamente, sí es posible dividir su red; el proceso se llama "subnetting" y no será necesario que solicite otras direcciones IP.

# SP9 / H1: Problema del agotamiento de las direcciones IP por clases

## Un poco de historia

En cada año, el número de redes en Internet se fue incrementando. Sin embargo, el uso de las redes de clase A, B y C difirió mucho: la mayoría de las redes asignadas en la década de los 80 fueron de clase B, por otro lado, las redes de clase C apenas se usaban.

La razón de esta tendencia fue que la mayoría de los usuarios potenciales hallaban a las redes de clase B lo bastante grandes para sus necesidades previstas, ya que permite hasta 65534 hosts, mientras que una red de clase C, con un máximo de 254 hosts, restringe considerablemente el crecimiento potencial de las redes, aún las pequeñas.

La mayoría de las redes de clase B fueron asignadas a redes pequeñas, que no necesitaban 65534 direcciones de host, pero para las cuales 254 era un límite muy bajo.

En resumen, aunque las divisiones de clase A, B y C de las direcciones IP son lógicas y fáciles de usar (se efectúan a nivel de byte), en la práctica no son adecuadas. Por un lado las redes de clase C son demasiado pequeñas para la mayoría de las organizaciones, mientras que las clase B son demasiado grandes para ser bien aprovechadas por las organizaciones.

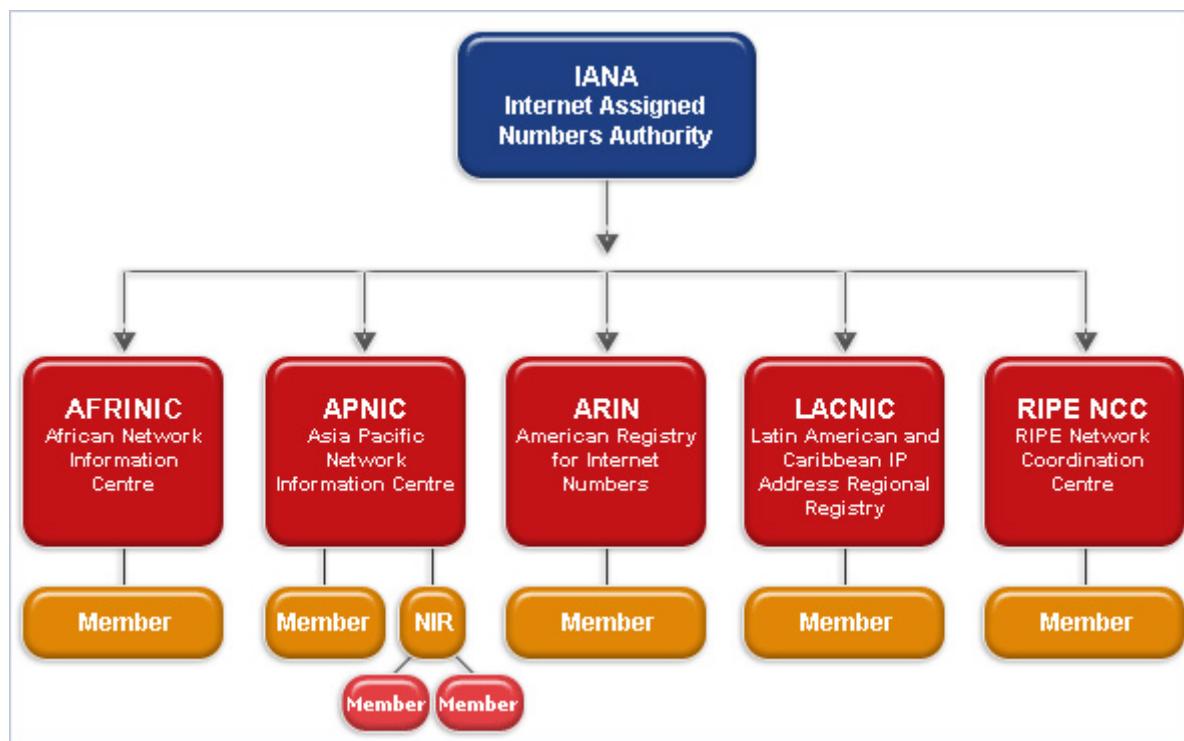
## Algunos aspectos importantes

**ICANN** (*Internet Corporation for Assigned Names and Numbers*) (Corporación de Internet para la Asignación de Nombres y Números).

Es una organización sin fines de lucro con objeto de encargarse de cierto número de tareas realizadas con anterioridad a esa fecha por otra organización, la IANA. Su sede radica en California, EEUU, opera a nivel internacional y es la responsable de asignar las direcciones del protocolo IP, de los identificadores de protocolo, de las funciones de gestión del sistema de dominio y de la administración del sistema de servidores raíz. Delega alguna de sus funciones a IANA y se dedica a preservar la estabilidad de Internet por medio de procesos basados en el consenso.

**IANA** (*Internet Assigned Numbers Authority*) (Autoridad de numeros asignados Internet)

Es la entidad que tiene la responsabilidad de supervisar la asignación global de direcciones IP, nombres de dominio DNS y otros recursos relativos a los protocolos de Internet. Actualmente es un departamento de ICANN. Tuvo sus inicios en el Instituto de Ciencias de la Información (ISI) de la Universidad del Sur de California (USC), en virtud de un contrato de con el Departamento de Defensa estadounidense, hasta que en 1998 se creó la ICANN para asumir toda la responsabilidad bajo un contrato del Departamento de Comercio.



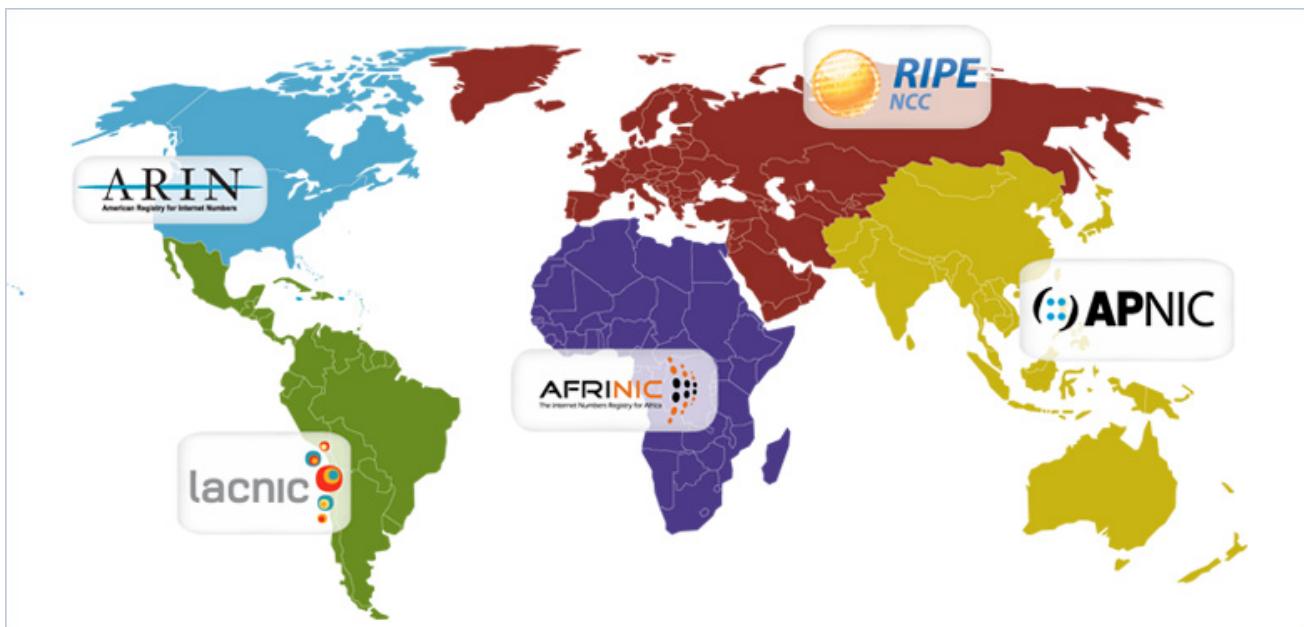
"IR Localización" | fuente: <http://www.nro.net/about-the-nro/regional-internet-registries>

### RIR (Regional Internet Registries) (Registros Regionales de Internet)

La numeración de los recursos en Internet se distribuye de manera jerárquica. La IANA ha delegado rangos de numeración de internet a los RIR, que luego asignan estos recursos dentro de sus regiones a los miembros, Registros Nacionales, Registros Locales y usuarios finales. Los RIR administran, distribuyen y registran la numeración dentro de sus respectivas regiones.

Existen cinco regiones:

1. ARIN (American Registry for Internet Numbers) para América Anglosajona
2. RIPE NCC (RIPE Network Coordination Centre) para Europa, el Oriente Medio y Asia Central.
3. APNIC (Asia-Pacific Network Information Centre) para Asia y la Región Pacífica.
4. LACNIC (Latin American and Caribbean Internet Address Registry) para América Latina y el Caribe.
5. AFRINIC (African Network Information Centre) para África



"RIR Regiones" | fuente: <http://www.nro.net/about-the-nro/regional-internet-registries>

Según IANA, las redes **asignadas** son la cantidad de números de red en uso. Las cantidades de la clase C son algo imprecisas, puesto que no incluyen muchas redes de clase C en Europa que se destinaron a RIPE \* 16.1 y fueron asignadas posteriormente, aunque aún están registradas como parte de RIPE. Las redes **reservadas** incluyen todas las redes asignadas y adicionalmente, aquellas otras que han sido reservadas por IANA (por ejemplo, las 63 redes de clase A que IANA ha destinado a registros nacionales que posteriormente podrán asignarlas). Entonces, el estado de una red es asignado o reservado, pero el estado reservado incluye al asignado; por lo que, para determinar cuánto espacio "libre" queda se puede calcular restando de 100% el porcentaje reservado.

Hay que tener en cuenta que es probable que cada red tenga espacio libre, pero como este espacio no se puede utilizar fuera de la organización que controla la red, debe considerarse como espacio efectivamente utilizado.

Además, una decimosexta parte del espacio total es absorbido por las direcciones de multicast de clase D. Se consideran direcciones en uso. Otra decimosexta parte restante del espacio de direcciones, las direcciones de clase E, también las ha reservado IANA, son las correspondientes a las direcciones IP con los cuatro bits de orden superior puestos a uno.

Para frenar el agotamiento del espacio de direcciones de clase B, la política sobre la concesión de números de red cambió desde 1990 para preservar el espacio de direcciones existente, en particular, **las nuevas políticas se pueden resumir en:**

- La mitad superior del espacio de direcciones de clase A se reserva indefinidamente para tener la posibilidad de usarlo en la transición a un nuevo sistema de numeración.
- Las redes de clase B sólo se asignan a organizaciones que puedan probar claramente que las necesitan. Lo mismo ocurre, por supuesto, con las direcciones de clase A. Los requerimientos para las redes de clase B son que la organización solicitante :
  - tenga un esquema de subnetting con más de 32 subredes dentro de su red operativa;
  - tenga más de 4096 hosts.

Cualquier solicitud de una red de clase A se trataría considerando estrictamente el caso particular.

- A las organizaciones que no satisfacen los requerimientos para una red de clase B se les asigna un bloque de redes clase C numeradas consecutivamente.
- La mitad inferior del espacio de direcciones de clase C (números de red del 192.0.0 al 223.255.245) se divide en 8 bloques que para las autoridades regionales están reservadas del siguiente modo:

**192.0.0 - 193.255.255 Multi-regional**

**194.0.0 - 195.255.255 Europa**

**196.0.0 - 197.255.255 Otros**

**198.0.0 - 199.255.255 Norte América**

**200.0.0 - 201.255.255 Centro y Sur América**

**202.0.0 - 203.255.255 Borde del Pacífico**

**204.0.0 - 205.255.255 Otros**

**206.0.0 - 207.255.255 Otros**

Los rangos definidos como "otros" se utilizan donde hace falta flexibilidad por encima de las limitaciones de las fronteras regionales. El rango definido como "multi-regional" incluye las redes clase C que habían sido asignadas antes de que se adoptase este nuevo esquema. El InterNIC asignó 192 redes, y 193 habían sido previamente reservadas para el RIPE en Europa.

La mitad superior del espacio de direcciones de clase C (208.0.0 a 223.255.255) permanece sin asignar y sin reservar.

En las organizaciones que tienen una serie de números de clase C, el rango asignado contiene números de red contiguos a nivel de bit y el número de redes de ese rango es una potencia de dos. Es decir, todas las direcciones IP en ese rango tienen un prefijo común, y cada dirección con ese prefijo está a su vez dentro del rango. Por ejemplo, a una organización europea que requiera 1500 direcciones IP se le asignarían 8 números de red de clase C (2048 direcciones IP) del espacio reservado para redes europeas (194.0.0 a 195.255.255) y el primero de estos números de red sería divisible por ocho.

Un rango de direcciones que se adecuase a esta regla sería el 194.32.136 - 194.32.143, en cuyo caso contendría todas las direcciones IP con el prefijo de 21 bits 194.32.136, o '110000100010000010001'.

La cantidad máxima de números de red asignados contiguamente es 64, correspondiente a un prefijo de 18 bits. Una organización que requiera más de 4096 direcciones pero menos de 16,384 puede solicitar tanto una clase B como un rango de direcciones de clase C. En general, el número de clases C asignadas es el mínimo necesario para proporcionar la cantidad de direcciones IP que la organización requiera. Teniendo en cuenta una previsión para dos años siguientes.

Sin embargo, en algunos casos, una organización puede solicitar múltiples redes que sean tratadas por separado. Por ejemplo, a una organización con 600 host se le asignarían 4 redes de clase C. No obstante, si esos host estuvieran distribuidos a lo largo de 10 LAN con una cantidad de entre 50 y 70 hosts por LAN, tal esquema de direcciones causaría graves problemas, ya que la organización tendría que encontrar 10 subredes dentro de un rango de direcciones locales de 10 bits. Esto significaría que al menos alguna de las LAN tendría una máscara de subred de 255.255.255.192, que sólo permite 62 hosts por LAN.

La intención de las reglas no es forzar a la organización a que tenga un complicado sistema de subredes, así que la organización debería solicitar 10 números de clase C diferentes, uno para cada LAN.

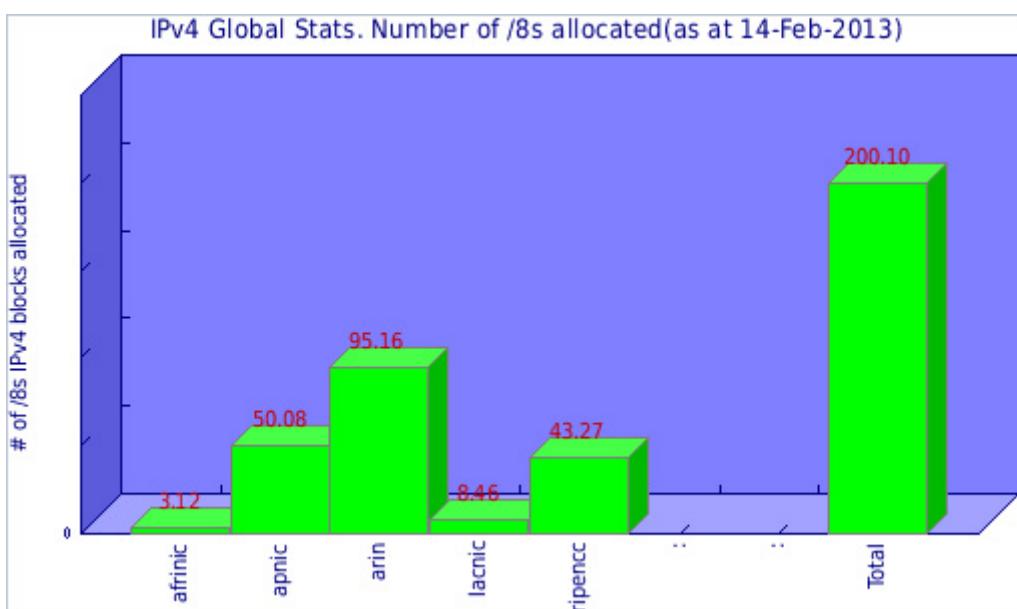
Usar números de clase C de esta forma ha frenado el problema del agotamiento de las direcciones de clase B, pero no es una solución definitiva a las limitaciones de espacio inherentes a IP. La solución a largo plazo se dará con IPv6 o IPng (*next generation*).

## Espacio de direcciones asignado en la actualidad

En el siguiente gráfico se puede observar el número de direcciones IPv4 asignadas hasta la fecha de publicación de este TID para cada Registro Internet Regional (RIR).

Aquí se cuentan todas las direcciones asignadas, incluyendo las que se asignaron antes de la creación de los RIRs.

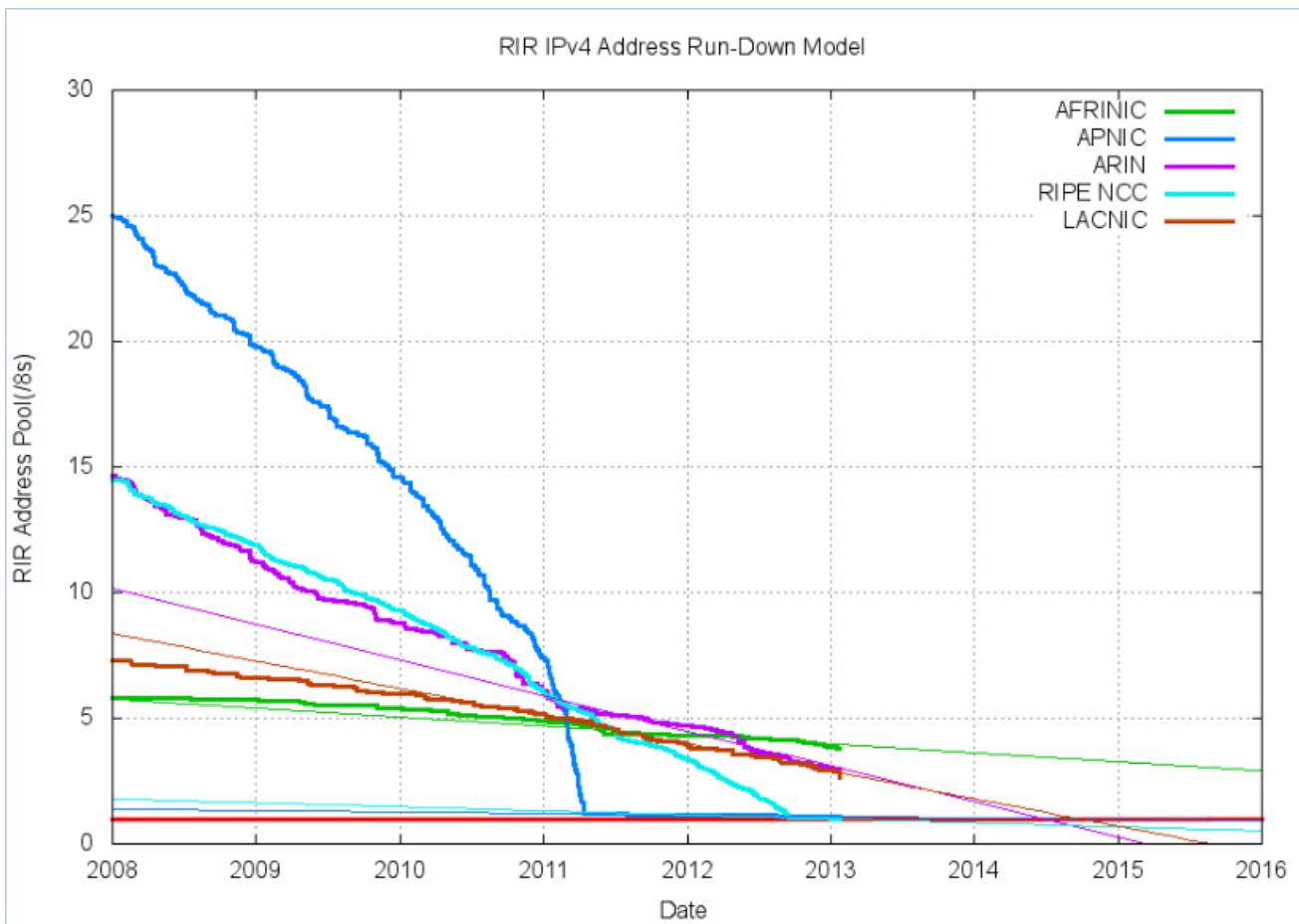
Verá en el gráfico que la cantidad de direcciones asignadas IPv4 se representan en cantidades "/8". Cada uno de esos "/8" contiene 16777216 direcciones IPv4. En la Herramienta 2 "Extensiónes de dirección de subred" de esta misma SP verá en profundidad el concepto de "/8". El total de "/8" asignados a los 5 RIRs se suma en la última barra.



"Distribucion Global IPV4" | fuente <http://portalipv6.lacnic.net/es/ipv6/estadisticas/ipv4/estadisticas-globales-de-ipv4-8-asignados>

## Proyección del agotamiento del espacio de direcciones

El siguiente gráfico muestra la evolución del total del espacio de direcciones IP desde 2004 hasta la actualidad, en todas las regiones



"IPV4 Espacio de direcciones" | fuente:

[http://upload.wikimedia.org/wikipedia/commons/5/52/Huston\\_rir\\_ipv4\\_exhaustion\\_projection.png](http://upload.wikimedia.org/wikipedia/commons/5/52/Huston_rir_ipv4_exhaustion_projection.png)

Se puede observar la proyección de las fechas de agotamiento del espacio de direcciones IP por cada RIR, lagunas de las cuales ya han sido alcanzadas (el caso de APNIC y RIPE) y las fechas probables proyectadas. Probablemente cuando usted lea esto ya habrá alguna otra de las RIR que haya agotado sus direcciones para entregar.

Para minimizar el efecto de este agotamiento, veremos en esta SP cuáles son las técnicas que normalmente se utilizan tales como el direccionamiento de subredes, máscaras de subred de longitud variable, direccionamiento de superredes, NAT (traducción de direcciones de red) y el sistema de nombres de dominio.

Deberá tener conocimiento de estos temas, pues es lo que hoy en día se está utilizando, hasta que se acuerde la implementación a nivel global de IPV6.

También expondremos los conceptos principales de este nuevo protocolo.

# REFERENCIAS 16

## 16.1 : RIPE

Réseaux IP Européennes. Grupo formado para coordinar y promover redes basadas en TCP/IP en Europa.

---



¿Te animás a medir cuánto aprendiste?

**1. Indique la opción correcta**

Una red "asignada" indica la cantidad de números de red en uso.

- Verdadero
- Falso

**2. Indique la opción correcta**

IANA (Internet Assigned Numbers Authority) (Autoridad de números asignados Internet) es la entidad que tiene la responsabilidad de supervisar la asignación global de direcciones IP.

- Verdadero
- Falso

**3. Indique la opción correcta**

El espacio de direcciones clase C que va desde el número 200.0.0.0 hasta el 201.255.255.255 es el que corresponde a la región de:

- Europa.
- Norte América.
- Centro y Sur América.
- Borde del Pacífico.

**4. Indique la opción correcta**

La fecha de agotamiento de capacidad de entrega de espacio de direcciones IPV4 ya ha sido alcanzada por:

- Ninguno de los RIR.
- ARIN y LACNIC.
- APNIC y RIPE.
- Todos los RIR.

**5. Indique la opción correcta**

Una organización que requiera más de 4096 direcciones pero menos de 16,384 puede solicitar:

- Una dirección clase A.
- Una dirección clase B.
- Un rango de direcciones de clase C.
- b y c son correctas.

#### 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

ARIN	es la región para América Latina y el Caribe
RIPE	es la región para Europa, el Oriente Medio y Asia Central
APNIC	es la región para Asia y la Región Pacífica
LACNIC	es la región para América Anglosajona

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Una red "asignada" indica la cantidad de números de red en uso.

Verdadero

Falso

## 2. Indique la opción correcta

IANA (Internet Assigned Numbers Authority) (Autoridad de números asignados Internet) es la entidad que tiene la responsabilidad de supervisar la asignación global de direcciones IP.

Verdadero

Falso

## 3. Indique la opción correcta

El espacio de direcciones clase C que va desde el número 200.0.0.0 hasta el 201.255.255.255 es el que corresponde a la región de:

Europa.

Norte América.

Centro y Sur América.

Borde del Pacífico.

## 4. Indique la opción correcta

La fecha de agotamiento de capacidad de entrega de espacio de direcciones IPV4 ya ha sido alcanzada por:

Ninguno de los RIR.

ARIN y LACNIC.

APNIC y RIPE.

Todos los RIR.

## 5. Indique la opción correcta

Una organización que requiera más de 4096 direcciones pero menos de 16,384 puede solicitar:

Una dirección clase A.

Una dirección clase B.

Un rango de direcciones de clase C.

X b y c son correctas.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

ARIN

es la región para América Anglosajona

RIPE

es la región para Europa, el Oriente Medio y Asia Central

APNIC

es la región para Asia y la Región Pacífica

LACNIC

es la región para América Latina y el Caribe



## SP9 / H2: Extensiones de dirección de subred

Desde mediados de los ochenta, Internet enfrenta dos graves problemas:

- Las tablas de ruteo crecen rápidamente.
- Los administradores locales de red se ven en la necesidad de utilizar más de una red para una organización determinada.

Pensemos en una organización que esté dividida en áreas, las cuales su vez estén divididas en departamentos, y que dentro de ellas haya diversos grupos de trabajo. Ante esta perspectiva es muy poco práctico que todas las computadoras se encuentren conectadas a una única red que les permita conectarse con el exterior. ¿Cuál era la perspectiva del administrador de red? Su opción era solicitar una nueva o varias direcciones IP. Claro que esto traía como consecuencia el agravamiento del primer problema mencionado anteriormente: al entregar mayor cantidad de direcciones IP, automáticamente crecen las tablas de ruteo; por otro lado, dado que la cantidad de direcciones IP es limitada y relativamente escasa, esto podría llevar al agotamiento de las mismas.

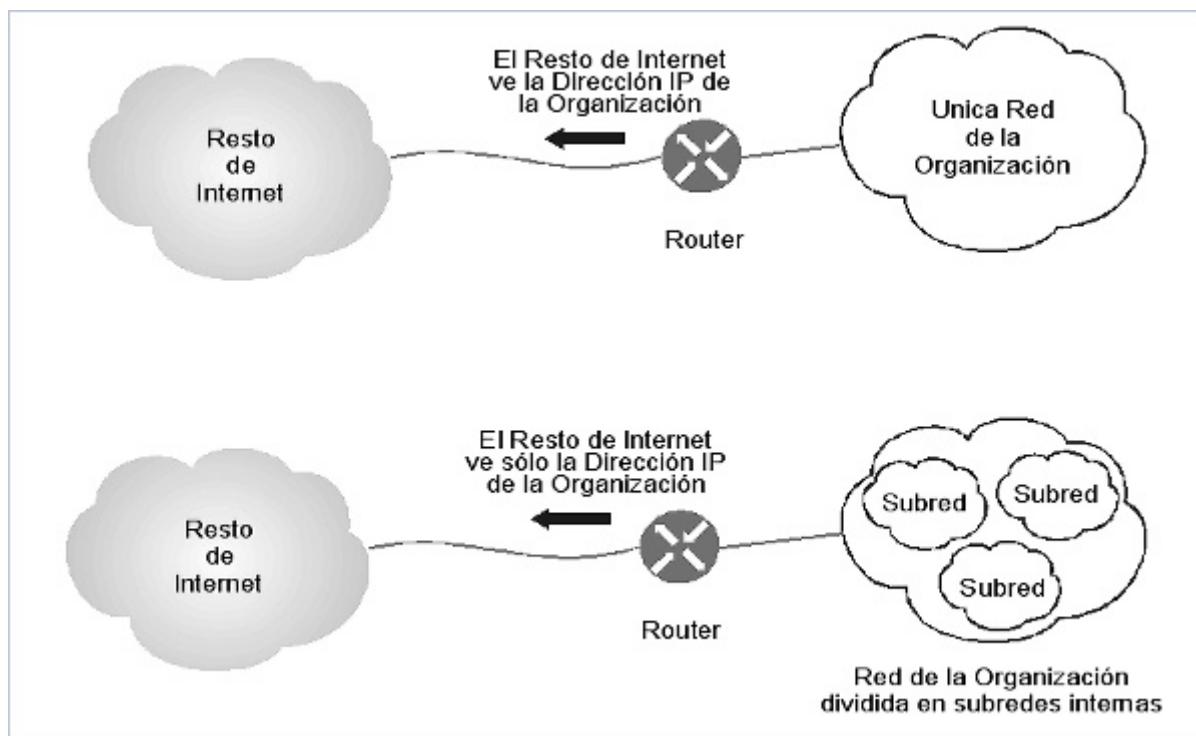
En 1985, surgió la RFC 950, que definió los procedimientos estándar para soportar el direccionamiento de subred.

**La idea principal que subyace detrás del direccionamiento de subred, es permitir al administrador de la red (también denominado sistema autónomo) que la subdivida en redes más pequeñas (denominadas subredes) según sean sus necesidades;** de esta forma, para el entorno exterior a la red, ésta seguirá siendo una sola red con una única dirección IP; sin embargo internamente estará subdividida en muchas subredes más pequeñas.

Al poder dividir un sistema autónomo en redes más pequeñas el administrador consigue:

- Mayor flexibilidad.
- Un uso más eficiente de las direcciones de red.
- Capacidad de manejar tráfico de broadcast o difusión (una difusión no puede atravesar un Router).

Observe que esta estrategia permite dar solución a los dos problemas antes mencionados: dado que externamente la red sigue siendo una sola con una única dirección IP, no crecerán las tablas de ruteo, y no será necesario agotar nuevas direcciones IP por parte de InterNic. Además, le brinda flexibilidad al administrador de la red para que la subdivida según las conveniencias de la organización a la que asiste.



"Red dividida en subredes internas" | El Resto de Internet "ve" sólo la Dirección IP de la Organización, independientemente de que la Red esté dividida en Subredes o no. Esto ayuda a mantener reducidas las Tablas de Rutas al no tener que asignar una dirección IP para cada subred dentro de la organización. También colabora evitando el agotamiento de las direcciones IP posibles.

El direccionamiento de subred permite solucionar los dos problemas mencionados al agregar un nuevo nivel de jerarquía a las dos ya existentes en las direcciones IP tradicionales.

## Cálculo de Subredes

La estructura estándar de una dirección IP puede ser localmente modificada usando bits de direcciones de host como bits de direcciones de red adicionales. Esencialmente, la "línea de división" entre los bits de direcciones de red y los bits de direcciones de host se corre, creando una red adicional, pero reduciendo el número máximo de host que pueden pertenecer a cada red. Estos nuevos bits definen una red dentro de la gran red, llamada "subred" (*subnet*).

Las organizaciones utilizan las subredes a fin de superar problemas topológicos u organizacionales.

Las subredes permiten descentralizar la administración del direccionamiento de los host. Con el esquema de direccionamiento estándar, una única administración es responsable de la gestión de las direcciones de host de toda la red. Con la división en subredes (*subnetting*), el administrador puede delegar asignaciones de direcciones a organizaciones más pequeñas, lo cual puede ser una política expeditiva o un requerimiento técnico.

La "*subnetting*" puede también ser usada para superar diferencias de hardware y limitaciones de distancias. Los router IP pueden enlazar redes físicas disímiles, pero sólo si cada una de las redes físicas tiene su propia dirección de red.

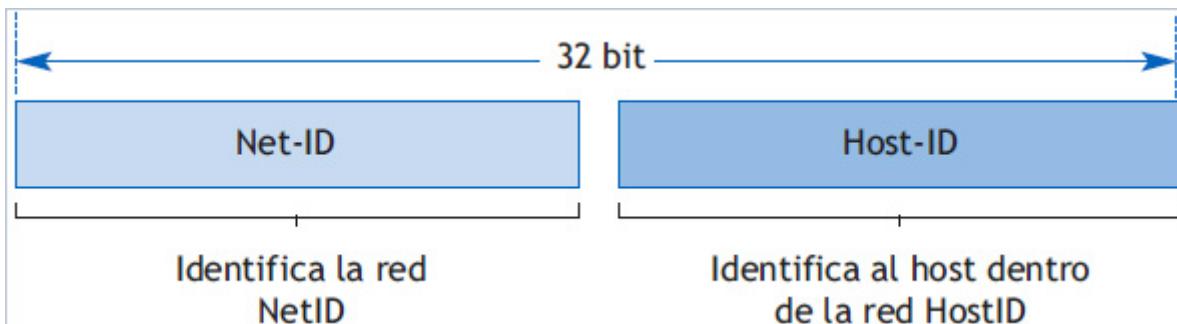
El "*Subnetting*" divide una única dirección de red en muchas direcciones de subredes únicas, de modo que cada red física puede tener su propia dirección única.

Una subred es definida aplicando una máscara de bit, la "máscara de subred", a la dirección IP. Si un bit en la máscara está en "on" (1), el bit equivalente en la dirección es interpretado como un bit de red. Si un bit en la máscara está en "off" (0), el bit corresponde a la parte de host de la dirección. La subred es sólo conocida localmente. Para el resto de la Internet, la dirección es interpretada como una dirección IP estándar.

Una dirección IP tradicional, tiene un doble nivel de jerarquía: el NetID y el HostID. El direccionamiento de subred permite utilizar parte del HostID como un elemento para identificar a las subredes. Observe que al utilizar una parte del HostID para identificar a las subredes, no se agregan bits a la dirección IP, la cual sigue siendo de 32 bits; de otra forma no hubiera habido compatibilidad en la versión IPv4.

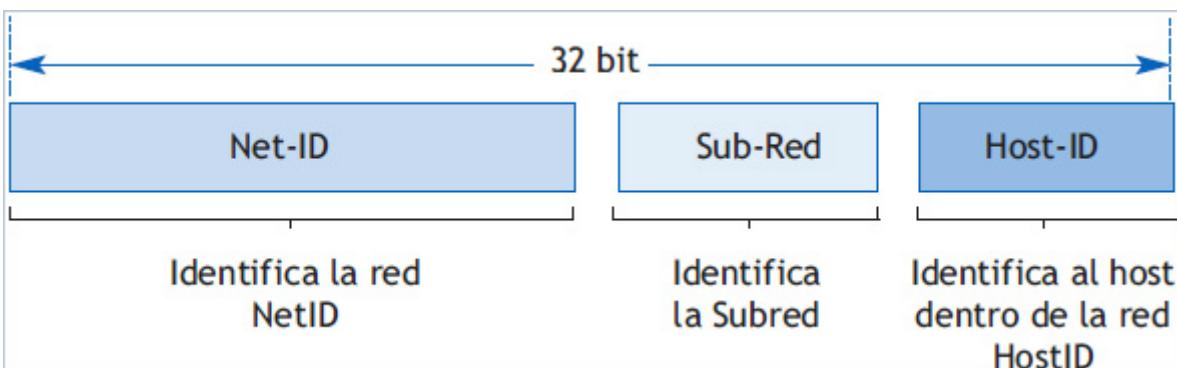
La siguiente figura ilustra cómo se implementa el nivel de tres jerarquías:

Esquema de jerarquía doble de la Dirección IP:



"Esquema de jerarquía doble de la Dirección IP" | *Elaboración propia*

Esquema de jerarquía triple de la Dirección IP:



"Esquema de jerarquía triple de la Dirección IP" | *Elaboración propia*

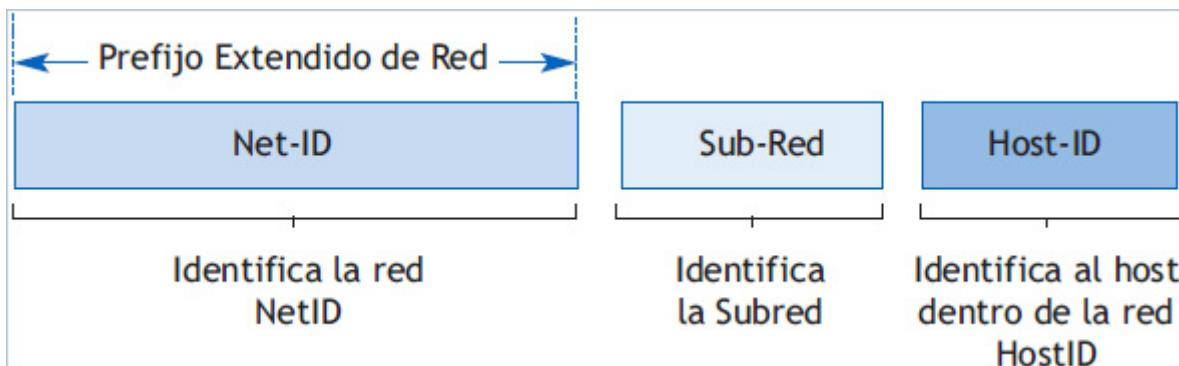
Para poder direccionar subredes internas, se utilizan los bits más significativos de la parte de Host del esquema de Jerarquía Doble, obteniéndose un esquema de Jerarquía Triple.

Obsérvese que el NetID en ambos esquemas jerárquicos no cambia, lo cual simplemente significa que no se cambiarán las tablas de ruteo en los Routers externos (los del resto de Internet). El hecho lógico de que parte del HostID se utilice internamente para identificar una subred y el resto para identificar un host particular dentro de ella es prerrogativa de la organización propietaria de la red y sus administradores.

Distinta es la situación dentro de la red. Allí sí tiene trascendencia el hecho de que exista un Identificador de Subred y de host. ¿Cómo se identifican las distintas subredes internas, cómo se identifican los hosts dentro de ellas? Esas son las cuestiones de las que nos ocuparemos en el resto de esta herramienta.

## Prefijo Extendido de red

Los Routers el NetID del destino para rutear el tráfico, los Routers internos de un entorno formado por subredes, necesitan más información que la provista por el NetID (ya que en todas las subredes tienen el mismo NetID). Para rutear tráfico interno entre subredes, los Routers utilizan el Prefijo Extendido de Red. El Prefijo Extendido de Red se compone del NetID + el Prefijo de Subred (el denominado Identificador de Red Interna en la figura anterior).



"Prefijo Extendido de red" | *Elaboración propia*

Los routers internos necesitan más información que la provista por el Net-ID, ya que éste es común a todas las subredes. Para efectuar el ruteo del tráfico, utilizan el Prefijo Extendido de Red, el cual incluye, además del Net-ID, el prefijo que identifica a la Subred.

Antes de continuar con un ejemplo debemos ver qué son las máscaras de red y de subred y una nomenclatura "más moderna" que la clasificación de direcciones en A, B y C.

## Las Máscaras de red

Como sabemos, un Router de Internet (o externo) sólo necesita conocer el NetID de la dirección IP para rutear el tráfico, pero el Router al recibir el paquete IP, recibe la secuencia de 32 bits correspondiente a la dirección IP completa del destino. ¿Cómo hace para extraer de ella sólo el NetID? Primero inspecciona los primeros bits de la cadena, para determinar qué tipo de dirección es (A, B o C); esto le proporciona información muy valiosa, ya que conociendo la clase de la dirección IP sabe cuántos bits corresponden al NetID. Recordemos que en el caso de una dirección clase A, el NetID ocupa los primeros 8 bits; en el caso de una clase B, los primeros 16 bits y en el caso de una C, los primeros 16 bits.

Supongamos que un router de Internet recibe la siguiente dirección IP de destino:

**10000000 . 00110000 . 00101000 . 01010000**

Inspecciona los primeros bits y, como encuentra la secuencia 10 al inicio, determina que la dirección es clase B. A partir de este momento "sabe" que los primeros 16 bits corresponden al NetID y los 16 restantes al HostID.

Más que "saber", en realidad lo que hace es aplicar una máscara de red compuesta por 32 bits de los cuales los primeros 16 serán 1 y los 16 últimos serán 0.

Máscara de red para direcciones clase B:

**11111111 . 11111111 . 00000000 . 00000000**

Haciendo el producto lógico (operación AND) entre la dirección IP y la máscara obtendrá el NetID del destino.

Dirección IP	11000000	00110000	00101000	01010000
Máscara de red	11111111	11111111	00000000	00000000
Resultado de la Operación	11000000	00110000	00000000	00000000

"operación AND" | *Elaboración autor*

Como era de esperar, el resultado de la operación da por resultado sólo el NetID buscado por el router.

La misma operación puede pensarse en términos de la notación decimal con puntos, en esta nomenclatura, la dirección IP destino es

**128 . 48 . 40 . 80**

Y la máscara de red es:

**255.255.0.0**

El resultado del producto lógico da por resultado 128. 48, que es el NetID buscado.

Obviamente que si el router hubiera identificado que la dirección era Clase A, hubiera aplicado una máscara de red con los primeros 8 bits iguales a 1 y los restantes iguales a 0, y que si el caso hubiera correspondido a una dirección clase C, la máscara de red hubiera estado compuesta por los primeros 24 bits iguales a 1 y los 8 restantes iguales a 0.

### Una nomenclatura más moderna para las clases de direcciones IP

Dado que los Routers de Internet necesitan establecer una máscara para obtener el NetID, es muy útil expresar las direcciones indicando "la cantidad de unos" que ésta debe tener.

De esta forma, como a una dirección clase A, por ejemplo 25.115.68.70 le corresponde una máscara con los 8 primeros bits iguales a 1, se la puede escribir como:

**25.115.68.70 / 8 (se lee "barra 8")**

De la misma forma para una dirección clase B como 135.87.90.200, la nueva notación sería:

**135.87.90.200 / 16**

Y para la dirección clase C, 208.32.168.93,

**208.32.168.93 / 24**

Si bien puede parecer que esta nueva nomenclatura no aporta nada nuevo, más allá de indicarnos a simple vista a qué clase pertenece la dirección; tiene poderosas ventajas cuando hablamos de ruteos internos, donde, como veremos, se deben utilizar máscaras de subred con cantidades de unos distintas de 8, 16 o 24; ya que deben incluirse no sólo los bits del NetID, sino también los del Prefijo de Subred.

### Cómo asignar las Direcciones de las Subredes

Supongamos que un administrador de Red solicita una dirección IP Clase B a InterNic, la cual le provee la dirección de Red: 131.15.0.0 o bien como hemos visto 131.15.0.0 / 16.

Si algún host externo remite un paquete IP a alguno de los hosts de este dominio, por ejemplo al

131.15.49.108, los Routers que se encargan de encaminar el mensaje a través de las distintas redes del mundo sólo necesitan conocer su NetID; por lo tanto, aplicarán una máscara de 16 bits iguales a 1 y 16 bits iguales a 0 (255.255.0.0), ya que es una dirección clase B.

Ahora veamos cómo puede dividirse este dominio en subredes internas.

Supongamos que el administrador de la red interna decide dividirla en 4 subredes. Como sabemos, deberá utilizar bits del HostID para codificarlas. Como pretende sólo 4 subredes, necesitará sólo 2 bits, (ya que si necesitara 8 subredes, hubiera requerido 3 bits).

Antes de continuar, observe que no puede subdividirse en 5 subredes ó 6 ó 14; dado que las subredes se codifican con bits siempre se obtendrán cantidades de subredes que son potencias de 2: subredes, subredes, subredes; subredes; etc. Claro que esto no significa que deba usarlas todas; por ejemplo, si necesita 14 subredes, utilizará 4 bits, con lo cual obtendrá en realidad 16 subredes, de las cuales utilizará las 14 que quería y dejará 2 para una posible expansión futura.

### Ahora continuemos con nuestro ejemplo.

Habíamos establecido que, como necesita 4 subredes, necesita usar 2 bits del HostID para codificarlas, con lo cual el Prefijo Extendido de Red (NetID + 2 bits del HostID que se usarán como identificadores de Subred) estará compuesto por los 18 primeros bits.

Aclaremos un poco las cosas.

La dirección de red es: **131.15.0.0 / 16**

Que escrita en bits es:

NetID		HostID	
131	15	0	0
10000011	00001111	00000000	00000000

"Que escrita en bits es" | *Elaboración propia*

El espacio completo de las direcciones posibles para esta red es (por ahora no compliquemos las cosas recordando que en realidad hay dos combinaciones de bits del HostID que no se pueden utilizar):

NetID		HostID	
10000011	00001111	xxxxxxxx	xxxxxxxx

"Direcciones posibles" | *Elaboración propia*

Para conformar las 4 subredes, el administrador tomará los 2 primeros bits del HostID para codificarlas:

NetID		HostID		
Prefijo Extendido de Red		Identificador del Host en la Subred		
NetID		Prefijo de Subred	Identificador del Host en a Subred	
10000011	00001111	xx	xxxxxx	xxxxxxxx
Primer Byte	Segundo Byte	Tercer Byte		Cuarto Byte

"2 primeros bits del HostID" | *Elaboración propia*

Las direcciones correspondientes a las 4 subredes internas se obtienen combinando los valores 0 y 1 en los dos bits correspondientes al Prefijo de Subred en la forma habitual:

00
01
10
11

"Prefijo de Subred en la forma habitual" | *Elaboración propia*

¿Cuáles serían entonces las direcciones en bits correspondientes a las 4 subredes? Tomando en cuenta que mantendremos la convención de dar el valor 0 a los bits que identifican a los hosts, como siempre hemos hecho a la hora de asignar direcciones a redes:

	Primer Byte	Segundo Byte	Tercer Byte	Cuarto Byte
Subred 0	10000011	00001111	00	000000
Subred 1	10000011	00001111	01	000000
Subred 2	10000011	00001111	10	000000
Subred 3	10000011	00001111	11	000000

"Direcciones en bits" | *Elaboración propia*

Llegó el momento de la pregunta clave: ¿de cuántos bits estará compuesta la máscara de subred?

De 18. Los 16 correspondientes al NetID + los 2 bits necesarios para codificar las subredes. Este hecho tomará gran trascendencia ahora, cuando escribamos las direcciones en nomenclatura decimal con puntos y agreguemos la barra (le aconsejo que realice las cuentas correspondientes para comprender en profundidad el proceso):

	<b>Primer Byte</b>	<b>Segundo Byte</b>	<b>Tercer Byte</b>	<b>Cuarto Byte</b>	
<b>Subred 0</b>	10000011	00001111	<b>00 000000</b>	00000000	131.15. <b>0</b> .0/18
<b>Subred 1</b>	10000011	00001111	<b>01 000000</b>	00000000	131.15. <b>64</b> .0/18
<b>Subred 2</b>	10000011	00001111	<b>10 000000</b>	00000000	131.15. <b>128</b> .0/18
<b>Subred 3</b>	10000011	00001111	<b>11 000000</b>	00000000	131.15. <b>192</b> .0/18

"De 18" | Elaboración propia

En el párrafo anterior se le indicó que tuviera muy en cuenta que la máscara de subred debía ser de 18 bits y que lo indicaríamos en la nomenclatura con barra, ¿dónde radica la importancia? Busque unos párrafos más arriba la dirección de la red en nomenclatura decimal con puntos, luego compárela con la dirección decimal con puntos de la Subred 0.

Seguramente la primera reacción sea decir: ¡son iguales!

Son iguales ... pero no son iguales. La dirección de la red hacia fuera (hacia el resto de Internet) tiene una máscara de red de 16 bits, su dirección es 131.15.0.0/16. La dirección de la subred 0, es una dirección interna y por lo tanto utiliza una máscara de 18 bits, con lo cual su dirección es: 131.15.0.0/18.

Aquí hay que hacer una aclaración muy importante: es obvio que para que no se produzca confusión, el Protocolo de Ruteo del router debe poder conocer la máscara utilizada; lamentablemente no todos los protocolos de ruteo utilizados en Internet la soportan.

Los protocolos que soportan la asignación de máscaras para cada dirección en su tabla de ruteo utilizan las técnicas de *Classless InterDomain Routing* (CIDR) o Ruteo Inter Dominio Sin Clases. Por ejemplo, un protocolo de ruteo muy difundido (hoy algo antiguo), el RIP (*Routing Information Protocol* – Protocolo de Información de Ruteo) o RIP-1, como se lo conoce ahora, no acepta máscaras de red distintas para cada dirección que almacena en sus tablas de ruteo. Entre los que sí las soportan tenemos a BGP-4 (*Border Gate-way Protocol* o Protocolo de Pasarela Exterior; RFC 1771), RIP-2 (RFC 1723), OSPF (Open Shortest Path First, Abrir Primero la Trayectoria más Corta) y el IS-IS.

Aunque parezca incómodo no hay forma de que un router que soporte máscaras de red para cada dirección almacenada se confunda: si hablamos de un router externo, éste utiliza una máscara de red de 16 bits; si hablamos de un router interno, utiliza una máscara de red (o de subred) de 18 bits para el ruteo interno. Las máscaras internas las decide y fija el administrador de la red, así que la única forma de que se genere una confusión es que el administrador se confunda al establecer la máscara de red interna.

Possiblemente administrará alguna red, por lo tanto, debemos procurar que no se confunda, así que debo agregar un detalle técnico más: lamentablemente los Routers de la actualidad no reciben las direcciones con la /, esto no está incluido en el protocolo IP actual (IPv4), así que lo que nos resulta útil a los humanos no lo es para los Routers. Los Routers siguen usando las máscaras de red, así que deberemos explicitar bit a bit y en notación decimal la máscara de subred que utilizaremos internamente. Es sencillo.

Como habíamos establecido, la máscara de subred interna, debe tener los primeros 18 bits en 1 y los 14 restantes en 0, así que en bits será:

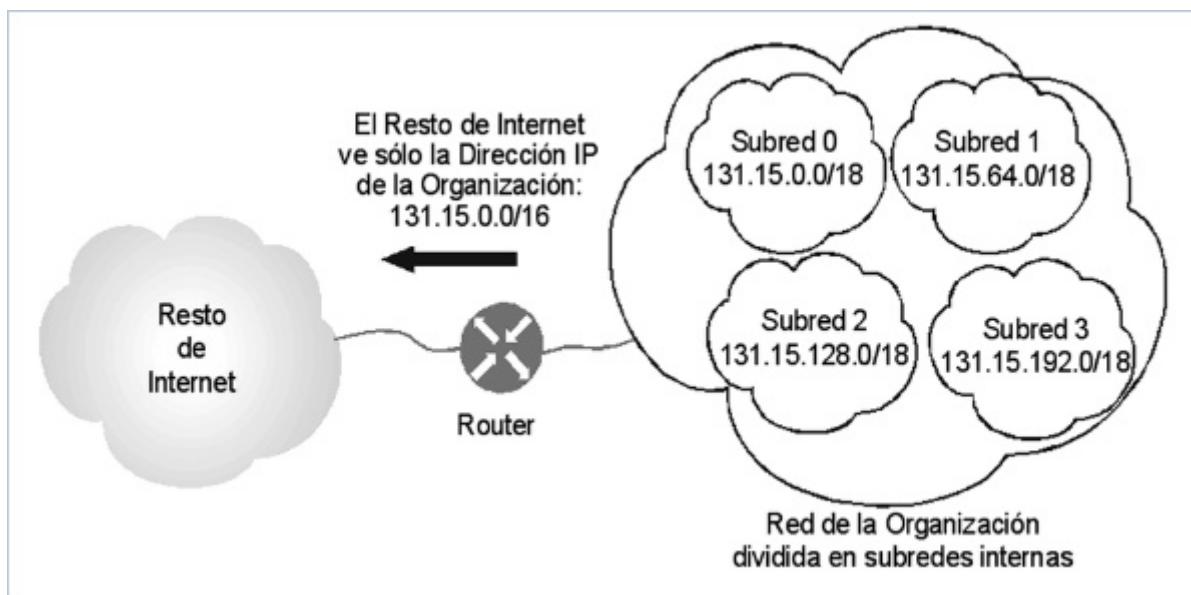
**11111111.11111111.11000000.00000000**

Convertiendo a la nomenclatura decimal con puntos obtenemos:

**255.255.192.0**

Ésta es la máscara de red (o subred) que utilizarán los Routers para rutear internamente.

La siguiente figura resume lo dicho anteriormente:

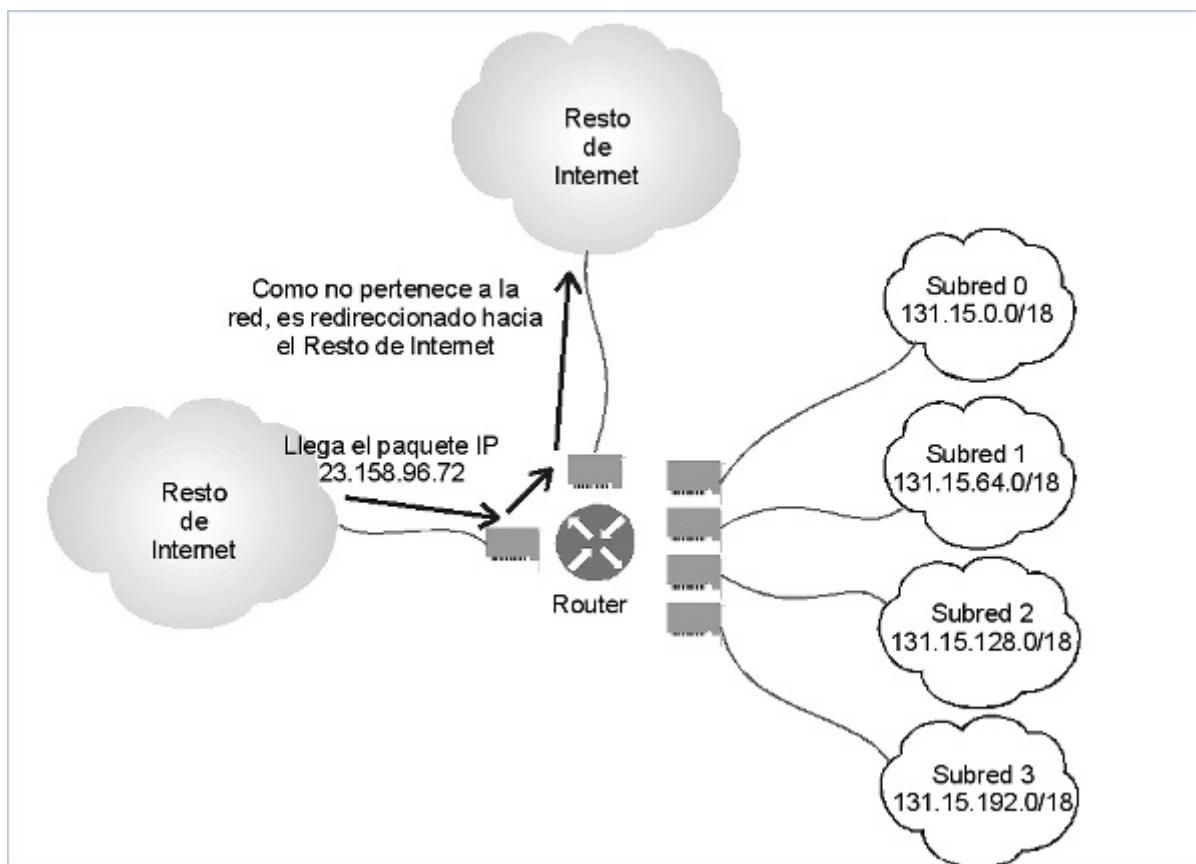


"Red de la Organización dividida en subredes internas" | Cuando rutea paquetes IP internos, el Router aplica una máscara de red de 18 bits (255.255.192.0), esto le permite direccionar 4 subredes internas. Para el resto de Internet, sigue siendo una única red, cuya dirección IP es 131.15.0.0/16, a la cual rutean aplicando una máscara de 16 bits (255.255.0.0).

Para completar el concepto supongamos que desde el resto de Internet llega un paquete IP, dirigido a otra red; supongamos uno con dirección IP 23.158.96.72, el Router detecta que es una dirección tipo A, le aplica una máscara apropiada, es decir, una que tiene los 8 primeros bits iguales a 1 (255.0.0.0); efectuando la operación AND, extrae el NetID destino del paquete, obteniendo 23. Busca en su tabla de ruteo y lo deriva hacia el router adecuado para que el paquete siga camino. Si le resulta incómodo no saber físicamente cómo lo rutea, puede pensar que el router está conectado a 6 placas de red, como se muestra en la figura siguiente.

Ahora supongamos que al router le llega un paquete dirigido a un host de la red, digamos que la dirección IP de destino es 131.15.72.128. El router detecta que es una dirección clase B, y le aplica una máscara apropiada para extraer el NetID. La máscara utilizada será 255.255.0.0. El NetID obtenido es 131.15, con lo cual el Router se da cuenta de que pertenece a un host de la red. Para remitirlo internamente aplica la máscara definida por el administrador de red, es decir la máscara de 18 bits:

- Dirección IP destino: 131.15.72.128 = 10000011 . 00001111 . 01001000 . 10000000
- Máscara aplicada: 255.255.192.0 = 11111111 . 11111111 . 11000000 . 00000000
- Dirección de Subred obtenida (AND) = 10000011 . 00001111 . 01000000 . 00000000



Esta dirección no es otra que la dirección de la Subred 1, 131.15.64.0 / 18. Por ende, el *router* ha determinado que el host destino se encuentra en la subred 1 y hacia ella rutea el paquete IP (si quiere algo más de precisión, digamos que una vez que sabe a qué subred debe dirigir el paquete, busca en su tabla interna la dirección MAC o de hardware asociada a ella y utilizando la placa de red correspondiente envía el paquete encapsulado en una trama con el formato adecuado a la tecnología de la subred, por ejemplo Ethernet. Otra versión reemplazaría las 4 placas de red internas por una conexión a un switch, el cual con la dirección MAC distribuiría la trama.)

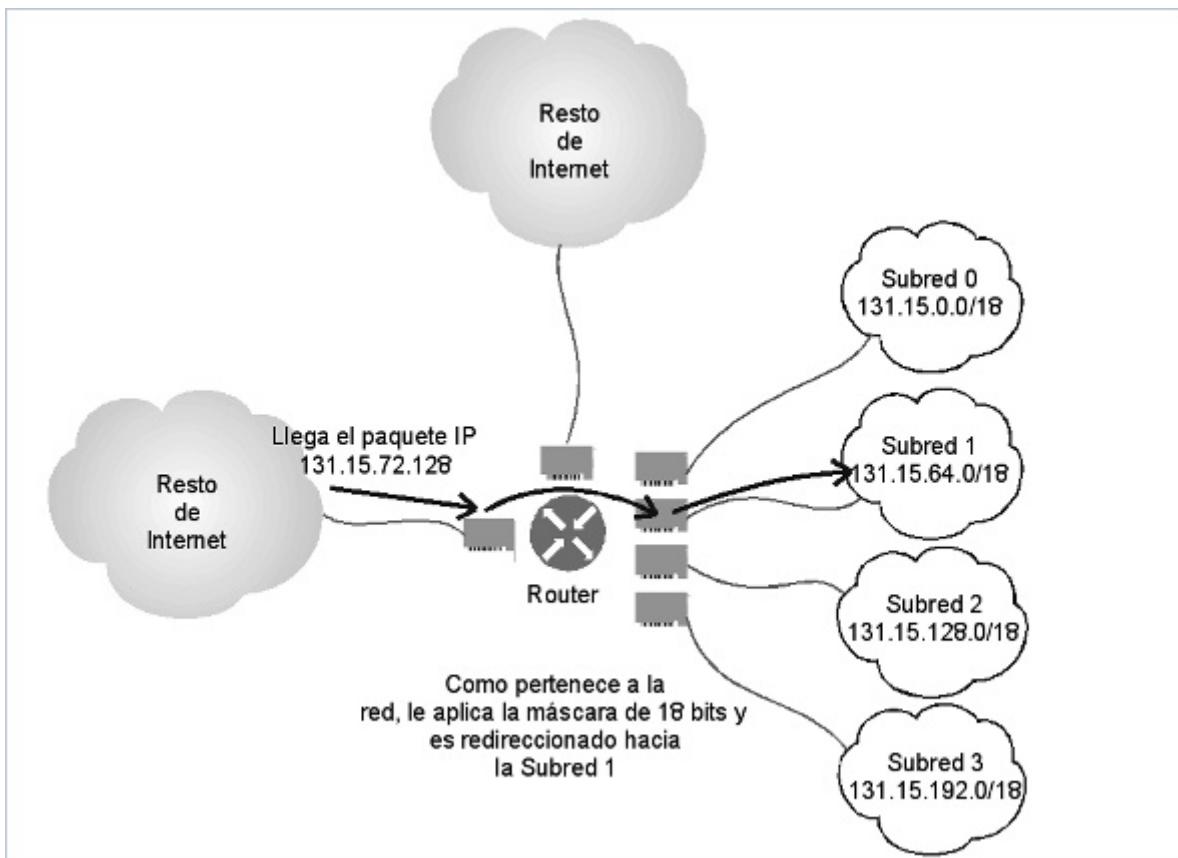
Siguiendo la práctica habitual al asignar direcciones IP a los host que participarán en comunicaciones vía Internet, se reservarán el identificador de host con todos los valores iguales a 0 para identificar la red (o subred) y el correspondiente a todos los valores iguales a 1 para identificar la difusión dentro de la subred.

De esta forma la cantidad de hosts en una subred será igual a  $(2^n - 2)$ , siendo n la cantidad de bits asignados para identificar los hosts dentro de cada subred.

En nuestro ejemplo disponemos de 14 bits para identificar los hosts de cada subred, con lo cual cada subred podrá contar con:

$$2^{14} - 2 = 16382 \text{ Host}$$

¿Cómo asignar las Direcciones de los hosts en cada Subred?



"Asignar Direcciones de host en cada Subred" | *Como pertenece a la red, le aplica la máscara de 18 bits y es redireccionado a la Subred 1.*

Veamos algunas de las direcciones correspondientes a host de la Subred 0:

Subred 0: 10000011.00001111.00000000.00000000 = 131.15.0.0 /18

Host 1 : 10000011.00001111.00000000.00000001 = 131.15.0.1 /18

Host 2 : 10000011.00001111.00000000.00000010 = 131.15.0.2 /18

Host 3 : 10000011.00001111.00000000.00000011 = 131.15.0.3 /18

Host 4 : 10000011.00001111.00000000.00000100 = 131.15.0.4 /18

Host 15 : 10000011.00001111.00000000.00001111 = 131.15.0.15 /18

Host 16 : 10000011.00001111.00000000.00010000 = 131.15.0.16 /18

Host 16382: 10000011.00001111.00111111.11111110=131.15.63.254/18

**Por último:**

Dirección de difusión dentro de la Subred 0:

10000011.00001111.00111111.11111111 =

131.15.63.255 /18

Obsérvese que una forma práctica para determinar los bits correspondientes al host es simplemente convertir a binario el número de identificación del host, así por ejemplo al host número 15, cuya representación binaria es 1111, se le asigna esta combinación, escribiéndolo siempre en el conjunto de bits más bajo (los de la

derecha).

## Consideraciones para diseñar Subredes

Diseñar redes y subredes requiere una planificación cuidadosa por parte del administrador de red. Las siguientes son las cuatro preguntas fundamentales a las que se debe dar respuesta antes de comenzar a inventar subredes dentro de una organización; no dar una precisa respuesta a ellas sólo puede acarrearle dolores de cabeza en el futuro.

- ¿Cuántas subredes necesita la organización hoy?
- ¿Cuántas subredes necesitará en el futuro?
- ¿Cuál es la máxima cantidad de hosts (en la subred más grande) que necesita hoy la organización?
- ¿Cuál será la máxima cantidad de hosts (en la subred más grande) que necesitará la organización en el futuro?



¿Estás listo para un desafío?

**1. Indique la opción correcta**

La idea principal que subyace detrás del direccionamiento de subred, es permitir al administrador de la red (también denominado sistema autónomo) que la subdivida en redes más pequeñas (denominadas subredes) según sean sus necesidades.

- Verdadero
- Falso

**2. Indique la opción correcta**

El direccionamiento de subred permite solucionar problemas al agregar un nuevo nivel de jerarquía a las dos ya existentes en las direcciones IP tradicionales.

- Verdadero
- Falso

**3. Indique la opción correcta**

Una subred es definida aplicando una máscara de bit, la "máscara de subred", a la dirección IP.

- Verdadero
- Falso

**4. Indique la opción correcta**

Los protocolos que soportan la asignación de máscaras para cada dirección en su tabla de ruteo utilizan las técnicas de Classless InterDomain Routing (CIDR) o Ruteo Inter Dominio Sin Clases.

- Verdadero
- Falso

**5. Indique la opción correcta**

Si un router identifica que una dirección es Clase B:

- Aplica una máscara de red con los primeros 8 bits iguales a 1 y los restantes iguales a 0.
- Aplica una máscara de red con los primeros 16 bits iguales a 1 y los restantes iguales a 0.

- Aplica una máscara de red con los primeros 24 bits iguales a 1 y los 8 restantes iguales a 0.
- Aplica una máscara de red con los todos los bits iguales a 1 y ningún bit igual a 0.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Las subredes	permiten rutear el tráfico interno entre subredes
Los prefijos extendidos de red	permiten descentralizar la administración del direccionamiento de los host
Los protocolos que soportan asignación de máscaras	utilizan técnicas CIDR

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

La idea principal que subyace detrás del direccionamiento de subred, es permitir al administrador de la red (también denominado sistema autónomo) que la subdivida en redes más pequeñas (denominadas subredes) según sean sus necesidades.

- Verdadero
- Falso

## 2. Indique la opción correcta

El direccionamiento de subred permite solucionar problemas al agregar un nuevo nivel de jerarquía a las dos ya existentes en las direcciones IP tradicionales.

- Verdadero
- Falso

## 3. Indique la opción correcta

Una subred es definida aplicando una máscara de bit, la "máscara de subred", a la dirección IP.

- Verdadero
- Falso

## 4. Indique la opción correcta

Los protocolos que soportan la asignación de máscaras para cada dirección en su tabla de ruteo utilizan las técnicas de Classless InterDomain Routing (CIDR) o Ruteo Inter Dominio Sin Clases.

- Verdadero
- Falso

## 5. Indique la opción correcta

Si un router identifica que una dirección es Clase B:

- Aplica una máscara de red con los primeros 8 bits iguales a 1 y los restantes iguales a 0.
- Aplica una máscara de red con los primeros 16 bits iguales a 1 y los restantes iguales a 0.
- Aplica una máscara de red con los primeros 24 bits iguales a 1 y los 8 restantes iguales a 0.
- Aplica una máscara de red con los todos los bits iguales a 1 y ningún bit igual a 0.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Las subredes	permiten descentralizar la administración del direccionamiento de los host
Los prefijos extendidos de red	permiten rutear el tráfico interno entre subredes
Los protocolos que soportan asignación de máscaras	utilizan técnicas CIDR



## SP9 / H3: VLSM: máscaras de subred de longitud variable

Seguramente coincidiremos en que la implementación de una máscara de Subred al permitir fragmentar un único dominio autónomo en varias subredes es un gran avance. Esto otorga flexibilidad al administrador para crear subredes dentro de una organización, según el criterio que estime más conveniente: por áreas, grupos de trabajo e inclusive por niveles de seguridad.

Sin embargo, es muy posible que aun así se siga haciendo una mala asignación de un recurso escaso y valioso: las direcciones IP. Si por ejemplo, al dividir una red clase C en subredes, la subred más grande que se piensa implementar consta de 30 hosts, En base a ese valor, tomando 3 bits, habrá conformado seguramente 8 subredes ( $2^3=8$ ) de 32 hosts= ( $2^5 =32$ ).

Siguiendo la práctica habitual se reservará el identificador de host con todos los valores iguales a 0 para identificar la red o subred y el identificador de host con todos los valores iguales a 1 para identificar la difusión dentro de la red o subred. Por lo cual para cada subred en realidad solo pueden utilizarse 30 números.

Pero observe que esta decisión lo ha obligado a diseñar a todas las subredes con 30 máquinas, aunque hubiera otras en las que sólo necesitara menos.

Necesariamente en esas redes que poseerán menos host, se estarán desperdiando direcciones IP.

Esto se debe a que hemos trabajado con una única máscara de subred, y esto automáticamente hace que todas dispongan de la misma cantidad de hosts posibles conectados a ella.

El próximo paso, como seguramente estará previendo, es utilizar distintas máscaras de subred, de tal forma que puedan direccionarse subredes de distinto tamaño. Éstas serán las Máscaras de Subred de Longitud Variable VLSM, definidas en la RFC 1009.

Antes de avanzar, quiero recordarle que el protocolo de ruteo RIP o RIP v1 mencionado anteriormente, al no agregar información concerniente a las máscaras de subred, permite utilizar sólo una máscara de subred, y, por lo tanto, no será útil para implementar VLSM.

Las dos grandes ventajas de implementar VLSM son:

1. Permite hacer un uso más eficiente del espacio de direcciones IP dentro de una organización.
2. Consigue reducir la cantidad de información requerida para el ruteo, al proporcionar un mejor nivel de agregación de las rutas dentro del dominio al permitir una división recursiva del espacio de direcciones IP dentro de la organización.

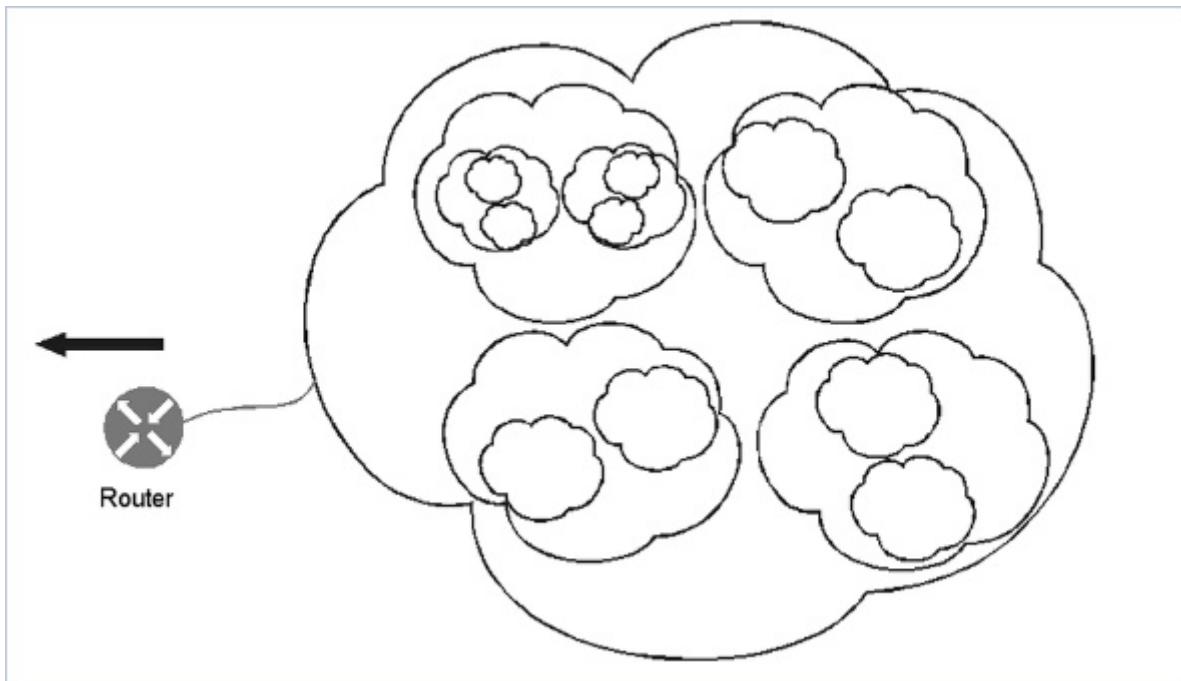
### La idea principal en VLSM

La idea que subyace en VLSM es la siguiente: hasta ahora hemos aprendido a dividir a una red que "nos quedaba grande" en varias subredes más pequeñas; si aun así, algunas de las subredes "nos siguen quedando grandes", las seguimos dividiendo en sub-sub redes.

¿Y si algunas de las sub - sub - redes son, todavía, demasiado grandes?, nuevamente la subdividimos en sub - sub -sub -redes. ¡Como si fuera una muñeca rusa, que al abrirla tiene otra muñeca, y dentro de ésta se encuentra otra, y así sucesivamente!

Cada nuevo nivel de división se dice que es una desagregación de la red (o subred) del nivel superior. Si bien podemos seguir así hasta el infinito, obviamente estaremos limitados por las cantidad de bit que podemos "pedir prestados" a la porción de Host.

El diseño recursivo en VLSM se muestra en la figura siguiente.



"Diseño recursivo en VLSM" | Red de la organización dividida en subredes internas, las cuales a su vez se dividen en sub-subredes, algunas de las cuales se desagregan en otro nivel de subredes.

Supongamos que a una organización cuyo dominio es **153.44.0.0/16**, vamos a dividirla en 4 subredes de nivel 1. Para ello necesitamos sólo 2 bits, con la cual la máscara será /18. Las 4 direcciones para estas subredes de nivel 1 serán (le recomendamos que realice los cálculos pertinentes para repasar):

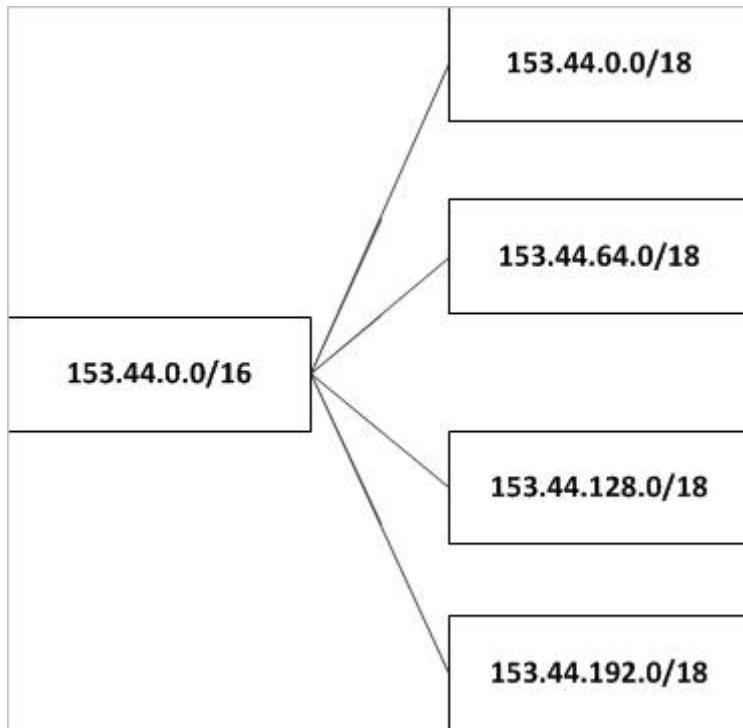
**153.44.0.0/18**

**153.44.64.0/18**

**153.44.128.0/18**

**153.44.192.0/18**

Como se muestra en la figura:



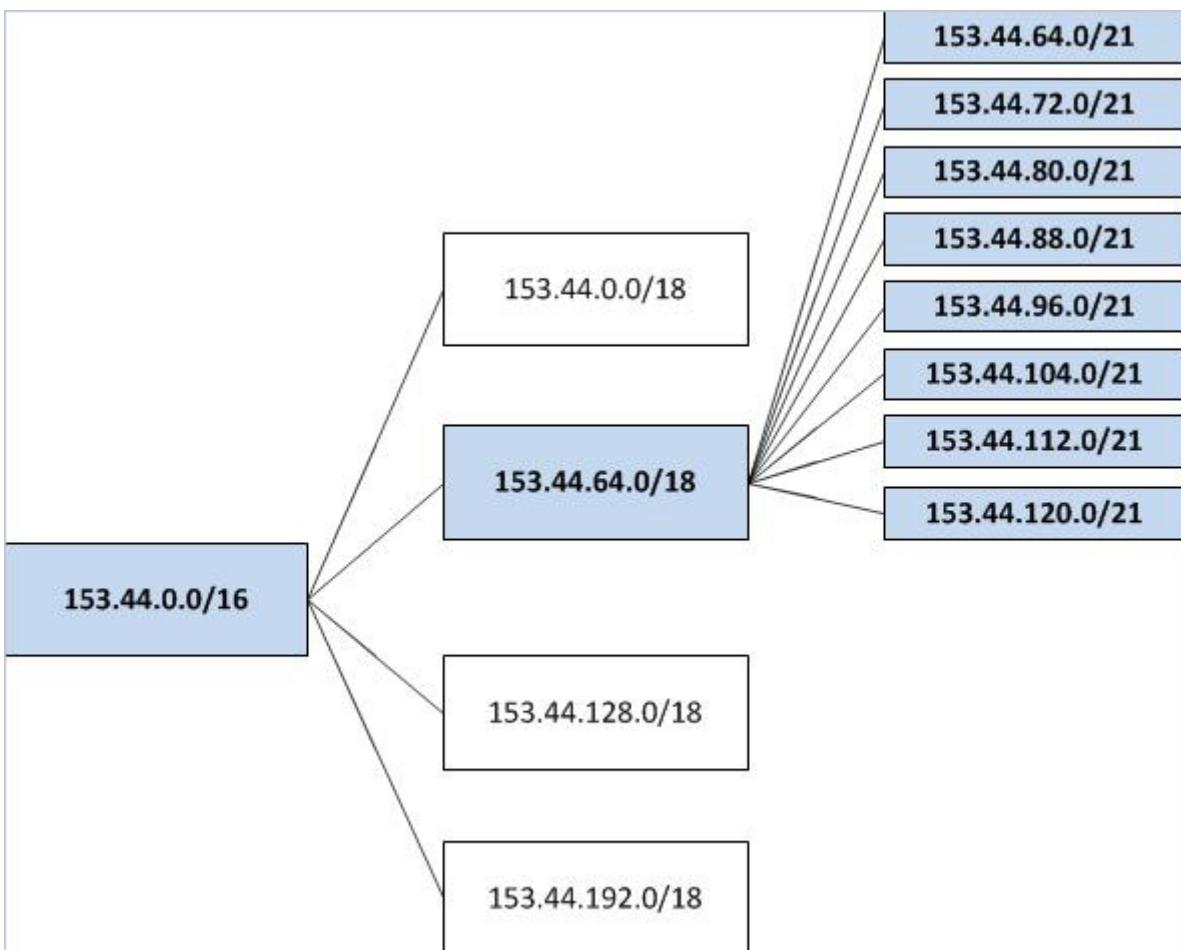
"4 subredes clase B" | *Elaboración propia Autor*

Supongamos que a la subred 2, 153.44.64.0/18 decidimos desagregarla en 8 subredes de nivel 2. Para ello necesitaremos 3 bits, con lo cual la máscara deberá poseer  $18 + 3 = 21$  bits.

Las 8 subredes en que se han desagregado serán (realice los cálculos):

- 153.44.64.0/21**
- 153.44.72.0/21**
- 153.44.80.0/21**
- 153.44.88.0/21**
- 153.44.96.0/21**
- 153.44.104.0/21**
- 153.44.112.0/21**
- 153.44.120.0/21**

Las que podemos disponer como se muestra en la siguiente figura:



"4 y 8 subredes clase B" | Elaboración propia Autor

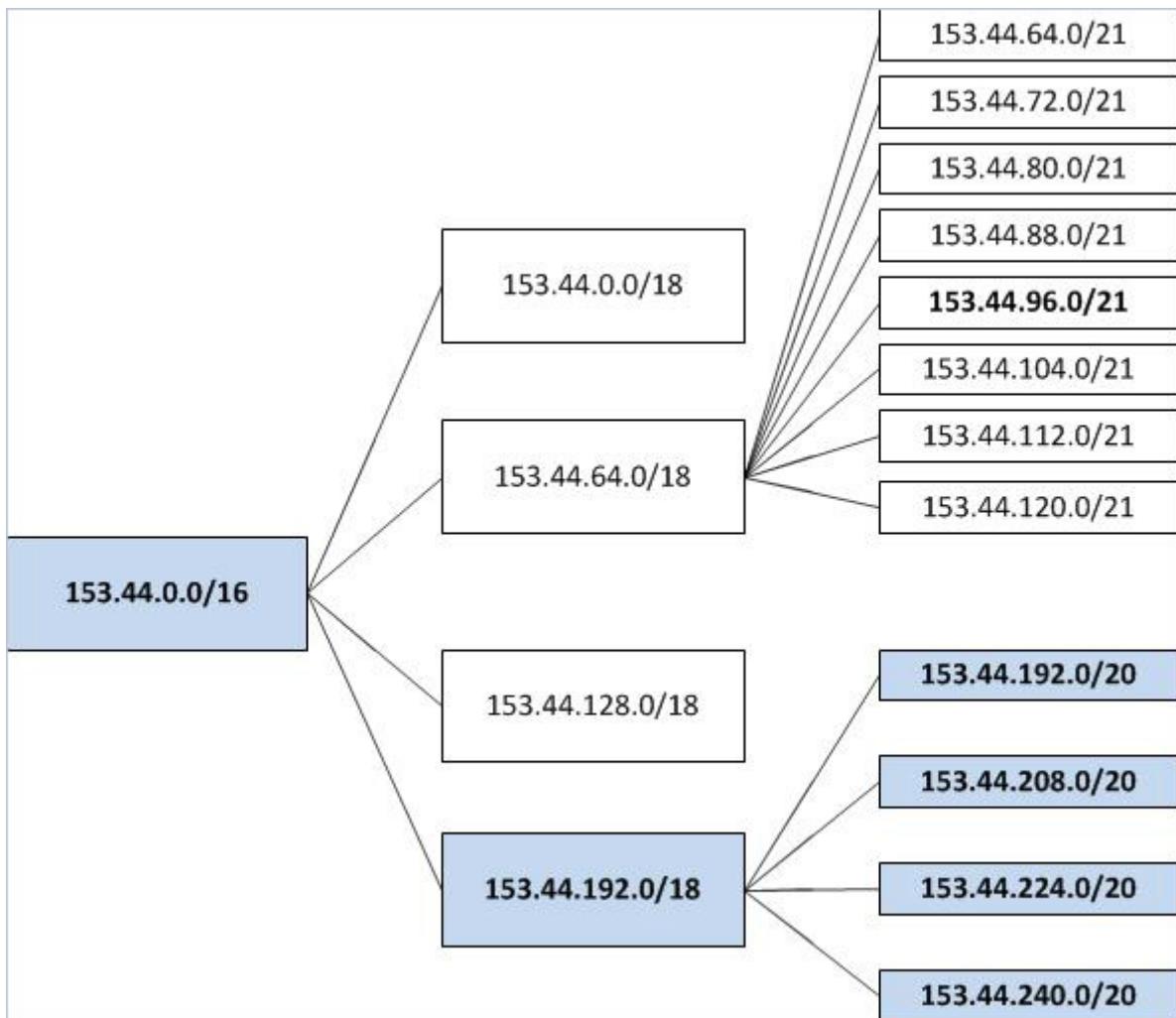
Supongamos también que otra de las subredes de nivel 1, la cuarta (153.44.192.0/18), se desagrega en 4 subredes de nivel 2. Necesitaremos 2 bits para poder hacerlo, con lo cual el prefijo será de  $18 + 2 = 20$  bits.

Observe que mediante la aplicación de este proceso recursivo no es necesario que los prefijos (o las máscaras) del mismo nivel tengan la misma cantidad de bits, el anterior era de 21 y éste es de 20.

Las direcciones de estas nuevas subredes de nivel 2 son (deberá, realizar los cálculos):

153.44.192.0/20  
 153.44.208.0/20  
 153.44.224.0/20  
 153.44.240.0/20

Las correspondientes subredes con estos números asignados se muestran en la siguiente figura:

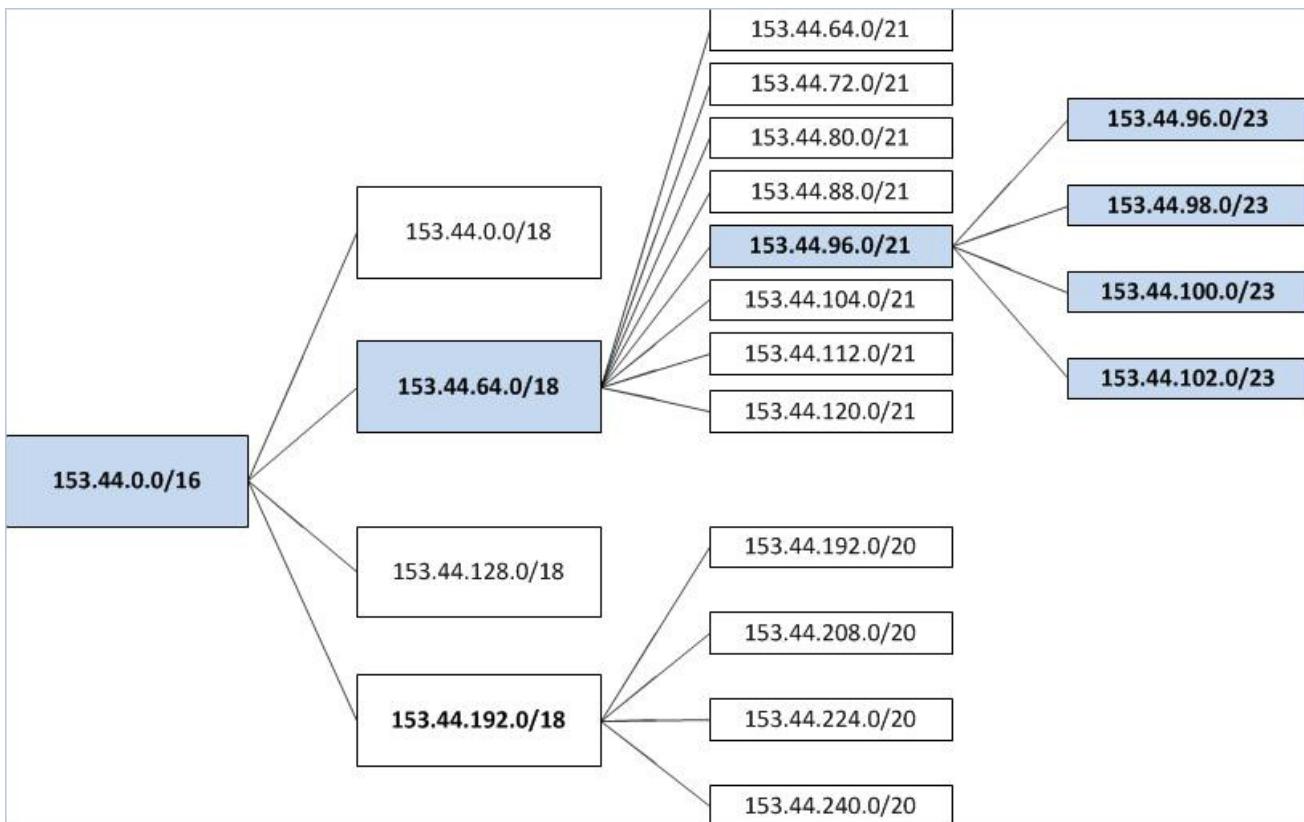


"4 8 y 4 subredes de clase B" | Elaboración propia Autor

Profundicemos un poco más el ejemplo, tomemos una de las subredes de nivel 2, por ejemplo la 153.44.96.0/21 y dividámosla en 4 subredes. Nuevamente necesitaremos 2 bits más para el prefijo, el cual pasará a ser de 23 bits. Las direcciones de cada una de estas subredes de tercer nivel de profundidad serán:

**153.44.96.0/23**  
**153.44.98.0/23**  
**153.44.100.0/23**  
**153.44.102.0/23**

Las agregamos al diagrama:

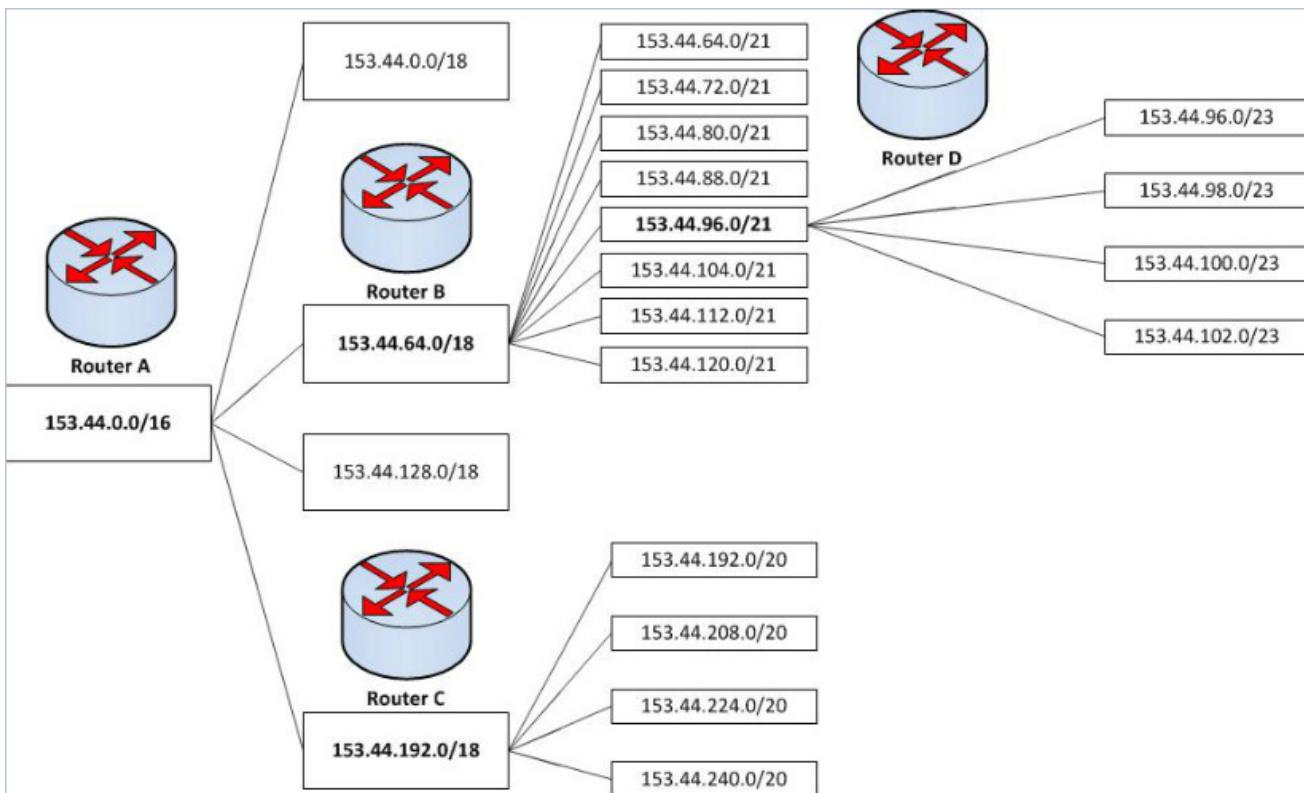


"4 4 y 8 subredes clase B" | Elaboración propia Autor

Nota: Si bien con lo visto hasta aquí usted está en condiciones de armar subredes correctamente, es útil utilizar programas que agilicen el cálculo de subredes, cantidad de hosts, máscaras a utilizar, etc; algunos de ellos están disponibles on-line y su utilización es libre y abierta a sugerencias de mejoría, como por ejemplo la siguiente:  
*Calculadora de subnetting on-line* <http://jodies.de/ipcalc>

## Reducción de tablas de ruteo

La figura que sigue mostrará cómo VLSM permite reducir el tamaño de las tablas de ruteo internas de la organización, simplemente mostraremos la ubicación de los Routers:



"Ubicación de los routers" | Fuente: elaboración Autor

¿Por qué decimos que VLSM reduce las tablas de ruteo de la red interna?

Observe la figura anterior: el router D, por ejemplo "resume" en una única dirección el acceso a las 4 subredes conectadas a él, de la misma forma el router C "oculta" las direcciones correspondientes a "sus" 4 subredes y el router B resume en su dirección a las 8 subredes que dependen de él. Por supuesto que el router A oculta toda esta organización en subredes al resto de Internet, de tal forma que puede accederse a cualquiera de las subredes mediante la única dirección IP de la organización.

Cuando decimos "resume" u "oculta" queremos significar que el router no anuncia a sus vecinos todas las direcciones de las subredes que de él dependen, sino sólo la dirección que le corresponde a él junto con la longitud del prefijo o la máscara de red que le corresponde, y esto reduce el tamaño de las tablas de ruteo de los Routers vecinos.

## Requisitos para implementar VLSM

Para implementar exitosamente VLSM en una organización se deben tener en cuenta los siguientes ítems:

- Los protocolos de ruteo deben soportar el prefijo extendido de red en cada entrada de las tablas de ruteo y en los anuncios a otros Routers.
- Todos los Routers deben implementar un algoritmo de envío de anuncios basado en la "equivalencia o correspondencia más larga (*longest match*)".
- Para que las tablas de ruteo se mantengan reducidas y se produzcan los niveles de agregación, las direcciones deben asignarse sobre una topología jerárquica.

## **Los protocolos de ruteo deben soportar el prefijo extendido de red**

Los protocolos de ruteo modernos como OSPF, I-IS-IS, o RIP-2 remiten el largo del prefijo extendido de red o la máscara correspondiente) cuando anuncian las rutas a los Routers vecinos, por lo cual permiten implementar VLSM.

**Todos los Routers deben implementar un algoritmo de envío de anuncios basado en la "equivalencia o correspondencia más larga (*longest match*)".**

Basémonos en el ejemplo dado anteriormente y supongamos que se debe remitir un paquete a la dirección IP: **153.44.104.7**. Supongamos que en la tabla de ruteo se encuentren los siguientes posibles destinos concordantes o equivalentes:

153.44.64.0/18

153.44.96.0/21

153.44.104.0/23

El algoritmo debe elegir el destino que tenga una **concordancia mayor**, es decir, **con el cual concuerde una mayor cantidad de bits**. En este caso, el elegido sería el último. Se han destacado los bits en los cuales concuerdan el destino deseado con los posibles ruteos:

153.44.104.7 = **10011001 . 00101100 . 01101000 . 00000111**

153.44.64.0/18 = **10011001 . 00101100 . 01000000 . 00000000**

153.44.96.0/21 = **10011001 . 00101100 . 01100000 . 00000000**

153.44.104.0/23 = **10011001 . 00101100 . 01101000 . 00000000**

Como se puede apreciar, es el último el que presenta la mayor cantidad de bits de concordancia, y por lo tanto debe ser el elegido. Observe nuestro esquema de red interna y podrá ver que es la subred a la que pertenece el host destino.

## **Las direcciones deben asignarse sobre una topología jerárquica**

La asignación de direcciones a las subredes debe hacerse en forma jerárquica, como lo hicimos en el ejemplo, de tal forma que haya correspondencia entre la organización lógica de las direcciones y la topología física de la red. De otra forma sería imposible reducir las tablas de ruteo.



¡Vamos a comprobar cuánto aprendiste!

**1. Indique la opción correcta**

Mediante la aplicación de VLSM, las máscaras tienen longitud variable.

- Verdadero
- Falso

**2. Indique la opción correcta**

La ventaja principal de implementar VLSM es:

- Permite hacer un uso más eficiente del espacio de direcciones IP.
- Permite reducir la cantidad de información requerida para el ruteo.
- Todas las anteriores.
- Ninguna de las anteriores.

**3. Indique la opción correcta**

Para implementar VLSM se debe tener en cuenta lo siguiente:

- Los protocolos de ruteo deben soportar el prefijo extendido de red.
- Los Routers deben implementar un algoritmo de envío de anuncios basado en la equivalencia o correspondencia más larga.
- Para que las tablas de ruteo se mantengan reducidas, las direcciones deben asignarse sobre una topología jerárquica.
- Todas las anteriores.

**4. Indique la opción correcta**

Supongamos que a una organización cuyo dominio es 193.44.0.0, vamos a dividirla en 4 subredes de nivel 1. La máscara será

- /2
- /4
- /18
- /26

**5. Indique la opción correcta**

Para poder disminuir las tablas de ruteo, la asignación de direcciones a las subredes debe hacerse en forma:

- Binaria.
- Aleatoria.
- Lineal.
- Jerárquica.

**6. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

El router	permite hacer un uso más eficiente del espacio de direcciones IP
VLSM	debe asignarse sobre una topología jerárquica
El protocolo de ruteo	debe soportar el prefijo extendido de red en cada entrada de las tablas
La dirección	resume en una única dirección el acceso a las subredes conectadas a él

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Mediante la aplicación de VLSM, las máscaras tienen longitud variable.

Verdadero

Falso

## 2. Indique la opción correcta

La ventaja principal de implementar VLSM es:

Permite hacer un uso más eficiente del espacio de direcciones IP.

Permite reducir la cantidad de información requerida para el ruteo.

Todas las anteriores.

Ninguna de las anteriores.

## 3. Indique la opción correcta

Para implementar VLSM se debe tener en cuenta lo siguiente:

Los protocolos de ruteo deben soportar el prefijo extendido de red.

Los Routers deben implementar un algoritmo de envío de anuncios basado en la equivalencia o correspondencia más larga.

Para que las tablas de ruteo se mantengan reducidas, las direcciones deben asignarse sobre una topología jerárquica.

Todas las anteriores.

## 4. Indique la opción correcta

Supongamos que a una organización cuyo dominio es 193.44.0.0, vamos a dividirla en 4 subredes de nivel 1. La máscara será

/2

/4

/18

/26

## 5. Indique la opción correcta

Para poder disminuir las tablas de ruteo, la asignación de direcciones a las subredes debe hacerse en forma:

Binaria.

Aleatoria.

Lineal.

Jerárquica.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

El router

resume en una única dirección el acceso  
a las subredes conectadas a él

VLSM

El protocolo de  
ruteo

La dirección

permite hacer un uso más eficiente del espacio de direcciones IP  
debe soportar el prefijo extendido de red en cada entrada de las tablas  
debe asignarse sobre una topología jerárquica

## SP9 / H4: Direccionamiento de superred (CIDR)

Hemos visto cómo el direccionamiento de Subred, en todas sus variantes, aunque particularmente VLSM, permite un mejor aprovechamiento de las direcciones IP (ya que hacen innecesario que una organización solicite varios dominios por el sólo hecho de poseer varias redes internas). Éste es un recurso a nivel interno de cada organización; sin embargo, con lo visto hasta ahora, parte del problema se mantiene: a las organizaciones se les debe asignar una dirección IP de clase A, B o C.

Recordemos que el gran "hueco" que se produce entre la cantidad de hosts que se pueden direccionar con las distintas clases hace que muchas organizaciones "desperdician" gran cantidad de direcciones IP, ya que si, por ejemplo, desea asignar direcciones IP a 300 hosts, una dirección clase C le resultará escasa y se verá obligada a solicitar una clase B, en cuyo caso se desperdiciarán cerca de 65.000 direcciones posibles.

Obviamente que el problema se origina desde el momento en que se decidió dividir el espacio total de direcciones posibles en clases, porque esto provoca un gran "gap" (brecha) entre las direcciones habilitadas para cada una de ellas. Recordemos también que esto no se hizo por capricho, sino por la necesidad de mantener lo más reducidas posibles las tablas de ruteo, ya que para rutear sólo se necesita el NetID.

¿Cómo solucionar esta situación de conflicto? ¿asignar más eficientemente las direcciones IP vs. mantener las tablas de ruteo reducidas?

Conocemos la solución. Aplicando VLSM a nivel externo de las organizaciones; lo cual simplemente significa olvidarse de las clases de direcciones IP y utilizar la información provista por el prefijo extendido de red. Este tipo de ruteo se denomina CIDR *Classless Inter-Domain Routing* o ruteo sin clases entre dominios.

### CIDR (**C**lassless **I**nter-**Domain **R**outing) (enrutamiento entre dominios sin clases)**

CIDR fue oficialmente admitido en Septiembre de 1993 en las RFC 1517 a 1520 y ofrece una solución transitoria a la poco eficiente disposición de direcciones IP en clases de IPv4, hasta que entre en funcionamiento la nueva versión de IP, el IPv6. Es muy probable que si CIDR no se hubiera implementado a tiempo, Internet hubiera colapsado hace mucho tiempo por la magnitud de las tablas de ruteo y la mala asignación de direcciones.

El uso de un rango de direcciones de clase C en vez de una sola de clase B acarrea un gran problema: cada red ha de ser direccionada por separado. El encaminamiento IP estándar sólo comprende las clases A, B y C. Dentro de cada uno de estos tipos de red, se puede usar "subnetting" para proporcionar mejor granularidad del espacio de direcciones en cada red, pero no hay forma de especificar que existe una relación real entre múltiples redes de clase C.

Esto se denomina el problema de la explosión de la tabla de enrutamiento: una red clase B de 3000 host requiere una entrada en la tabla de enrutamiento para cada "router troncal"; pero si la misma red se direcciona como un rango de redes de clase C, requeriría 16 entradas. La solución a este problema es el método llamado CIDR.

El método CIDR no encamina de acuerdo a la clase del número de red (de ahí el término "*classless*": sin clase) sino sólo según los bits de orden superior de la dirección IP, que se denominan prefijo IP. Cada entrada de encaminamiento CIDR contiene una dirección IP de 32 bits y una máscara de red de 32 bits, que en conjunto dan la longitud y valor del prefijo IP. Esto se puede representar como "Dirección\_IP" "Máscara\_Red". Por ejemplo, 200.0.0.0 254.0.0.0 representa el prefijo de 7 bits '1100100'.

CIDR maneja el encaminamiento para un grupo de redes con un prefijo común con una sola entrada de encaminamiento. Ésta es la razón por la que múltiples números de red de clase C, asignados a una sola organización, tienen un prefijo común. Al proceso de combinar múltiples redes en una sola entrada se lo llama reducción de direcciones. También se lo llama *supernetting* porque el encaminamiento se basa en máscaras de red más cortas que la máscara de red natural de la dirección IP, en contraste con el subnetting, donde las máscaras de red son más largas que la máscara natural.

A diferencia de las máscaras de subred, que normalmente son contiguas pero pueden tener una parte local no contigua, las máscaras de superred son siempre contiguas

Si se representan las direcciones IP como un árbol que muestre la topología de encaminamiento, donde cada rama del árbol significa un grupo de redes que se consideran como una sola unidad, llamada dominio de enrutamiento y el esquema de direccionamiento IP se elige de modo que cada bifurcación del árbol corresponda a un incremento en la longitud del prefijo IP, entonces el CIDR permite realizar la reducción de direcciones muy eficientemente. Por ejemplo, si un "router" en América Latina encamina todo el tráfico del país a través de un único enlace, entonces una sola entrada de encaminamiento para "200.0.0.0 254.0.0.0" incluye el grupo de direcciones de redes clase C asignadas a América Latina.

Esta única entrada toma el lugar de todas las entradas de los números de red asignados, que son un máximo de  $2^{17} = 131072$ . En el extremo local del enlace, hay entradas de encaminamiento con prefijos más largos que mapean la topología de la red, pero esta información de encaminamiento no hace falta en el extremo externo.

La filosofía de CIDR es "la mejor aproximación es la que tiene más aciertos", de modo que si es necesario hacer una excepción para un rango de direcciones, como por ejemplo las 64 redes "200.1.64.0 255.555.192.0", necesita sólo una entrada adicional, que en la tala de encaminamiento se superpone a otras entradas más generales (más cortas) de las redes que contiene. En este ejemplo se hace evidente que, a medida que aumenta el uso del espacio de direcciones IP, particularmente de las de clase C, los beneficios de CIDR aumentan por igual, siempre que la asignación de direcciones siga la topología de la red. El estado actual del espacio de direcciones IP no sigue este esquema, ya que el desarrollo de CIDR fue posterior.

Sin embargo, se están asignando nuevas direcciones de clase C de tal modo que sean compatibles con CIDR, lo que debería tener el efecto de aliviar el problema de la explosión de las tablas de enrutamiento a corto plazo.

A largo plazo, puede ser necesaria una reestructuración del espacio de direcciones IP siguiendo pautas topológicas. Esto supone la re-numeración de un gran número de redes, que implica un enorme trabajo de implementación, debiendo ser un proceso gradual.

Asumir que la topología de encaminamiento se puede representar con un simple árbol es un exceso de simplificación; aunque la mayoría de los dominios de enrutamiento tienen un solo enlace que proporciona acceso al resto de Internet, hay también muchos dominios con enlaces múltiples.

Los dominios de encaminamiento de estos dos tipos se llaman "*single-homed*" (unipuerto) y "*multi-homed*" (multipuerto). Es más, la topología; no es estática. No sólo se unen nuevas organizaciones a un ritmo creciente, sino que las ya existentes pueden cambiar partes de su topología, por ejemplo, si cambian de proveedor de servicios por razones comerciales o de otra índole. Aunque estos casos complican la implementación práctica del encaminamiento basado en CIDR y reducen la eficiencia de la agregación de direcciones que se puede conseguir, la estrategia no deja de ser válida.

Las políticas actuales para la distribución de direcciones de Internet y las suposiciones en las que se basan se describen en el **RFC 1518 - Una arquitectura para la distribución de direcciones IP con CIDR**.

Se pueden resumir en:

- La asignación de direcciones IP refleja la topología física de la red y no de la organización; las restricciones organizacionales y administrativas no deberían usarse en la asignación de direcciones cuando no se ajusten a la topología de la red.
- En general, la topología de la red seguirá de cerca los límites continentales y nacionales y, por tanto, las direcciones IP se deberían asignar partiendo de esta base.
- Habrá un número relativamente pequeño de redes que transportarán una elevada cantidad de tráfico entre dominios de enrutamiento y que estarán conectadas de modo no jerárquico, traspasando los límites nacionales. Estas redes se denominan TRD ("Transit Routing Domains"). Cada TRD tendrá un prefijo IP único. En general, los TRD no se organizarán jerárquicamente. Sin embargo, cuando un TRD se halle por completo dentro de los límites continentales, su prefijo IP debería ser una extensión del prefijo IP continental.
- Habrá organizaciones con enlaces a otras organizaciones para su uso privado y que no transportarán tráfico dirigido a otros dominios (tráfico de tránsito). Estas conexiones privadas no tienen un efecto significativo sobre la topología de red y pueden ser ignoradas.
- La gran mayoría de los dominios de encaminamiento serán *single-homed*. Es decir, estarán conectadas a un sólo TDR. Se les debería asignar direcciones que comiencen por el prefijo IP de ese TRD. Por tanto, todas las direcciones de los dominios "*single-homed*" conectados a un TDR se pueden agregar en una sola entrada de la tabla de encaminamiento para todos los dominios externos a ese TRD.
- Hay una serie de esquemas de asignación de direcciones que se pueden usar con dominios "*multi-homed*".

Algunos son:

- El uso de un único prefijo IP para el dominio: los "router" externos deben tener una entrada para la organización que se halla parcial o totalmente fuera de la jerarquía normal, donde un dominio sea "*multi-homed*", pero todos los TRD conectados estén topológicamente cerca, sería apropiado que el prefijo IP del dominio incluya los bits comunes a todos los TRD conectados. Por ejemplo, si todos los TRD estuvieran totalmente dentro de Argentina, un prefijo IP indicando un dominio exclusivo de Argentina sería lo adecuado.
- El uso de un prefijo IP para cada TRD conectado, con host en el dominio que tengan direcciones IP que contengan el prefijo del TRD más apropiado. La organización será como un conjunto de dominios de enrutamiento.
- Asignar un prefijo IP de uno de los TRD conectados. Este TRD se convierte en un TRD por defecto para el dominio, aunque otros dominios pueden encaminar explícitamente sus mensajes por uno de los TRD alternativos.
- El uso de prefijos IP para referirse a conjuntos de dominios "*multi-homed*" con conexiones a TRD. Por ejemplo, puede haber un prefijo IP que se refiera a dominios "*single-homed*" conectados a la red A; uno que se refiera a dominios "*single-homed*" conectados a la red B y otro para los dominios conectados a A y a B.
- Cada uno de estos esquemas tiene sus ventajas, desventajas y efectos colaterales. Por ejemplo, el primero tiende a generar un tráfico interno mayor en el dominio receptor más cercano al host origen, que el generado por el segundo esquema, aumentando recursos de red consumidos en la organización receptora.

Debido a que los dominios "*multi-homed*" varían mucho en su carácter y ninguno de los esquemas anteriores

parece apropiado para todos, no existe una política que sea la mejor, y el RFC 1518 no especifica ninguna regla para elegir entre ellas.

## Implementación de CIDR

La implementación de CIDR en Internet se basa fundamentalmente en BGP ("Border Gateway Protocol", versión 4). En el futuro CIDR también se implementará con una variante del estándar ISO IDRP, ISO 10747 ("Inter-Domain Routing Protocol"), llamado IDRP para IP, que está estrechamente relacionado con BGP-4.

La estrategia de implementación, descrita en el RFC 1520 - Intercambiando información de encaminamiento a través de las fronteras de los proveedores en el entorno CIDR-, implica un proceso por fases a través de la jerarquía de encaminamiento, empezando por los "router" troncales.

Los proveedores de servicios de red se dividen en cuatro tipos:

- Tipo 1. Aquellos que no pueden emplear ningún IDRP.
- Tipo 2. Aquellos que usan IDRP por defecto pero que requieren rutas explícitas para una proporción considerable de los números IP de red asignados.
- Tipo 3. Aquellos que usan IDRP por defecto y añaden, además, un pequeño número de rutas explícitas.
- Tipo 4. Aquellos que ejecutan IDRP utilizando sólo rutas por defecto.

La implementación de **CIDR** \* 17.1 implica una primera fase por medio de los proveedores de tipo 0, luego los de tipo 2 y, finalmente, los de tipo 3. CIDR ya se ha instituido ampliamente en troncales y más de 9000 rutas se han reemplazado por aproximadamente 2000 rutas CIDR.

## Reducción de direcciones

La dirección IP, que provee direccionamiento universal a través de todas las redes de la Internet, es una de las grandes capacidades del conjunto de protocolos TCP/IP. No obstante, la estructura de las direcciones IP tienen algunos problemas. Los diseñadores no tuvieron en cuenta la enorme escala actual de la red. Cuando TCP/IP fue diseñado, la conectividad estaba limitada a proveer servicios de conectividad a la comunidad académica universitaria, de manera de proporcionar sistemas de computación a esta organización.

La idea de proveer servicio al escritorio del usuario no existía, y mucho menos se pensaba en los poderosos Sistemas Operativos actuales. Al mismo tiempo, una dirección de 32 bit aparecía como una dirección muy larga y por ello fue dividida en clases para reducir la carga de procesamiento en los routers, como ya vimos en la situación anterior. Esta división de la dirección en clases reduce notablemente el número de direcciones disponibles.

De las originales:

$$2^{32} = 4.294.967.296 \text{ Direcciones distintas}$$

Al dividirlas en Clases, se pierden muchas direcciones. Por ejemplo, al asignarle una única dirección Clase B a una gran red, en lugar de seis direcciones Clase C, sin duda reducirá la carga del router, pero difícilmente una gran organización pueda tener 65535 (64K) computadoras conectadas. De esta manera, la mayoría de las direcciones de host disponibles en la organización, jamás serán asignadas.

Este tipo de direccionamiento, a favor de los routers por sobre el crecimiento de la red, ha colapsado debido al

rápido crecimiento de Internet.

Al presente, las direcciones Clase B están casi agotadas. Para prevenir esto, se les asigna a las organizaciones, bloques de direcciones Clase C, pero cada una de las direcciones Clase C requiere su propia entrada en la Tabla de Enrutamiento. Esta solución puede causar el crecimiento muy rápido de la Tabla de Enrutamiento, lo que puede terminar abrumando a los routers.

Estos problemas fueron tratados por el grupo de trabajo ROAD (ROuting and ADdressing) de la "*Internet Engineering Task Force* (IETF)".

Este grupo llegó a las siguientes conclusiones:

- Se puede aliviar el problema de las direcciones, utilizando direcciones largas o a direcciones sin clases.
- No se puede acelerar el crecimiento de la tabla de enrutamiento y no se puede incrementar la carga sobre los routers.
- Puede implementarse en los routers sin requerir cambios en los sistemas finales.

Una sugerencia es asignar grandes bloques contiguos de direcciones Clase C para los "proveedores de servicio". Éstos asignan partes de esos bloques a las organizaciones a las cuales les proveen servicios de red. Esto alivia en el corto plazo la insuficiencia de las direcciones Clase B, pero causa un rápido crecimiento de la Tabla de Enrutamiento.

Para manejar este otro problema, cada uno de los bloque de direcciones es dado a sólo una única dirección destino en la tabla de enrutamiento. El protocolo necesita, para distribuir las direcciones destinos, una máscara de direcciones que defina cómo serán interpretadas esas direcciones.

Los router necesitan interpretar esas direcciones como "sin clase", las cuales no son evaluadas de acuerdo a las reglas de las clases vistas anteriormente, sino de acuerdo a la máscara de bit que acompaña a las direcciones. Esas máscaras de bit son justamente semejantes a las usadas para división en subredes. El uso con la máscara de bit para crear grandes redes es llamado "supernetting".

# REFERENCIAS 17

## 17.1 : CIDR

Referencias:

- RFC 1467-Difusión de CIDR en Internet.
  - RFC 1517- Condiciones de aplicabilidad de CIDR.
  - RFC 1518- Una arquitectura para la distribución de direcciones IP con CIDR.
  - RFC 1519-CIDR: asignación de direcciones y estrategia de agregación.
  - RFC 1520- Intercambiando información de encaminamiento a través de las fronteras de los proveedores en el entorno CIDR.
-



¿Te animás a medir cuánto aprendiste?

**1. Indique la opción correcta**

CIDR sustituye la sintaxis previa para nombrar direcciones IP, las clases de redes. En vez de asignar bloques de direcciones dentro de los límites de los octetos, que fijan prefijos naturales de 8, 16 y 24 bits, CIDR usa la técnica VLSM para hacer posible la asignación de prefijos de longitud arbitraria.

- Verdadero
- Falso

**2. Indique la opción correcta**

El problema que se produce al aumentar las entradas en la tabla de enrutamiento, cuando se usan muchas direcciones clase C se denomina explosión de la tabla de enrutamiento.

- Verdadero
- Falso

**3. Indique la opción correcta**

CIDR encamina de acuerdo a los bits de orden superior de la dirección IP, que se denomina prefijo IP.

- Verdadero
- Falso

**4. Indique la opción correcta**

CIDR:

- Encamina de acuerdo a la clase del número de red.
- No encamina de acuerdo a la clase del número de red.
- Encamina según los bits de orden superior de la dirección IP.
- b y c son correctas.

**5. Indique la opción correcta**

CIDR permite:

- El uso eficiente de las cada vez mas escasas direcciones IP.

- Una mayor utilización de la jerarquía en las direcciones.
- Disminuir las tablas de ruteo.
- Todas las anteriores.

#### 6. Ordene relaciones

Unir conceptos:

VLSM	utiliza la máscara de bits para crear subredes
CIDR	utiliza la máscara de bits para crear grandes redes
Subnetting	permite la implementación de CIDR
BGP	utiliza la máscara de bits para crear redes de longitud variable

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

CIDR sustituye la sintaxis previa para nombrar direcciones IP, las clases de redes. En vez de asignar bloques de direcciones dentro de los límites de los octetos, que fijan prefijos naturales de 8, 16 y 24 bits, CIDR usa la técnica VLSM para hacer posible la asignación de prefijos de longitud arbitraria.

- Verdadero
- Falso

## 2. Indique la opción correcta

El problema que se produce al aumentar las entradas en la tabla de enrutamiento, cuando se usan muchas direcciones clase C se denomina explosión de la tabla de enrutamiento.

- Verdadero
- Falso

## 3. Indique la opción correcta

CIDR encamina de acuerdo a los bits de orden superior de la dirección IP, que se denomina prefijo IP.

- Verdadero
- Falso

## 4. Indique la opción correcta

CIDR:

- Encamina de acuerdo a la clase del número de red.
  - No encamina de acuerdo a la clase del número de red.
  - Encamina según los bits de orden superior de la dirección IP.
- X b y c son correctas.

## 5. Indique la opción correcta

CIDR permite:

- El uso eficiente de las cada vez mas escasas direcciones IP.
- Una mayor utilización de la jerarquía en las direcciones.
- Disminuir las tablas de ruteo.

X Todas las anteriores.

## 6. Ordene relaciones

Unir conceptos:

VLSM	utiliza la máscara de bits para crear redes de longitud variable
CIDR	utiliza la máscara de bits para crear grandes redes
Subnetting	utiliza la máscara de bits para crear subredes
BGP	permite la implementación de CIDR

# SP9 / H5: DNS (Domain Name System)

## Direcciones estándar \* 18.1

En Internet, la "dirección", se refiere a la forma de identificar a alguien en la red. Se trata de una dirección electrónica.

Todas las "direcciones" tienen la misma forma: el identificador de usuario, utilizado en la primera parte de la dirección Internet, seguido del carácter @ (arroba), seguido del nombre del dominio. Cada dominio tiene un nombre único.

La "dirección" estaría constituida de la siguiente manera:

**identificador\_de\_usuario@dominio**

A continuación veremos ejemplos de direcciones Internet:

ncura@ies21.edu.ar  
rpiña@ies21.com.ar  
vperez@ies21.edu.ar  
anvicperez@gmail.com  
anvicperez@hotmail.com

Como puede verse, un identificador de usuario por si sólo no es único, como puede verse en los dos últimos ejemplos, donde la identificación de usuario es "anvicperez". Es probable, que dentro de la Internet, haya varios usuarios que tengan la misma identificación, sobre todo si esa identificación es un nombre de persona, como Antonio, Víctor, Pérez, etc. Sin embargo, la combinación de identificador\_de\_usuario y dominio debe ser única.

Por lo tanto, si bien puede haber varios identificadores de usuario "anvicperez", solamente existe un único "anvicperez@gmail.com"

Toda dirección Internet incluye el signo "@".

Expresar el nombre del host de esta forma se llama "nombre por dominios totalmente calificado" (FQDN = Fully Qualified Domain Name).

El protocolo DNS es un protocolo estándar (STD 13). Su status es recomendado. Es descrito en:

- RFC 1034 - Nombres de dominio - conceptos y servicios
- RFC 1035 - Nombres de dominio - implementación y especificación

Las configuraciones iniciales de Internet requerían que los usuarios emplearan sólo direcciones IP numéricas. Esto evolucionó hacia el uso de nombres de host simbólicos muy rápidamente.

Inicialmente, el NIC (*Network Information Center*) mantenía el mapeado de nombres a direcciones en un sólo fichero (HOSTS.TXT) que todos los host obtenían vía FTP. Se denominó espacio de nombres plano.

Debido al crecimiento explosivo del número de host, este mecanismo se volvió demasiado tosco y poco práctico, (considere el trabajo necesario para añadir un host a Internet) y fue sustituido por un nuevo concepto: DNS (*Domain Name System*). Los host pueden seguir usando un espacio de nombres local plano (el archivo HOSTS.LOCAL) en lugar o además del DNS. Salvo en redes pequeñas, el DNS es prácticamente esencial.

DNS permite que un programa ejecutándose en un host, le haga a otro host el mapeo de un nombre simbólico de nivel superior a una dirección IP, sin que sea necesario que cada host tenga una base de datos completa de

los nombres simbólicos y las direcciones IP.

Examinaremos cómo funciona el DNS desde el punto de vista del usuario.

### El espacio de nombres jerárquico

Consideremos la estructura interna de una gran organización. Como el gerente no puede hacerlo todo, organización tendrá que dividirse en divisiones, cada una de ellas autónoma dentro de ciertos límites.

Especificamente, el ejecutivo a cargo de una división tiene autoridad para tomar decisiones sin requerir el permiso de su jefe.

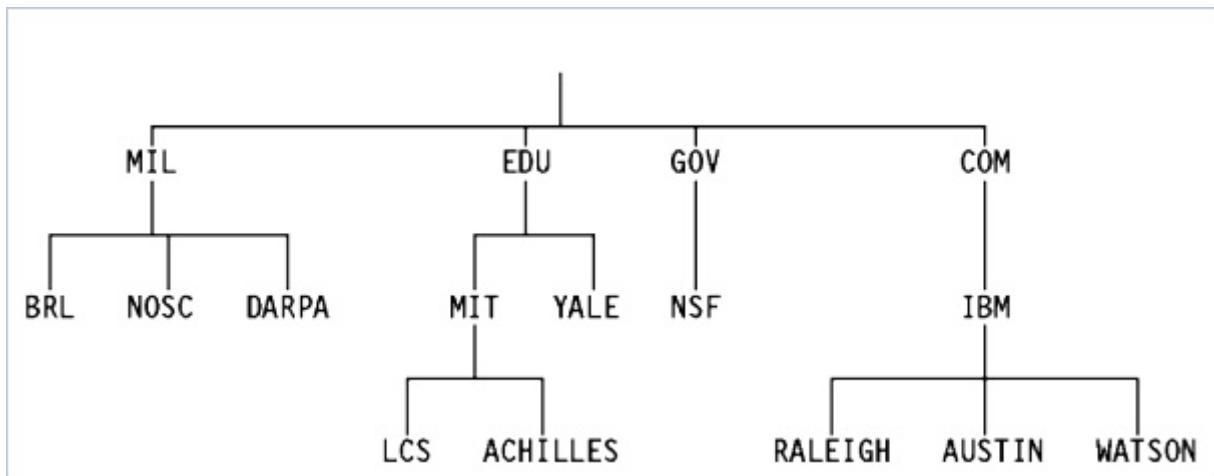
Los nombres de dominio se forman de modo similar y, con frecuencia, reflejarán la delegación jerárquica de autoridades usada para asignarlos.

Por ejemplo, considerar el nombre:

universidad.cordoba.edu

colegio\_ies21.cordoba.edu

Aquí, universidad.cordoba.edu, o colegio\_ies21.cordoba.edu es el nombre de dominio de nivel inferior, un subdominio de universidad.cordoba, o colegio\_ies21.cordoba que, a su vez, es un subdominio de edu (education), conocido como dominio raíz. También podemos representar esta forma de asignar nombres con un árbol jerárquico, ver siguiente figura.



Esta figura muestra la cadena de autoridades en la asignación de nombres de dominio. Este árbol es sólo una fracción mínima del espacio de nombres real. El dominio único que se halla sobre la cima no tiene nombre y se le conoce como dominio raíz.

### Nombre por dominios y subdominios

Una dirección Internet está formada por varias partes. Cada parte de ese dominio es un "subdominio". Los subdominios están separados por puntos. La forma de entender un dominio es leer los subdominios de derecha a izquierda. El nombre está constituido de forma que cada subdominio determina algo sobre la computadora.

El subdominio situado en el extremo derecho, llamado "subdominio de primer nivel" es el más general. Los subdominios que va apareciendo hacia la izquierda son cada vez más específicos.

Veamos el siguiente ejemplo:

[norberto@universidad.cordoba.edu](mailto:norberto@universidad.cordoba.edu)

En este ejemplo, el subdominio de primer nivel edu, nos indica que la computadora pertenece a una institución educativa (más adelante veremos los significados de los dominios). El siguiente subdominio, cordoba, nos indica el nombre de la institución. Por último, el dominio más a la izquierda es el nombre específico de la computadora, llamada univedrsidad.

En las direcciones pueden mezclarse letras mayúsculas y minúsculas y también números, como por ejemplo:

[Virginia21@universidad4.cordoba.edu.ar](mailto:Virginia21@universidad4.cordoba.edu.ar)

Esta dirección indica un usuario llamado Virginia21, que pertenece a la organización cordoba de la República Argentina. Más adelante vamos a hablar de los dominios territoriales.

En algunos sistemas, las mayúsculas y minúsculas no tienen el mismo significado. O sea virginia no es lo mismo que VIRGINIA, y éstos tampoco significan lo mismo que Virginia.

## Variaciones del formato estándar

Como ya vimos, todas las direcciones Internet siguen el formato estandar:

[identificador\\_de\\_usuario@dominio](mailto:identificador_de_usuario@dominio)

El ejemplo que mostramos tenía tres subdominios, pero es posible encontrar direcciones que tengan más subdominios.

Muchos utilizan patrones o esquemas para nombrar las máquinas, que tienen que ver con la actividad que realizan, o bien con elementos propios de la región. Así, podemos ver que existen máquinas con nombres de dibujos animados, nombres de planetas, héroes de historietas, etc.

Como anécdota podemos decir que en Estados Unidos tienen por costumbre referirse a los estados con apodos. Por ejemplo, California es el *Golden State*, Nueva York es el *Empire State*, Wisconsin es el *Cheese State* (Estado del Queso). Por ello, muchas computadoras de la Universidad de Wisconsin tienen nombres de quesos.

Así tenemos la siguiente dirección:

[jhonson@emmenthaler.cs.wisc.edu](mailto:jhonson@emmenthaler.cs.wisc.edu)

Si interpretamos este dominio, podemos decir que se trata de una computadora llamada emmenthaler, del departamento de informática (cs = computer science) de la Universidad de Wisconsin (wisc).

Existen otras direcciones que sólo tienen dos subdominios, como por ejemplo:

[alejandro@diel.com](mailto:alejandro@diel.com)

[nasanew@space.edu](mailto:nasanew@space.edu)

[info@wrq.com](mailto:info@wrq.com)

Cuando encontramos una dirección con dos subdominios puede significar dos cosas: que la organización es tan pequeña que sólo tiene una computadora en Internet. Éste es el caso de la primera dirección, en donde el usuario alejandro tiene un subdominio principal (com), dedicado a la actividad comercial. El otro subdominio es el nombre de su computadora (diel), que en este caso tiene el nombre de la compañía DIEL, que tiene una sola computadora en la red.

Los otros ejemplos pertenecen a una organización que tiene muchas computadoras en Internet. En algunas organizaciones es muy común utilizar una sola computadora para enviar y recibir correo electrónico. En nuestros ejemplos los nombres de las computadoras son space.edu y wrq.com.

En nuestros casos, el administrador de sistemas ha definido las direcciones del correo electrónico, de modo que todo el correo es recibido en una única dirección. Para ver cómo se hace, tomemos el ejemplo de nasanew@space.edu.

El término pasarela (gateway) se refiere a un enlace entre dos sistemas (redes o computadoras) diferentes. En este caso existe una "pasarela de correo electrónico" (mail gateway) y la computadora space.edu actúa como enlace entre la red interna y el mundo exterior. Esta pasarela tiene un listado de nombres de usuario y direcciones locales. Cuando llega un mensaje, comprueba esta lista y reenvía el mensaje a la computadora apropiada.

Por ejemplo, supongamos que Glenis es parte integrante de la organización de información sobre vuelos espaciales y otros acontecimientos de la NASA y que tiene su computadora en el departamento dedicado al espacio, conectada a Internet bajo la dirección:

glenis@glen.space.edu

Pero para poder simplificar la dirección de correo, el administrador de sistema registra a Glenis en la pasarela de correo electrónico con el nombre glenis@space.edu. Desde ese momento recibe correo enviado a la dirección indicada.

Como conclusión, podemos decir, que una dirección con sólo dos dominios puede pertenecer a una organización muy pequeña o muy grande.

Otra variante de las direcciones Internet que pueden encontrarse en las direcciones de correo electrónico: esta variante utiliza un carácter "%" (porcentaje) como parte de la dirección. En este caso el carácter % está a la izquierda del carácter "@". Por ejemplo:

glenis%glen@space.edu

En este caso, la computadora que recibe el mensaje (space.edu) examina la información a la izquierda de @, (glenis%glen) y comprueba que esto corresponde a un identificador de usuario y a una máquina local. El símbolo % es un separador del identificador de usuario del nombre de un host local.

## Dominios genéricos o subdominios de primer nivel

A los tres dominios de la cima de la figura que vimos anteriormente se los llama dominios genéricos u organizacionales.

Como ya se ha dicho anteriormente, la forma de entender una dirección es leerla de derecha a izquierda. El subdominio de primer nivel, que indica la especificación más general, es el que está más a la derecha.

Así vimos algunos ejemplos, como los indicados más abajo:

alejandro@diel.com

nasanew@space.edu

Observemos que los subdominios de primer nivel indican cosas distintas. Así tenemos edu, com, ar.

En general, hay dos tipos de subdominios de primer nivel: el formato antiguo, que indicaba "dominios de organizaciones", como edu y com. Y el formato nuevo que indica "dominios geográficos", como ar.

Los dominios de organizaciones están basados en un esquema de direcciones desarrollado antes de que las redes se internacionalizarán. Fue proyectado principalmente para los Estados Unidos. La idea era que éste identificara a la organización responsable de la computadora conectada a la red.

La tabla muestra las distintas categorías. Todas estas categorías existían desde los comienzos de Internet,

excepto "int", que fue agregada para identificar organizaciones internacionales como la ONU, OTAN, etc.

DOMINIO	SIGNIFICADO
com	Organización comercial
edu	Institución educativa
gov	Gobierno
Int	Organización internacional
mil	organización militar
net	organización de la red
org	organización sin fines de lucro

"Distintas categorías" | *Elaboración Autor*

#### **Dominios de primer nivel de organizaciones:**

Una vez que Internet se extendió a lo largo de todo el mundo, fue necesario crear dominios de primer nivel más específicos, desarrollándose de esta manera los dominios territoriales o geográficos, en el que una abreviatura de dos letras identifica al país. Existen muchos dominios de este tipo, uno por cada país integrante de la Internet. Estos dominios están indicados en la siguiente tabla. Hay dominios para cada uno de los códigos internacionales de dos caracteres ISO 3166 para países. Se los conoce como dominios de países o dominios geográficos.

DOMINIO	SIGNIFICADO
ae	Emiratos Árabes Unidos
aq	Antártica
ar	Argentina
at	Austria
au	Australia
be	Bélgica
bg	Bulgaria
ca	Canadá
br	Brasil
ca	Canadá
ch	Suiza
cl	Chile
cn	China
cr	Costa Rica
cs	República Checa y Eslovaquia
de	Alemania
dk	Dinamarca
ec	Ecuador
ee	Estonia
eg	Egipto
es	España
fi	Finlandia
fr	Francia
gb	Gran Bretaña
gr	Grecia

"Códigos" | Elaboración autor

### **Dominios de primer nivel Geográficos**

En Gran Bretaña y Nueva Zelanda, a veces, la dirección es exactamente al revés (¿podía ser de otra manera?). Es posible encontrar direcciones de la forma.

scott@uk.ac.oxford.comp1

Los sistemas de correo deben invertir los dominios para poder comunicarse con el mundo exterior.

### **Unicasting, broadcasting y multicasting**

La mayoría de las direcciones IP se refieren a un solo destinatario. Se denominan direcciones unicast. Sin embargo, como se ha señalado anteriormente, hay dos tipos especiales de direcciones IP que se utilizan para dirigir a múltiples destinatarios: las direcciones de broadcast y de multicast. Cualquier protocolo no orientado a conexión, puede enviar mensajes de broadcast o de multicast, además de los unicast.

Un protocolo orientado a conexión sólo puede usar direcciones de unicast porque la conexión existe entre un

par específico de host.

## Broadcasting

Hay una serie de direcciones que usan para el broadcast en IP: todas manejan el convenio de que "todos los bits 1" indica "todos los host". Las direcciones de *broadcast* nunca son válidas como direcciones fuente, sólo como direcciones de destino.

Los diferentes tipos de broadcast se listan aquí:

- Direcciones de broadcast limitado

La dirección 255.255.255.255 (todos los bits a 1 en toda la dirección IP) se usa en redes que soportan *broadcast*, y se refiere a todos los host de la subred. No requiere que el host tenga conocimiento alguno de la configuración IP. Todos los host de la red local reconocerán la dirección, pero los "router" nunca enviarán el mensaje. Esta regla tiene una excepción, llamada retransmisión BOOTP o el más moderno DHCP. Estos protocolos emplean el broadcast limitado para permitir a estaciones de trabajo sin disco contactar con un servidor para el boot remoto. La retransmisión es una opción de configuración disponible en algunos "router". Sin esta posibilidad, haría falta un servidor BOOTP o DHCP en cada subred. Sin embargo, no se trata de una simple retransmisión, ya que el "router" también interviene en el desarrollo del protocolo.

- Direcciones de broadcast dirigidas a red

Si el número de red es un válido, la red no se subdivide en subredes y el número de host referencia todos los hosts de la red especificada, (por ejemplo, 128.2.255.255). Los "router" deberían enviar estos mensajes de broadcast, a menos que están configurados para no hacerlo. Este tipo de broadcast se utiliza en solicitudes ARP (ver ARP "Address Resolution").

- Direcciones de broadcast dirigidas a subred

Si el número de red y el de subred son válidos, y el de host tiene todos sus bits a 1, entonces la dirección referencia a todos los host de la subred especificada. Debido a que la subred fuente y la de destino pueden tener distintas máscaras de subred, la fuente debe resolver de algún modo la máscara usada en la subred de destino. El broadcast lo efectúa realmente el "router" de subred que recibe el datagrama.

- Direcciones de broadcast dirigidas a todas las subredes

Si el número de red es válido, la red se subdivide en subredes y la parte local de la dirección tiene todos los bits a 1 (por ejemplo, 128.2.255.255), y la dirección se refiere a todos los hosts en todas las subredes de la red especificada. En principio, los "router" pueden propagar broadcasts por todas las subredes, aunque no están obligados a hacerlo. En la práctica, no lo hacen; hay pocas circunstancias en las que un broadcast sea deseable, y puede causar problemas, particularmente si un host se ha configurado incorrectamente sin su máscara de subred. Considerar el derroche de recursos que se produciría si el host 95.120.144.102 en la red local clase A con subredes no fuera consciente de la existencia de esas subredes y usara 95.255.255.255 como dirección de broadcast "local" en vez de 95.120.144.255 y todos los "router" aceptaran la solicitud de enviar mensajes a todos los clientes.

Si los "router" respetan todos los mensajes de broadcast dirigidos a subredes, utilizan un **algoritmo** \* 18.2 llamado Retransmisión Inversa (*Reverse Path Forwarding*) para evitar que los mensajes de broadcast se multipliquen descontroladamente.

# REFERENCIAS 18

## 18.1 : DNS

Referencias: para mas detalles sobre al implementación del DNS y el formato de mensajes entre servidores de nombres, ver DNS (Domain Name System).

Los siguientes RFC definen el estándar de DNS y la información que almacena.

- RFC 1032 - Guía de administrador de DNS.
- RFC 1033 - Guía de las operaciones de administrador de DNS.
- RFC 1034 - Nombres de dominio - Conceptos y servicios.
- RFC 1035 - Nombres de dominio - Implementación y especificación.
- RFC 1101 - Codificación DNS de nombres de red y de otros tipos.
- RFC 1183- Nuevas definiciones de DNS RR.
- RFC 1706 - Registros de recursos DNS NSAP.

---

## 18.2 : Algoritmo

Ver el RFC 922 para más detalles de este algoritmo.

---



¿Estás listo para un desafío?

**1. Indique la opción correcta**

Una "dirección" en Internet está constituida por: dominio@identificador\_de\_usuario

- Verdadero
- Falso

**2. Indique la opción correcta**

Un identificador de usuario deber ser único.

- Verdadero
- Falso

**3. Indique la opción correcta**

DNS permite que un programa ejecutándose en un host, le haga a otro host el mapeo de un nombre simbólico de nivel superior a una dirección IP, sin que sea necesario que cada host tenga una base de datos completa de los nombres simbólicos y las direcciones IP.

- Verdadero
- Falso

**4. Indique la opción correcta**

Los dominios .com, .edu y .mil son dominios de organizaciones.

- Verdadero
- Falso

**5. Indique la opción correcta**

¿Qué es una dirección de broadcasting?

- Es una dirección cuyos bit de host están todos en 0 (cero).
- Es una dirección cuyos bit de host están todos en 1 (uno).
- Es una dirección cuyos bit de red están todos en 0 (cero).
- Es una dirección cuyos bit de red están todos en 1 (uno).

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

DNS	transmite información a todos los host de una red específica, se utiliza en solicitudes ARP.
Broadcasting	transmite información a una multitud de receptores en forma simultánea.
Subdominio	constituye una parte de un dominio.
Broadcast dirigido	resuelve nombres inteligibles para las personas en identificadores asociados con los equipos conectados a la red.

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Una "dirección" en Internet está constituida por: dominio@identificador\_de\_usuario

Verdadero

Falso

## 2. Indique la opción correcta

Un identificador de usuario deber ser único.

Verdadero

Falso

## 3. Indique la opción correcta

DNS permite que un programa ejecutándose en un host, le haga a otro host el mapeo de un nombre simbólico de nivel superior a una dirección IP, sin que sea necesario que cada host tenga una base de datos completa de los nombres simbólicos y las direcciones IP.

Verdadero

Falso

## 4. Indique la opción correcta

Los dominios .com, .edu y .mil son dominios de organizaciones.

Verdadero

Falso

## 5. Indique la opción correcta

¿Qué es una dirección de broadcasting?

Es una dirección cuyos bit de host están todos en 0 (cero).

Es una dirección cuyos bit de host están todos en 1 (uno).

Es una dirección cuyos bit de red están todos en 0 (cero).

Es una dirección cuyos bit de red están todos en 1 (uno).

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

DNS

resuelve nombres inteligibles para las personas en identificadores asociados con los equipos conectados a la red.

Broadcasting

transmite información a una multitud de receptores en forma simultánea.

Subdominio

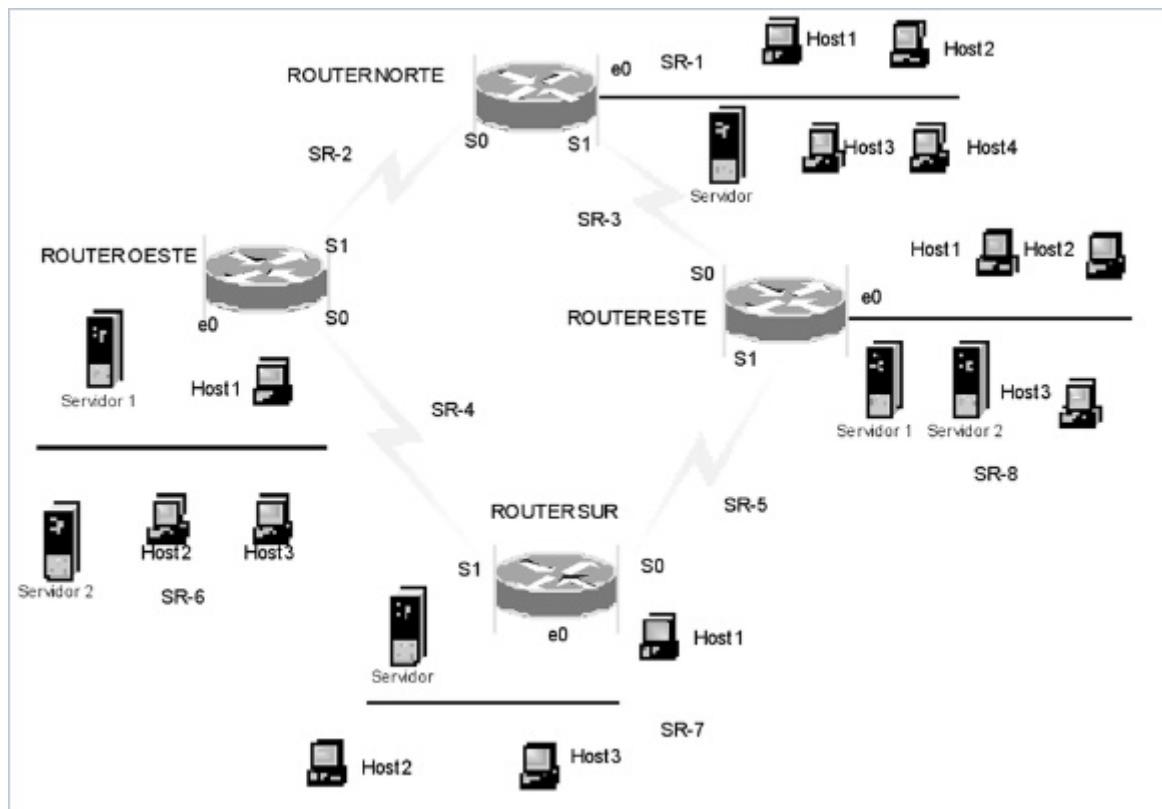
constituye una parte de un dominio.

Broadcast  
dirigido

transmite información a todos los host de una red específica, se utiliza en solicitudes ARP.

## SP9 / Ejercicio resuelto

La empresa a la que Ud. concurre es una empresa muy grande y ya la han dividido en 8 subredes, denominadas SR-1, SR-2....hasta SR-8. Ud. deberá ayudarlos con el cálculo de las subredes, las máscaras de subred, las direcciones de broadcast, la asignación IP a cada host y a cada interface de router con las subredes en las que tienen más problemas, que son la SR-1 y la SR-6.



En la tabla siguiente podrá observar:

En la primer columna el nombre de la Subred (SR-1...SR-8)

En la segunda columna la dirección IP asignada para cada subred

En la tercer columna el número de subred dentro de cada SR donde deberá trabajar

Subred	Dirección IP de la red	Nº de subred
SR-1	200.255.0.0	8
SR-2	172.16.0.0	19
SR-3	176.0.0.0	5
SR-4	189.0.0.0	115
SR-5	189.0.0.0	14
SR-6	10.0.0.0	3211
SR-7	10.0.0.0	31
SR-8	10.0.0.0	4125

"Tabla 1" | Elaboración autor

Para las SR-1 y la SR-6 se pide:

- Calcular cuál es la dirección IP de la subred de referencia
- Cuál es su máscara de subred
- Cuál es su dirección de broadcast
- Asignar dirección IP a cada Host y a cada interface de Router.

Subred	Dirección IP de la red	Nº de subred
SR-1	200.255.0.0	8
SR-2	172.16.0.0	19
SR-3	176.0.0.0	5
SR-4	198.0.0.0	115
SR-5	198.0.0.0	14
SR-6	10.0.0.0	3211
SR-7	10.0.0.0	31
SR-8	10.0.0.0	4125

"Tabla 2" | Elaboración autor

## Resolución para SR-1

### a. Cálculo de las subredes

Para realizar el cálculo de las subredes, debemos tener en cuenta que esta "gran red" está compuesta de varias direcciones IP, correspondientes cada una de ellas a una red.

Por ello debemos tener en cuenta cada una de ellas en particular.

- Cálculo de la subred "SR-1"

Vemos de la tabla, que la SR-1 corresponde a la red cuya IP es: 200.255.0.0

Además, se nos pide que de esta red debamos calcular la subred N° 8.

¿Cuál será la dirección de subred?

- Paso 1: comencemos analizando la Clase de dirección: obviamente se trata de una dirección Clase C, que está compuesta de 3 Bytes (los tres primeros) para el NetID y 1 Byte para el HostID.

Net ID = 200.255.0

Como vemos se trata de una dirección de red por cuanto el HostID es cero.

HostID = 0 (cero)

- Paso 2: para poder crear 8 subredes debemos pedir prestados 4 bit como mínimo para cumplir con la expresión:  $2^n - 2 >$  cantidad de subredes.

En nuestro caso,  $24 - 2 = > 8$

- Paso 3: ahora vamos a tomar el último octeto y lo pasamos a binario.

128	64	32	16	8	4	2	1
Bit3	Bit2	Bit1	Bit0	0	0	0	0
Sub red				HostID			

Los 4 primeros bits contando desde la izquierda son ahora bit de subred, o sea que ya no los podemos usar para Host.

Para dar direcciones a los Host nos quedan  $2^4 - 2 = 14$  posibilidades distintas. Recordar que las direcciones de Host todos ceros y todos unos, son direcciones de Red y de Broadcast respectivamente.

- Paso 4: ahora vamos a calcular el valor que le corresponde a la subred 8.

Para ello debemos realizar todas las combinaciones posibles según la tabla que se indica y ubicar los bit en los casilleros sombreados. De acuerdo a la combinación de los bit tendremos que el octeto tendrá el valor indicado en la última columna de la tabla (recordar que los bit de host están en cero por cuanto corresponde a la subred).

Subred	Bit 3	Bit 2	Bit 1	Bit 0	Valor
0	0	0	0	0	0
1	0	0	0	1	16
2	0	0	1	0	32
3	0	0	1	1	48
4	0	1	0	0	64
5	0	1	0	1	80
6	0	1	1	0	96
7	0	1	1	1	112
8	1	0	0	0	128
9	1	0	0	1	144
10	1	0	1	0	160
11	1	0	1	1	176
12	1	1	0	0	192
13	1	1	0	1	208
14	1	1	1	0	224
15	1	1	1	1	240

Si seguimos con nuestro ejemplo, la dirección IP de la subred será:

IP Subred = 200.255.0.128 (se le pide prestado al último byte por ser el de HostID)

### b. Cálculo de la máscara de subred

La Máscara de subred será: (recordar que la máscara se forma poniendo en "1" todos los bit de Red y de Subred, y poniendo en "0" a todos los bit de Host).

Máscara = 255.255.255.240 los 4 bit más significativos del último octeto son ahora de subred, por lo tanto si están todos en "1", tendremos:

128	64	32	16	8	4	2	1	Peso según su posición
1	1	1	1	0	0	0	0	$128+64+32+16 = 240$
Sub red				Host ID				

"Cálculo de la máscara de subred" | Elaboración autor

Si sumamos todos los valores nos da 240 como vemos en la tabla

### c. Cálculo de la dirección de broadcast

Ahora nos queda por calcular el valor de la dirección de Broadcast. Como sabemos la dirección de broadcast es aquella en la cual la Red queda inalterable, y los bit de host valen todos "1" (todos unos)

De esta manera será:

128	64	32	16	8	4	2	1	Peso según su posición
1	0	0	0	1	1	1	1	$128+8+4+2+1 = 143$
Sub red				HostID				

Esto es muy sencillo, ya que al valor de la IP de la subred: 200.255.0.128, solo le tenemos que sumar los bit de host (que ahora valen todos unos), y que en nuestro ejemplo suman 15.

$$8+4+2+1 = 15$$

Por lo tanto, nuestro último octeto será: 128 que corresponde a la subred, más 15 que corresponde al host. Ello nos dà el valor de 143, como puede verse en el dibujo anterior.

#### d. Asignar dirección IP a cada Host y a cada interface de Router

Hagamos una última verificación:

IP Subred = 200.255.0.128

IP de Broadcast = 200.255.0.143

Entre estos dos extremos están las direcciones de Host disponibles, en nuestro caso será:

Dirección IP	Asignaciones	
200.255.0.128	Subred	IP especial
200.255.0.129	e0 Router Norte	IP host válida 1
200.255.0.130	Servidor	IP host válida 2
200.255.0.131	Host 1	IP host válida 3
200.255.0.132	Host 2	IP host válida 4
200.255.0.133	Host 3	IP host válida 5
200.255.0.134	Host 4	IP host válida 6
200.255.0.135	Host 5 (Uso futuro)	IP host válida 7
200.255.0.136	Host 6 (Uso futuro)	IP host válida 8
200.255.0.137	Host 7 (Uso futuro)	IP host válida 9
200.255.0.138	Host 8 (Uso futuro)	IP host válida 10
200.255.0.139	Host 9 (Uso futuro)	IP host válida 11
200.255.0.140	Host 10 (Uso futuro)	IP host válida 12
200.255.0.141	Host 11 (Uso futuro)	IP host válida 13
200.255.0.142	Host 12 (Uso futuro)	IP host válida 14
200.255.0.143	Broadcast	IP especial

"direcciones de Host disponibles" | Elaboración autor

Como podemos verificar, se cumple la expresión  $2^4 - 2 = 14$  para la cantidad de direcciones de Host posibles. Ahora sólo nos resta designar los host y las direcciones IP que le corresponden.

- Paso 5: otra forma de calcular el valor del octeto de subred, y que nos va a servir para el caso de que debamos pedir más de ocho bit para la subred, será el siguiente:

1. Pasar el valor de la subred solicitada a binario. En nuestro ejemplo el valor será:

$$1\ 0\ 0\ 0 = 8$$

2. Estos bit los ubicamos en el octeto, en la parte de Subred, de la forma que se indica a continuación:

128	64	32	16	8	4	2	1	Peso según su posición
1	0	0	0	0	0	0	0	= 128
								Sub red      HostID

"bit" | Elaboración autor

3. Obviamente llegamos a la misma solución anterior.

4. Esto será apreciado cuando calculemos las Subredes SR-6, SR-7 y SR-8.

## Resolución para SR-6

### a. Cálculo de la subred

Vemos de la tabla, que la SR-6 corresponde a la red cuya IP es: 10.0.0.0

Además se nos pide que de esta red debamos calcular la subred N° 3211.

Subred	Dirección IP de la red	Nº de subred
SR-1	200.255.0.0	8
SR-2	172.16.0.0	19
SR-3	176.0.0.0	5
SR-4	198.0.0.0	115
SR-5	198.0.0.0	14
SR-6	10.0.0.0	3211
SR-7	10.0.0.0	31
SR-8	10.0.0.0	4125

"calcular la subred N° 3211" | Elaboración autor

¿Cuál será la dirección de subred?

- Paso 1: comencemos analizando la Clase de dirección. Obviamente se trata de una dirección

Clase A, que está compuesta de 1 Byte (el primero) para el NetID y 3 Bytes para el HostID.

Net ID = 10

Como vemos se trata de una dirección de red por cuanto el HostID es cero.

HostID = 0.0.0

- Paso 2: Para poder crear 3211 subredes, debemos pedir prestados 12 bit como mínimo para cumplir con la expresión  $2^n - 2 >$  cantidad de subredes.

En nuestro caso,  $2^{12} - 2 = 4096 - 2 = 4094 > 3211$

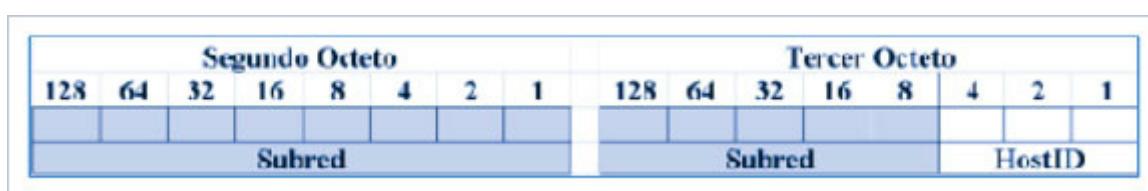
Pero cuidado, esta no es la máxima subred, ya que la SR-8, es también una subred de la 10.0.0.0, y es mayor que la subred SR-6. Y si observamos en la expresión el valor 4096 es menor que el valor de la SR-8 = 4125.

Esto nos obliga a tomar 13 bit en lugar de 12.

Recalculemos:  $2^{13} - 2 = 8192 - 2 = 8190 > 4125 > 3211$

O sea que debemos tomar prestados 13 bit, que conforman más de un octeto.

En nuestro caso tomaremos el segundo byte completo (8 bits), más cinco bit del tercer octeto, todo de acuerdo a la figura:



"Figura" | Elaboración autor

Como en este caso no podemos utilizar el "multiplicador" por tratarse de más de 8 bits, tendremos que usar el segundo método, por lo que es necesario pasar el número decimal 3211 a binario.

Una forma muy sencilla de hacerlo es la que se explica a continuación:

1. Confeccionemos el esquema de binario con los pesos de los bits, para 13 bits. Vea el dibujo que sigue:

Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1
4096	2048	1024	512	256	128	64	32	16	8	4	2	1

2. Ahora que tenemos este esquema, tomemos el número decimal que tenemos que pasar a binario. En nuestro caso 3211, y comencemos con el siguiente procedimiento:

Y el número binario correspondiente:

0	1	1	0	0	1	0	0	0	1	0	1	1
---	---	---	---	---	---	---	---	---	---	---	---	---

3. Ahora sólo nos resta ubicar esos bit en los 13 bit que habíamos pedido prestados. De acuerdo a la figura siguiente nos queda.

Segundo Octeto								Tercer Octeto							
128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
0	1	1	0	0	1	0	0	0	1	0	1	1	0	0	0
Subred								Subred							
HostID								HostID							

4. Por último debemos calcular los valores decimales del Segundo y Tercer Octeto.

a) Segundo Octeto:  $64 + 32 + 4 = 100$

b) Tercer Octeto:  $64 + 16 + 8 = 88$  (Recordar que los bit de Host deben ser ceros)

5. Ahora si, ya tenemos el valor de la sub red que será:

Net ID = 10.100.88.0

### b. Cálculo de la máscara de subred

Calculamos ahora la máscara, que como vemos está conformada de la siguiente manera:

a) Primero: NetID (deben ser todos 1) = 255

b) Segundo Octeto: Subred (deben ser todos 1) = 255

c) Tercer Octeto: los 5 bit más significativos son de Subred (deben ser todos 1), los 3 bit menos significativos son de Host (deben ser todos 0) = 248

$128+64+32+16+8 = 248$

d) Cuarto Octeto: HostID (deben ser todos 0) = 0

La máscara será: 255.255.248.0

### c. Cálculo de la dirección de broadcast

Calculamos la dirección de broadcast, que como sabemos la Red – Subred queda inalterable y los bit de Host todos en 1 (uno).

a) Primero: NetID = 10

b) Segundo Octeto: Subred = 100

c) Tercer Octeto: los 5 bit más significativos son de Subred (88), los 3 bit menos significativos son de Host (deben ser todos 1) =  $88 + 4 + 2 + 1 = 95$

d) Cuarto Octeto: HostID (deben ser todos 1) = 255

La dirección de broadcast será: 10.100.95.255

### d. Asignar dirección IP a cada Host y a cada interface de Router

Las direcciones IP disponibles para los Host serán las que van desde la Net ID a la Dirección de broadcast:

Net ID = 10.100.88.0

Broadcast = 10.100.95.255

Comprobando, tenemos para los host las direcciones que van desde 10.100.89.0 a la dirección 10.100.88.254

Dirección IP	Asignaciones	
10.100.88.0	Subred	IP especial
10.100.88.1	e0 Router Oeste	IP host válida 1
10.100.88.2	Servidor 1	IP host válida 2
10.100.88.3	Servidor 2	IP host válida 3
10.100.88.4	Host 1	IP host válida 4
10.100.88.5	Host 2	IP host válida 5
10.100.88.6	Host 3	IP host válida 6
10.100.88.7	(Uso futuro)	IP host válida 7
10.100.88.8	...	...
10.100.88.9	...	...
10.100.95.255	Broadcast	IP especial

"Comprobando" | *Elaboración autor*

Y con esto damos por terminado el cálculo de la subred SR-6.

## SP9 / Ejercicio por resolver

Gracias a su capacidad demostrada para resolver los problemas planteados en las subredes SR-1 y SR-6 de la empresa, lo contratan a Ud. para que los ayude a resolver los problemas definidos en las otras 6 subredes.

Para resolverlos, deberá completar el ejercicio resuelto, asignando direcciones IP a cada una de las subredes y dispositivos faltantes.

Para cada subred (SR), se pide:

- a. Calcular cuál es la dirección IP de la subred de referencia
- b. Cuál es su máscara de subred
- c. Cuál es su dirección de broadcast
- d. Asignar dirección IP a cada Host y a cada interface de Router.

Deberá aplicar los métodos indicados en el ejercicio resuelto.

Tenga en cuenta que para las subredes SR-7 y SR-8, ya tiene el esquema de 13 bit que necesita, solo deberá convertir a binario los números decimales 31 y 4125 respectivamente.

## SP9 / Evaluación de paso



¡Vamos a comprobar cuánto aprendiste!

**1. Indique la opción correcta**

Las redes reservadas incluyen todas las redes asignadas y adicionalmente, aquellas otras que han sido reservadas por IANA.

- Verdadero
- Falso

**2. Indique la opción correcta**

Una red Clase B pueden tener 65.534 host.

- Verdadero
- Falso

**3. Indique la opción correcta**

Las redes Clase D se usan para direcciones de Multicast. Se consideran direcciones en uso.

- Verdadero
- Falso

**4. Indique la opción correcta**

CIDR no encamina de acuerdo a la clase del número de red, sino con los bits de orden superior de la dirección IP.

- Verdadero
- Falso

**5. Indique la opción correcta**

Si un router identifica que una dirección es Clase c:

- Aplica una máscara de red con los primeros 8 bits iguales a 1 y los restantes iguales a 0.
- Aplica una máscara de red con los primeros 16 bits iguales a 1 y los restantes iguales a 0.
- Aplica una máscara de red con los primeros 24 bits iguales a 1 y los 8 restantes iguales a 0.
- Aplica una máscara de red con los todos los bits iguales a 1 y ningún bit igual a 0.

**6. Indique la opción correcta**

Siguiendo la práctica habitual al asignar direcciones IP a los host que participarán en comunicaciones vía Internet, se reservará:

- El identificador de host con todos los valores iguales a 0 para identificar la red.
- El identificador de host con todos los valores iguales a 0 para identificar la subred.
- El identificador de host con todos los valores iguales a 1 para identificar la difusión dentro de la red o subred.
- Todas las anteriores son correctas.

**7. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

IANA	es la entidad que tiene la responsabilidad de supervisar la asignación global de direcciones IP.
Subred	es una solución para el agotamiento de direcciones, que consiste en aplicar máscaras de longitud variable.
VLSM	es la solución encontrada para crear redes grandes utilizando VLSM.
CDIR	es definida aplicando una máscara de bit, la máscara de subred, a la dirección IP.

**8. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

RIR	es el sistema que resuelve nombres de dominio inteligibles para las personas en direcciones IP.
ICANN	es una organización dedicada a preservar la estabilidad de Internet.
Subnetting	es la división de una red en subredes únicas.
DNS	es el registros que administra, distribuye y registra la numeración dentro de sus respectiva región.

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Las redes reservadas incluyen todas las redes asignadas y adicionalmente, aquellas otras que han sido reservadas por IANA.

- Verdadero
- Falso

## 2. Indique la opción correcta

Una red Clase B pueden tener 65.534 host.

- Verdadero
- Falso

## 3. Indique la opción correcta

Las redes Clase D se usan para direcciones de Multicast. Se consideran direcciones en uso.

- Verdadero
- Falso

## 4. Indique la opción correcta

CIDR no encamina de acuerdo a la clase del número de red, sino con los bits de orden superior de la dirección IP.

- Verdadero
- Falso

## 5. Indique la opción correcta

Si un router identifica que una dirección es Clase c:

- Aplica una máscara de red con los primeros 8 bits iguales a 1 y los restantes iguales a 0.
- Aplica una máscara de red con los primeros 16 bits iguales a 1 y los restantes iguales a 0.
- Aplica una máscara de red con los primeros 24 bits iguales a 1 y los 8 restantes iguales a 0.
- Aplica una máscara de red con los todos los bits iguales a 1 y ningún bit igual a 0.

## 6. Indique la opción correcta

Siguiendo la práctica habitual al asignar direcciones IP a los host que participarán en comunicaciones vía Internet, se reservará:

- El identificador de host con todos los valores iguales a 0 para identificar la red.
- El identificador de host con todos los valores iguales a 0 para identificar la subred.
- El identificador de host con todos los valores iguales a 1 para identificar la difusión dentro de la red o subred.

X Todas las anteriores son correctas.

## 7. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

IANA	es la entidad que tiene la responsabilidad de supervisar la asignación global de direcciones IP.
Subred	es definida aplicando una máscara de bit, la "máscara de subred", a la dirección IP.
VLSM	es una solución para el agotamiento de direcciones, que consiste en aplicar máscaras de longitud variable.
CDIR	es la solución encontrada para crear redes grandes utilizando VLSM.

#### 8. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

RIR	es el registros que administra, distribuye y registra la numeración dentro de sus respectiva región.
ICANN	es una organización dedicada a preservar la estabilidad de Internet.
Subnetting	es la división de una red en subredes únicas.
DNS	es el sistema que resuelve nombres de dominio intellegibles para las personas en direcciones IP.

# Situación profesional 10: ¿Necesitaremos confiabilidad y/o velocidad?

## La capa de Transporte en el modelo TCP/IP

Su jefe le informa que necesita desarrollar aplicaciones para que los usuarios puedan comunicarse entre las distintas computadoras y entre las distintas redes LAN; por lo tanto necesita un protocolo de transporte. Su máxima preocupación es que la transmisión sea lo más veloz posible. El modelo TCP/IP ofrece dos tipos de servicio, ubicados en la Capa de Transporte: el protocolo UDP y el protocolo TCP. La alternativa UDP es para aplicaciones poco confiables, pero de estructura muy sencilla, mientras que TCP es mucho más confiable pero bastante más compleja.

# SP10 / H1: La Capa de Transporte en TCP/IP

Como hemos visto hasta ahora, el protocolo IP es capaz de permitirnos establecer comunicación entre dos host que posean dirección IP, brindando un servicio sin conexión y no confiable.

Actualmente, la mayor parte de los sistemas operativos que utilizan los host aceptan multiprogramación, lo cual significa permitir que varios programas de aplicación se ejecuten al mismo tiempo. Esto se refiere a que varios programas pueden estar utilizando los servicios IP para enviar o recibir datagramas de otros host. Sin embargo, IP es incapaz de distinguir entre las aplicaciones que están intentando conectarse. IP simplemente brinda un servicio que permite comunicar dos host, pero no distinguir aplicaciones dentro de ellos.

Sin considerar la naturaleza del **proceso** \* 19.1 que está intercambiando datos (por ejemplo transferencia de archivo, correo electrónico, login remoto, etc.), usualmente se requiere que los datos deban ser intercambiados fidedignamente.

El mecanismo para proveer exactitud es esencialmente independiente de la naturaleza del proceso. Por esta razón, esto da sentido a mecanismos en una capa común compartida por todos los procesos; y está puntualizado como "capa de transporte" o "capa *host-to-host*".

La capa de transporte es la que se encarga de direccionar los mensajes a las distintas aplicaciones que estén utilizando los servicios IP; dentro de TCP/IP esta función la llevan adelante dos protocolos de transporte distintos: UDP y TCP. Ambos cumplen una misma función:

1. Establecer conexiones entre aplicaciones de dos *host* distintos.
2. Permitir que varias aplicaciones utilicen simultáneamente los servicios IP dentro de un mismo host.

Una primera solución podría ser intentar identificar de alguna forma única a cada aplicación, para así poder direccionar los mensajes IP; con esto cubriríamos la función 1 enunciada anteriormente. Sin embargo este proceso tiene un defecto, no nos olvidemos de que una aplicación debe poder abrirse o ejecutarse simultáneamente varias veces (como, por ejemplo, cuando usted abre varias veces su browser en ventanas distintas), lo cual de esta forma sería imposible; por lo tanto no cubriríamos la función 2.

La solución final debe -entonces- contemplar la posibilidad de que una misma aplicación se encuentre ejecutándose varias veces, además de permitir que muchas aplicaciones distintas se comuniquen, y esto nos obliga a **no pensar en las aplicaciones como destino final de los mensajes**.

En su lugar se hace una abstracción, definiendo los llamados puertos de protocolo (estos son los SAP -Service Access Point - que se ubican entre el nivel de Transporte y el Nivel de Aplicación). Cada uno de ellos se identifica por medio de un número entero positivo; el sistema operativo local proporciona un mecanismo de interfaz que las aplicaciones utilizan para especificar o acceder a un puerto.



"A capa de Transporte en TCP/IP" | *Elaboración del autor*

Si le parece complicada la idea de un puerto de protocolo, simplemente piense que es muy probable que ya haya escrito algún programa que hace uso de "puertos" como el puerto LPT1 de las PC, habitualmente asociado a una impresora; claro que es un puerto de hardware. Sin embargo el concepto es muy similar, sólo que del otro lado del puerto, en vez de encontrarse con una impresora, se encuentra con un protocolo.

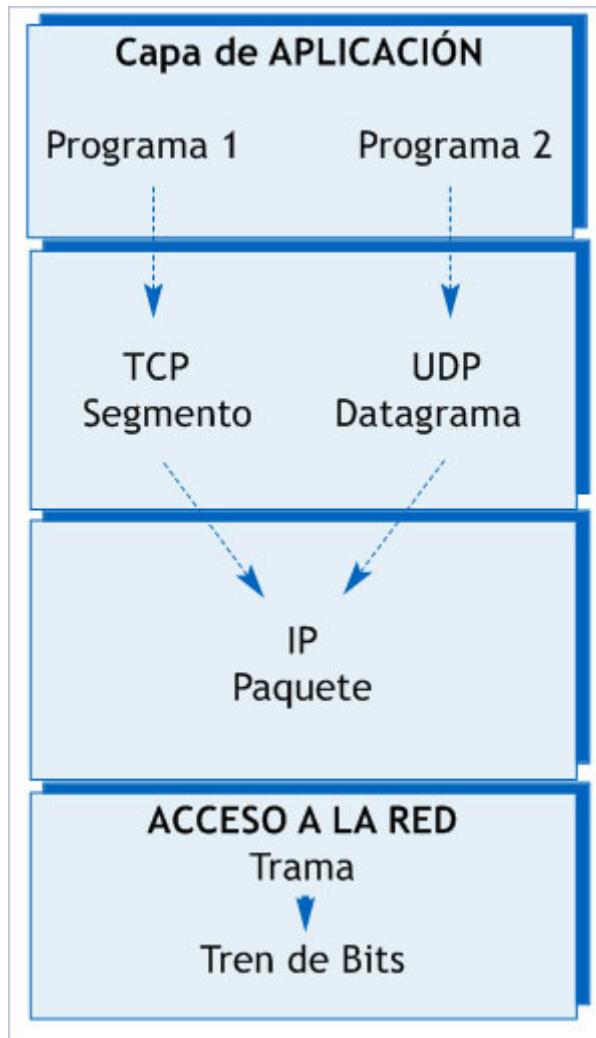
El protocolo de la Capa de Transporte, que está ubicado justamente encima de la Capa Internet, es la "Capa de Transporte o *Host-to-Host*". Este nombre normalmente es abreviado como "Capa de Transporte".

Los dos protocolos más importantes de la Capa de Transporte son:

- "Protocolo de Control de Transmisión" (TCP = *T ransmission Control Protocol*)
- "Protocolo de Datagramas de Usuario" (UDP = *User Datagram Protocol*).

TCP provee servicio de entrega segura de datos con detección y corrección de errores extremo a extremo. UDP provee un servicio "no orientado a conexión" de entrega de datagramas de baja sobrecarga (*low-overhead*).

Ambos protocolos entregan datos entre la Capa de Aplicación y la Capa Internet.



"Proceso de encapsulamiento en TCP/IP" | Elaboración del autor

# REFERENCIAS 19

## 19.1 : Proceso

Es habitual referirse a los programas en ejecución con los siguientes términos: proceso, tarea, programa de aplicación, o proceso a nivel de usuario.

---



¿Te animás a medir cuánto aprendiste?

**1. Indique la opción correcta**

La tarea de la capa de Transporte es direccionar los mensajes a las distintas aplicaciones, dentro de TCP/IP, a esta función la llevan adelante dos protocolos de transporte: UDP y TCP.

- Verdadero
- Falso

**2. Indique la opción correcta**

TCP y UDP ambos cumplen la función de establecer conexiones entre aplicaciones distintas y permitir que varias aplicaciones utilicen simultáneamente los servicios IP en el mismo host.

- Verdadero
- Falso

**3. Indique la opción correcta**

El protocolo más importantes de la capa de Transporte es:

- El Protocolo de Control de Transmisión (TCP).
- El Protocolo de Datagramas de Usuario (UDP).
- Los dos protocolos anteriores son los más importantes.
- Ningún protocolo nombrado anteriormente es el más importante.

**4. Indique la opción correcta**

¿Qué tipo de servicio provee TCP?

- Entrega poco segura de datos sin detección y corrección de errores extremo a extremo.
- Entrega segura de datos sin detección y corrección de errores extremo a extremo.
- Entrega poco segura de datos con detección y corrección de errores extremo a extremo.
- Entrega segura de datos con detección y corrección de errores extremo a extremo.

**5. Indique la opción correcta**

¿Qué tipo de servicio provee UDP?

- UDP es un protocolo de datagramas seguro, no orientado a conexión.
- UDP es un protocolo de datagramas poco seguro, orientado a conexión.
- UDP es un protocolo de datagramas poco seguro, no orientado a conexión.
- UDP es un protocolo de datagramas poco seguro, orientado a conexión.

#### 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

IP	se encarga de direccionar los mensajes a las distintas aplicaciones que estén utilizando los servicios IP
Capa de Transporte	permite establecer comunicación entre dos hosts brindando servicio sin conexión y no confiable
TCP	provee un servicio no orientado a conexión de entrega de datagramas de baja sobrecarga
UDP	provee un servicio de entrega segura de datos con detección y corrección de errores

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

La tarea de la capa de Transporte es direccionar los mensajes a las distintas aplicaciones, dentro de TCP/IP, a esta función la llevan adelante dos protocolos de transporte: UDP y TCP.

- Verdadero
- Falso

## 2. Indique la opción correcta

TCP y UDP ambos cumplen la función de establecer conexiones entre aplicaciones distintas y permitir que varias aplicaciones utilicen simultáneamente los servicios IP en el mismo host.

- Verdadero
- Falso

## 3. Indique la opción correcta

El protocolo más importantes de la capa de Transporte es:

- El Protocolo de Control de Transmisión (TCP).
- El Protocolo de Datagramas de Usuario (UDP).
- Los dos protocolos anteriores son los más importantes.
- Ningún protocolo nombrado anteriormente es el más importante.

## 4. Indique la opción correcta

¿Qué tipo de servicio provee TCP?

- Entrega poco segura de datos sin detección y corrección de errores extremo a extremo.
- Entrega segura de datos sin detección y corrección de errores extremo a extremo.
- Entrega poco segura de datos con detección y corrección de errores extremo a extremo.
- Entrega segura de datos con detección y corrección de errores extremo a extremo.

## 5. Indique la opción correcta

¿Qué tipo de servicio provee UDP?

- UDP es un protocolo de datagramas seguro, no orientado a conexión.
- UDP es un protocolo de datagramas poco seguro, orientado a conexión.
- UDP es un protocolo de datagramas poco seguro, no orientado a conexión.
- UDP es un protocolo de datagramas poco seguro, orientado a conexión.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

IP

permite establece comunicación entre dos hosts brindando servicio sin conexión y no confiable

Capa de Transporte

se encarga de direccionar los mensajes a las distintas aplicaciones que estén utilizando los servicios IP

TCP

provee un servicio de entrega segura de datos con detección y corrección de errores

UDP

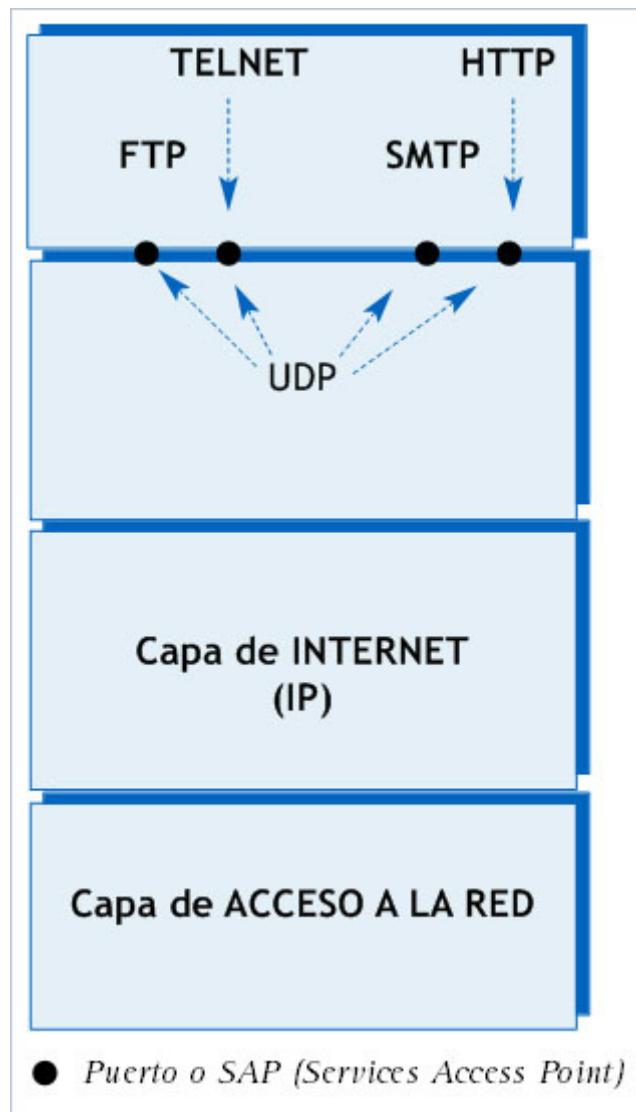
provee un servicio no orientado a conexión de entrega de datagramas de baja sobrecarga

## SP10 / H2: Protocolo de Datagramas de Usuario - UDP

El UDP (*User Datagram Protocol*) provee acceso directo a los programas de aplicación, brindando servicio de entrega de datagramas, parecido al servicio de IP. Permite a las aplicaciones intercambiar mensajes sobre la red con una sobrecarga de protocolo mínima.

UDP es un protocolo de datagramas no orientado a conexión, poco seguro. Antiguamente, "poco seguro" significaba que el protocolo no contenía una técnica que asegurase la entrega correcta de los datos en el otro extremo de la red, pero UDP puede entregar datos correctamente entre host.

UDP usa 16 bits de los 32 de la primera palabra de la cabecera para identificar los "Puerto Origen" (*Source Port*) y otros 16, para identificar el "Puerto Destino" (*Destination Port*).



"Proceso de encapsulamiento en TCP/IP" | Elaboración autor

Las aplicaciones que acceden a modelos "pregunta-respuesta" (*query-response*), son también excelentes candidatos para usar UDP. La respuesta puede ser usada como un reconocimiento positivo a la consulta. Si una respuesta no es recibida en un cierto período de tiempo, la aplicación debe enviar nuevamente la consulta. Sin

embargo, otras aplicaciones proveen su propia técnica para la entrega segura de datos y no requieren los servicios del protocolo de la Capa de Transporte. La imposición de reconocimientos en cualquier otra capa en estos tipos de aplicaciones es ineficiente y no tiene sentido.

Si UDP es un protocolo inseguro, ¿por qué razón los programadores de aplicación eligen UDP como un servicio de transporte de datos?

Hay un buen número de razones. Si la cantidad de datos transmitidos es pequeña, la sobrecarga (over-head) para el establecimiento de la conexión y la seguridad de una entrega confiable, puede ser mayor que el trabajo de retransmisión completa del conjunto de datos. En este caso, UDP es la opción más eficiente para el protocolo de la Capa de Transporte.

La mayor parte de los sistemas operativos proporcionan un acceso síncrono a los puertos. Esto significa que desde el punto de vista de una aplicación en particular, los cómputos se detienen durante una operación de acceso a puerto; por ejemplo, si un proceso intenta extraer datos de un puerto antes de que llegue cualquier dato, el sistema operativo bloquea temporalmente el proceso hasta que éstos lleguen. Una vez que esto sucede, el sistema operativo pasa los datos a la aplicación y lo vuelve iniciar.

En general, los puertos tienen memoria caché, para que los datos que llegan antes de que un proceso esté listo para aceptarlos no se pierdan.

Para comunicarse con un puerto ubicado en un host destino, el transmisor debe conocer tanto la dirección IP del host destino, como el número de puerto de protocolo dentro del host destino a dónde enviará los datos. En general, todos los mensajes llevan tanto el número del puerto de origen de la máquina fuente como el número de puerto en la máquina destino.

UDP proporciona entrega de datagramas, sin conexión y no confiable, igual que IP:

- No emplea acuse de recibo para asegurarse que lleguen los mensajes,
- No ordena los mensajes entrantes,
- No proporciona realimentación para controlar la velocidad a la que fluye la información entre las máquinas.
- Los mensajes IP se pueden perder, duplicar, o llegar sin orden.

Un programa de aplicación que utiliza UDP, acepta toda la responsabilidad por el manejo de los problemas de confiabilidad, incluyendo la pérdida, duplicación y retraso de mensajes, la entrega fuera de orden y la pérdida de conectividad.

## Formato de los mensajes UDP

Los mensajes UDP se conocen con el nombre de datagrama del usuario. Los datagrama de usuario constan de un encabezado y un área de datos; el encabezado está compuesto por cuatro campos de 16 bits, como se muestra en la figura siguiente.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Puerto Origen																Puerto Destino															
Longitud del Mensaje UDP (Bytes)																Suma de Verificación UDP (Checksum)															
Datos...																															
...Datos...																															

- **Puerto Origen y Puerto Destino:** los campos Puerto Fuente y Destino identifican los puntos terminales de la conexión. Es un valor que especifica la parte a la que se deben enviar las respuestas, de lo contrario, su valor debe ser nulo.
- **Campo de longitud:** contiene la cantidad de Bytes del datagrama UDP, incluyendo el encabezado y los datos del usuario UDP.
- **Campo suma de verificación o Checksum:** es opcional, un valor 0 en el campo significa que la misma no se ha computado. El campo Suma de Verificación incluye también a los datos del usuario, a diferencia de todos los otros campos checksum que hemos visto. Esta suma de verificación proporciona la única manera de garantizar que los datos lleguen intactos, por lo que se sugiere utilizarla. No nos olvidemos de que el protocolo IP no coteja en el checksum los datos de usuario sino solamente los valores del encabezado IP.

Para clarificar el concepto recordemos que IP sólo se encarga de identificar los host de origen y destino y que UDP se encarga de identificar los puertos de protocolo en ellos.

## UDP y el multiplexado

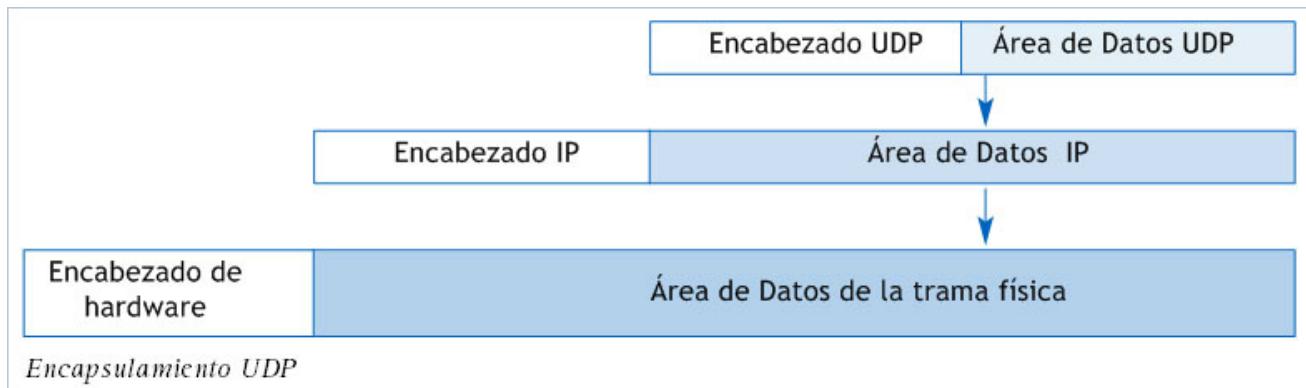
UDP presenta un claro ejemplo de multiplexado y demultiplexado. Pensemos en que UDP recibe mensajes de múltiples aplicaciones y las multiplexa en una única salida hacia IP; por otro lado, UDP recibe datagramas desde IP, los cuales debe demultiplexar para determinar hacia qué aplicación los debe derivar.

Todo el proceso de multiplexación y demultiplexación se realiza a través de los puertos y debe tenerse en cuenta que cada programa de aplicación debe negociar con el sistema operativo para obtener un puerto del protocolo y un de puerto asociado antes de poder enviar un datagrama UDP.

UDP es capaz de gestionar mensajes de reportes de error mediante ICMP. Como recordará, uno de estos mensajes correspondía a la situación de Puerto Inaccesible: cuando UDP recibe un mensaje para un puerto que no existe, remite un mensaje de error y descarta el datagrama.

## Encapsulamiento UDP

El encapsulado de un datagrama UDP es muy similar al caso de ICMP. El datagrama UDP posee un encabezado UDP y un área de datos para el usuario, al pasar este datagrama a la capa de Internet, IP agrega su propio encabezado y el datagrama UDP pasa a formar parte del área de datos del paquete IP, una capa más abajo, en la capa de enlace, se encapsula en una trama de hardware en la cual se agrega el correspondiente encabezado de Hardware.



## Pseudo encabezado UDP

Cuando vimos el formato del datagrama UDP, hicimos una mención a una característica novedosa que posee el campo de Suma de Verificación del encabezado del mismo y dijimos que profundizaríamos ese concepto. Éste es el momento de hacerlo.

El encabezado de un paquete IP incluye un campo de Suma de Verificación (checksum), donde se computan sólo los campos del encabezado IP. Por lo tanto, IP no verifica el contenido de los datos del usuario que transporta dentro del paquete.

*La suma de verificación UDP, en cambio, sí computa en su campo de Suma de Verificación el contenido de los campos de Datos del Usuario.*

Es hasta ahora el primer elemento que verifica la integridad de los datos enviados por el usuario.

También forman parte de la suma de verificación de UDP todos los campos del datagrama UDP: dirección UDP del origen, dirección UDP del destino, Longitud del datagrama UDP y el mismo campo de suma de verificación que se computa como 0,..., hasta aquí todo bastante "normal"; sin embargo, la suma de verificación de UDP agrega cierta función de redundancia ya que también computa en dicha suma las direcciones IP de origen y destino.

Es por esto que se dice que UDP agrega un pseudo encabezado al datagrama UDP para realizar su suma de verificación.

Concretamente, forman parte de la suma de verificación UDP:

- Todos los campos del encabezado UDP (el campo de suma de verificación con valor 0).
- Los datos del usuario del datagrama UDP.
- El pseudo encabezado.
- Un byte de ceros (para completar dicho pseudo encabezado, de tal forma que sea un múltiplo exacto de 16 bits).

En este momento se preguntará varias cosas: ¿qué hay en el pseudo encabezado?, ¿por qué agregar ciertos datos en este pseudo encabezado para computar la suma de verificación UDP y por qué usar datos que corresponden a otra capa de protocolo, como la IP? ¿Viola esto último el principio de independencia de capas?

Primero respondamos la última pregunta: sí, la fuerte interdependencia que se da entre UDP e IP, obviamente, infringe la idea de estratificación por capas, "idealmente" independientes.

Veamos ahora por qué esto es necesario, lo que responderá las demás preguntas que seguramente se habrá planteado.

¿Qué hay en el pseudo encabezado UDP?

El siguiente es su formato:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
<b>Dirección IP de Origen</b>																															
<b>Dirección IP de destino</b>																															
<b>Cero (0)</b>	<b>Protocolo (17 para UDP)</b>										<b>Longitud datagrama UDP</b>																				

El pseudo encabezado UDP se forma con datos obtenidos por el *software* que ejecuta UDP, el cual los obtiene del encabezado IP.

Tanto la dirección IP de Origen como la de Destino y el Protocolo, son extraídos por el *software* UDP del encabezado IP. El valor que se almacena en el encabezado IP para determinar que el protocolo utilizado es UDP es el valor 17.

*¿Por qué la Suma de Verificación UDP contiene las direcciones de IP?*

IP se encarga de transmitir datagramas entre la capa Internet del *host* origen y del *host* destino; UDP se encarga de establecer comunicación entre el puerto de origen en el *host* que envía el mensaje y el puerto de destino en el *host* que lo recibe; por lo tanto si UDP sólo verificara el número de puerto, circunstancialmente podría estar enviando datagramas UDP al número de puerto correcto en un *host* equivocado. La mejor manera de discurrir esto es no pensar que la dirección del puerto de destino es sólo un número entero de 16 bits, como por ejemplo puerto 23, sino pensar que la dirección del puerto es la unión de la dirección IP del *host* destino con el número identificador del puerto, por ejemplo, un puerto destino podría ser:

{201.48.115.18 , 23}.

Donde la estructura sería la siguiente {dirección IP, número de puerto}

Y por lo tanto, es responsabilidad también de UDP verificar que se encuentra en el *host* destino correcto.

Quizá esto pueda parecerle distinto de los casos anteriores, pero si lo medita bien, verá que en realidad no es así: pensemos, por ejemplo, que la dirección IP consta de 2 partes: NetID y HostID.

El NetID es utilizado por las capas más bajas del modelo para rutear el datagrama hasta la red a la que pertenece el *host* destino, por ende una vez que el datagrama ha llegado al *host* destino y comienza a ascender desde la capa física hacia la de Internet donde reside IP, si confiáramos plenamente en la robustez del medio físico, no sería necesario que IP controlara en su suma de verificación al NetID, sólo sería necesario que lo hiciera con el HostId; pero -sin embargo- lo hace; ya que debe verificar que se encuentre en el *host* pertinente y en la red correspondiente. De la misma forma, UDP verifica que el datagrama se encuentre en el puerto correcto del *host* correcto de la red correcta.

Otro punto más que reafirma la fuerte interdependencia que se da entre UDP e IP, está dado por el hecho de que uno puede suponer que el usuario conoce la dirección IP del *host* destino, pero puede no conocer la dirección IP del *host* origen. Y como no la conoce, la capa de Aplicación no la conocerá UDP. ¿Cómo puede ser esto? Pensemos simplemente que un *host* puede estar conectado a más de una red, y que en ese caso será IP en la capa de Internet quien decidirá por cuál placa de red le conviene hacer el ruteo y, por lo tanto, asignará la dirección IP correspondiente al origen. Así que UDP necesitará solicitar a IP que le indique la dirección IP del *host* origen para computar la suma de verificación inevitablemente.



¿Estás listo para un desafío?

**1. Indique la opción correcta**

La cabecera UDP esta formada por dos palabras de 32 bits.

- Verdadero
- Falso

**2. Indique la opción correcta**

UDP usa 16 bits de los 32 de la primera palabra de la cabecera para identificar los "Puerto Origen" y otros 16 para identificar el "Puerto Destino".

- Verdadero
- Falso

**3. Indique la opción correcta**

UDP emplea acuse de recibo para asegurarse de que lleguen los mensajes.

- Verdadero
- Falso

**4. Indique la opción correcta**

Si UDP es un protocolo inseguro, la razón los programadores de aplicación eligen UDP como un servicio de transporte de datos es que, si la cantidad de datos transmitidos es pequeña, la sobrecarga (overhead) para el establecimiento de la conexión y la seguridad de una entrega confiable puede ser mayor que el trabajo de retransmisión completa del conjunto de datos.

- Verdadero
- Falso

**5. Indique la opción correcta**

Dado que UDP es un protocolo inseguro, los programas de aplicación que utilizan UDP, aceptan toda la responsabilidad por el manejo de los problemas de confiabilidad, incluyendo:

- La pérdida, duplicación y retraso de mensajes.

- La entrega fuera de orden.
- La pérdida de conectividad.
- Todas las anteriores.

#### 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Puerto Origen y Puerto Destino	contiene la cantidad de Bytes del datagrama
Campo de longitud	proporciona la única manera de garantizar que los datos lleguen intactos
Campo Checksum	proceso que se realiza a través de los puertos
Multiplexado	identifican los puntos terminales de la conexión

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

La cabecera UDP esta formada por dos palabras de 32 bits.

Verdadero

Falso

## 2. Indique la opción correcta

UDP usa 16 bits de los 32 de la primera palabra de la cabecera para identificar los "Puerto Origen" y otros 16 para identificar el "Puerto Destino".

Verdadero

Falso

## 3. Indique la opción correcta

UDP emplea acuse de recibo para asegurarse de que lleguen los mensajes.

Verdadero

Falso

## 4. Indique la opción correcta

Si UDP es un protocolo inseguro, la razón los programadores de aplicación eligen UDP como un servicio de transporte de datos es que, si la cantidad de datos transmitidos es pequeña, la sobrecarga (overhead) para el establecimiento de la conexión y la seguridad de una entrega confiable puede ser mayor que el trabajo de retransmisión completa del conjunto de datos.

Verdadero

Falso

## 5. Indique la opción correcta

Dado que UDP es un protocolo inseguro, los programas de aplicación que utilizan UDP, aceptan toda la responsabilidad por el manejo de los problemas de confiabilidad, incluyendo:

La pérdida, duplicación y retraso de mensajes.

La entrega fuera de orden.

La pérdida de conectividad.

Todas las anteriores.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Puerto Origen y  
Puerto Destino

identifican los puntos terminales  
de la conexión

Campo de longitud

contiene la cantidad de Bytes del  
datagrama

Campo Checksum

proporciona la única manera de  
garantizar que los datos lleguen  
intactos

Multiplexado

proceso que se realiza a través de los puertos

# SP10 / H3: Protocolo de Control de Transmisión - TCP

Hemos visto anteriormente uno de los protocolos que residen en la capa de transporte del modelo TC-P/IP, el protocolo de datagrama de usuario o UDP.

Este protocolo está orientado a ser un servicio sin conexión, no confiable, lo cual indica que los datagramas enviados pueden perderse o llegar fuera del orden.

El otro protocolo residente también en la capa de transporte, el Protocolo de Control de Transmisión o TCP, que ofrece un servicio orientado a la conexión, de características confiables, y con control de flujo de datos. TCP asegura la entrega y la recepción en la secuencia correcta de los datos.

Recordemos que TCP utilizará el IP como servicio de entrega, esto puede plantearle ciertos interrogantes:

¿Cómo es posible que TCP empleando el sistema de entrega IP, que es un protocolo no confiable, garantice la confiabilidad a las aplicaciones superiores?

¿Cómo es posible que TCP esté orientada a conexión, mientras que IP no?

¿Cómo puede ser que TCP entregue datos como flujo de Bytes si usa datagramas IP como servicio de entrega?

Estos son los temas que se tratarán en esta Situación Profesional.

Usar un sistema de entrega sin conexión y no confiable para las transferencias de grandes volúmenes de datos se vuelve tedioso, molesto y requiere que los programadores incorporen en cada programa de aplicación la detección y solución de errores. Debido a esto es que se ha desarrollado el TCP, lo que posibilita a los programadores utilizar el servicio de flujo confiable sin tener que implementarlo en cada aplicación.

Las aplicaciones que requieren el protocolo de transporte para proveer entrega confiable de datos, usan TCP debido a que éste asegura que los datos son fielmente entregados a través de la red y en la secuencia apropiada.

TCP es un protocolo que se diseñó para tolerar el funcionamiento de redes inseguras. Asociado a éste se creó el protocolo de capa de red IP que ya hemos visto.

## Características generales del TCP

Las siguientes son las funciones que caracterizan a TCP como un servicio de entrega confiable.

### Orientación de flujo

Cuando dos programas de aplicación o procesos de usuario transfieren datos esperan enviar y recibir como un flujo de bits, divididos en Bytes. El servicio de entrega de flujo en la máquina de destino pasa al receptor exactamente la misma secuencia de Bytes que le pase el transmisor en la máquina de origen.

### Conexión de circuito virtual

En una transferencia de flujo de bits, conceptualmente, una aplicación realizada una "llamada", que la otra tiene que aceptar. Los protocolos TCP en los dos sistemas operativos se comunican enviándose mensajes a través de la Internet, verificando que la transferencia esté autorizada y que los dos extremos estén listos (orientación a la conexión). Una vez que se establecen todos los detalles, los módulos de protocolo TCP informan los programas de aplicación que ha establecido una conexión, y que la transferencia puede comenzar (arranque confiable). Durante la transferencia, el software TCP en cada una de las máquinas continúa la comunicación

para verificar que los datos se reciben correctamente.

Se utiliza el término "círculo virtual" para describir que dichas conexiones son vistas por los programas de aplicación como si fueran reales (físicas, a niveles hardware), aunque en realidad el servicio de entrega final está orientado a la no conexión. Las conexiones de TCP son virtuales porque, en realidad, se realizan por software, no por hardware.

## Flujo no estructurado

El servicio de flujo TCP IP no está obligado a formar flujos estructurados de datos; por ejemplo, no existe forma para que una aplicación de nómina de empleados haga que un servicio de flujo marque límites entre los registros de cada empleado, o que identifique el contenido del flujo de Bytes como campos distintos de una nómina (apellido, nombre, fecha de ingreso). Los programas de aplicación que utilizan el servicio de flujo deben entender el contenido del mismo y ponerse de acuerdo sobre su formato antes de iniciar una conexión.

## Transferencia con memoria intermedia

- **Comunicación Punto a Punto (o terminal a terminal):** se describe de esta forma que la comunicación TCP tiene dos puntos terminales.
- **Conexión full dúplex:** las conexiones TCP permiten que los datos fluyan en ambos sentidos y que cualquiera de los programas de aplicación transmita en cualquier momento. Como TCP maneja el búfer de los datos de entrada y salida en ambos sentidos, las aplicaciones pueden enviar datos y luego reanudar los cálculos.

En base a las características anteriores, las aplicaciones solicitan que TCP establezca la conexión, transmita, reciba y cierre la conexión.

## Confiabilidad

Unos párrafos más arriba planteamos el problema sobre cómo hace TCP para ofrecer un servicio confiable, cuando utiliza como elemento de transmisión a IP, que es no confiable: la solución es sencilla; agregando confirmaciones de recepción de los mensajes; si un mensaje no llegó a destino, simplemente se retransmite.

Estas confirmaciones se gestionan mediante el software TCP, lo cual hace que el servicio sea algo más lento (siempre habrá una disminución de la performance al implementar confiabilidad mediante software).

La mayoría de los protocolos confiables utilizan una técnica fundamental conocida como acuse de recibo positivo con retransmisión.

Esta técnica se basa en la siguiente idea: supongamos que un host emite un mensaje y el mismo llega al receptor; en ese momento el receptor envía un paquete distinto: denominado acuse de recibo (ACK). El host que inició la comunicación espera hasta recibir este acuse de recibo y al momento de recibirla habilita la opción de enviar un segundo mensaje.

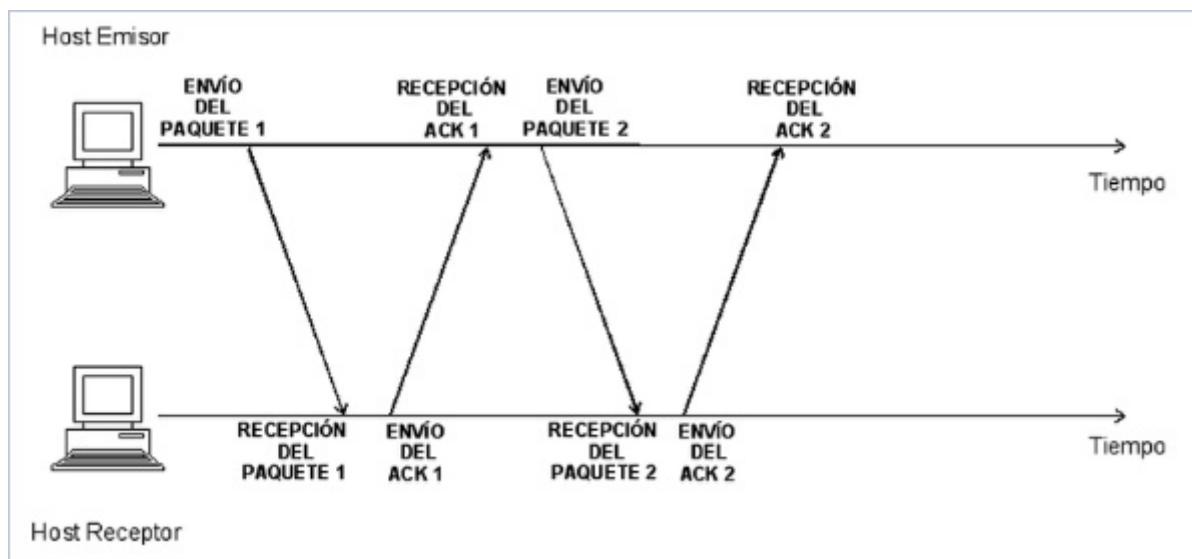
Una entidad de transporte TCP acepta mensajes de longitud arbitrariamente grandes procedente de los procesos de usuarios, los separa en trozos (segmentos) que no excedan de 64 Kbytes y transmite cada segmento como si fuera un datagrama separado.

La capa de red no garantiza que los datagramas se entreguen correctamente, por lo que TCP debe utilizar temporizadores y retransmitir los datagramas si es necesario.

Los datagramas que consiguen llegar pueden hacerlo en desorden y dependerá de TCP el re ensamblarlos en mensajes, con la secuencia correcta. Cada segmento transmitido por TCP tiene su propio número de secuencia

privado. El espacio de número de secuencia tiene una extensión de 32 bits, para asegurar que los duplicados antiguos hayan desaparecido.

TCP es un protocolo trenes de bytes, seguro y orientado a conexión. Vamos a ver cada uno de los términos: seguro, orientado a conexión y trenes de bytes (*byte stream*) con más detalles.



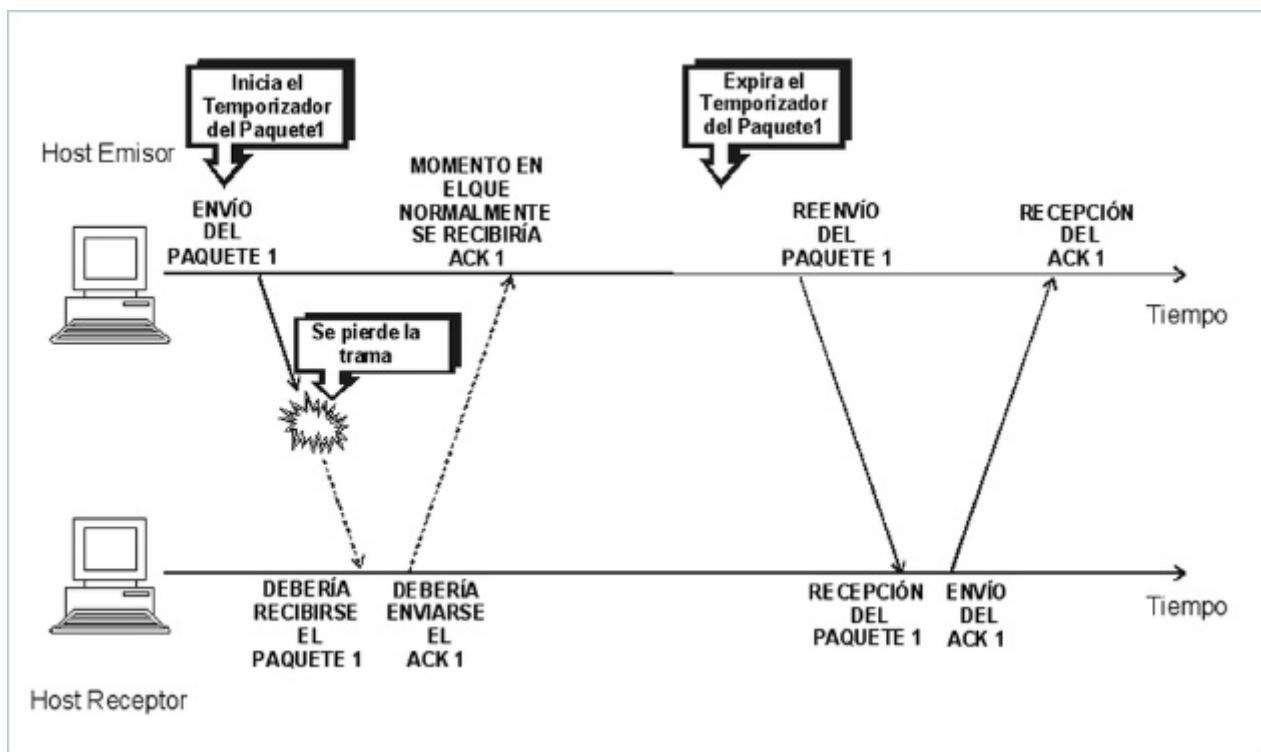
Puede observarse en la figura la comunicación con Acuses de Recibo ACK

TCP provee seguridad con un mecanismo llamado "Reconocimiento Positivo con Retransmisión" (PAR = Positive Acknowledgement with Retransmission). Indicado simplemente, un sistema que usa PAR envía los datos nuevamente, a menos que éste escuche desde el sistema remoto que los datos han arribado correctamente.

La unidad de datos intercambiada entre módulos TCP cooperativos es llamado "segmento". La figura anterior muestra este procedimiento.

Agreguemos un poco de complejidad al problema, ¿qué pasa si el paquete enviado se pierde?

Cuando el emisor envía el paquete, pone en funcionamiento un temporizador o reloj de cuenta regresiva; si el acuse de recibo no llega antes que el temporizador llegue a cero, el emisor supone que el paquete se perdió y lo retransmite. La siguiente figura muestra este concepto.



Puede observarse en la figura la representación de la pérdida de un paquete: tiempo excedido y retransmisión  
Se preguntará ¿cuánto debe esperar el emisor al mensaje de confirmación de acuse de recibo? ¿Cuánto es un tiempo razonable?

Si estamos hablando de una red de área local, unos pocos milisegundos son un valor aceptable, pero ¿qué pasa con una red abierta, con una Internet?

Obviamente que TCP no puede conocer los retardos exactos de todas las partes de Internet en todo momento. En cambio estima un retardo de ida y vuelta para cada conexión, midiendo el tiempo necesario para recibir una respuesta.

Cada vez que transmite un mensaje del que espera respuesta, TCP registra el momento de la emisión, al llegar la respuesta, resta ambos momentos. De esta forma posee un tiempo estimado del retardo de ida y vuelta de esa conexión. A medida que transmite paquetes y recibe acuses, TCP produce una secuencia de estimados de ida y vuelta y, mediante una función estadística, se genera un promedio ponderado. Además de este promedio, TCP guarda un estimado de la variación y emplea como medida de retransmisión una combinación lineal de ésta y la medida estimada.

La experiencia ha demostrado que la retransmisión adaptable de TCP funciona bien, la variación permite a TCP reaccionar con rapidez, cuando aumenta el retardo después de una ráfaga de paquetes. Con el promedio ponderado, TCP re establece el cronómetro de retransmisión si el retardo regresa una medida menor tras una ráfaga temporal. Cuando el retardo es constante, TCP ajusta la expiración de retransmisión a una cifra ligeramente mayor que el retardo medio. Al comenzar a variar los retardos, TCP ajusta la expiración de retransmisión a una cifra mayor que la media para adecuarse a los posibles picos.

El último problema referido a la confiabilidad sucede cuando un sistema de entrega de paquetes los duplica. Los duplicados pueden surgir cuando las redes tienen grandes retrasos que provocan una retransmisión prematura. Para complicar el problema, tenga en cuenta que tanto los paquetes como los acuses de recibo se

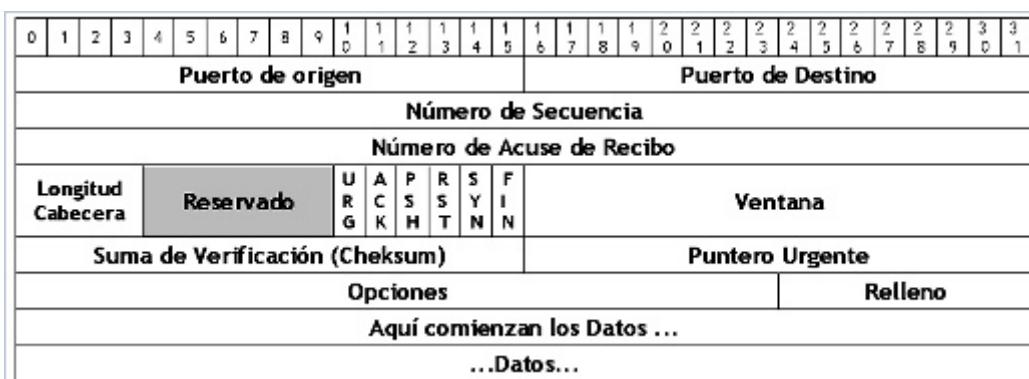
pueden duplicar. Por lo general, los protocolos confiables detectan los paquetes duplicados asignándole a cada uno un número de secuencia y al obligar al receptor a recordar qué números de secuencia recibe. Para evitar la confusión causada por acuses de recibo retrasados o duplicados, los protocolos envían los números de secuencia dentro de los acuses, para que el receptor pueda asociar correctamente los acuses de recibo con los paquetes.

Unos párrafos más arriba planteamos el problema sobre cómo hace TCP para ofrecer un servicio confiable cuando utiliza como elemento de transmisión a IP, que es no confiable: la solución es sencilla, agregando confirmaciones de recepción de los mensajes; si un mensaje no llegó a destino; simplemente se retransmite.

## Formato de un segmento TCP

Ahora está en condiciones de comprender los elementos que componen un segmento TCP.

En la figura se muestra la cabecera que utiliza TCP:



## Significado de los campos de la cabecera del segmento TCP

- Puerto Origen y Destino: identifican los puntos terminales de la conexión. Cada Host debe decidir por sí mismo como asignar sus puertos.
- Número de Secuencia: indica la secuencia con respecto a la transmisión total del primer byte de datos en el área de datos del segmento TCP.
- Número de Acuse de Recibo: identifica el siguiente Byte de datos que espera recibir en el flujo de datos. El emisor envía el reconocimiento (ACK) del segmento recibido anteriormente.
- Longitud de la Cabecera: indica el número de palabras de 32 bits que están contenidas en la cabecera.
- Banderas: compuesta por 6 Flag de 1 bit cada uno.

Descripción de las banderas o Flag					
URG	ACK	PSH	RST	SYN	FIN

"Banderas" | *Elaboración autor*

- URG: le indica al receptor que el mensaje es Urgente, y que por lo tanto debe procesar primero los datos marcados como tales por el puntero de Urgencia. Si el Puntero Urgente está en uso, entonces URG se coloca en 1.
- ACK: indica que el mensaje es de confirmación o acuse de recibo, y que, por lo tanto, el valor contenido en el Campo Número de Acuse de Recibo es válido.
- PSH: le indica al TCP del receptor que debe enviar los datos de inmediato a la Aplicación en el destino. En definitiva le indica que los mismos no deben pasar por el buffer de entrada. Por ejemplo, típicamente la utiliza Telnet.
- RST: le indica al receptor que debe re establecer la conexión TCP.
- SYN: el bit SYN se utiliza para el establecimiento de conexiones. Solicita al TCP del receptor que sincronice los números de secuencia para establecer el circuito virtual. La solicitud de conexión se realiza con el bit SYN = 1 y ACK = 0. La respuesta a la solicitud de conexión es SYN = 1 y ACK = 1.
- FIN: le indica al receptor que ha concluido la transmisión de datos. Esta bandera sólo cierra el flujo de datos en el sentido en el cual viaja. Para cerrar la conexión "el otro extremo" también debe enviar un mensaje con bandera FIN activada.
- Ventana: contiene el número de bytes que están en tránsito en la red sin confirmación. La ventana indica al emisor que puede continuar enviando segmentos mientras el número total de bytes que se ha enviado es menor que la "ventana" que el receptor puede aceptar. El receptor controla el flujo del emisor cambiando el tamaño de la ventana. Una ventana cero comunica al emisor que cese la transmisión hasta que reciba una ventana de valor distinto de cero. El control de flujo en TCP se realiza mediante este campo Ventana de 16 bits.
- Suma de Verificación: cada uno de los segmentos contiene un "checksum" que el receptor usa para verificar que los datos no han sido dañados. Si el segmento de datos es recibido sin daños, el receptor envía un "reconocimiento positivo" al emisor. Si el segmento de datos ha sido dañado, el receptor los descarta. Después de un período de tiempo apropiado (time-out), el módulo TCP emisor retransmite cualquier segmento para el cual no ha habido algún reconocimiento positivo.
- Puntero Urgente: apunta hacia el último Byte de datos urgentes en el área de datos TCP. El Puntero Urgente se usa para indicar un desplazamiento en bytes a partir del número de secuencia actual en el que se encuentran datos urgentes.
- Opciones: generalmente se utiliza con la Opción Tamaño Máximo de Segmento, la cual señala el tamaño más grande de segmento que espera recibir el módulo TCP que la emite. El campo Opciones se utiliza para diferentes cosas, por ejemplo para comunicar tamaño de buffers durante el procedimiento de establecimiento.



¡Vamos a comprobar cuánto aprendiste!

**1. Indique la opción correcta**

La mayoría de los protocolos confiables utilizan una técnica fundamental, conocida como acuse de recibo positivo con retransmisión.

- Verdadero
- Falso

**2. Indique la opción correcta**

El mecanismo que utiliza TCP para que la entrega de datagramas pueda ordenarse en el destino es el siguiente: cada segmento transmitido por TCP tiene su propio número de secuencia privado. El espacio de número de secuencia tiene una extensión de 32 bits, para asegurar que los duplicados antiguos hayan desaparecido.

- Verdadero
- Falso

**3. Indique la opción correcta**

La función de la Bandera SYN en la cabecera TCP se utiliza para el establecimiento de conexiones. Solicita al TCP del receptor que sincronice los números de secuencia para establecer el circuito virtual.

- Verdadero
- Falso

**4. Indique la opción correcta**

En la cabecera TCP la función de la ventana es contener el número de bytes que están en tránsito en la red sin confirmación.

- Verdadero
- Falso

**5. Indique la opción correcta**

Las funciones que caracteriza a TCP como un servicio de entrega confiable es:

- Orientación de flujo.
- Conexión de circuito virtual.
- Flujo no estructurado.
- Todas las anteriores.

#### 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Orientación de flujo

en el host destino pasa al receptor la misma secuencia de bytes que le pase el transmisor en el host origen.

Conexión de circuito virtual

el servicio TCP/IP no está obligado a formar flujos estructurados de datos.

Flujo no estructurado

verifica que la transferencia esté autorizada y que los dos extremos estén listos.

Confiabilidad

se consigue agregando confirmaciones de recepción de los mensajes.

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

La mayoría de los protocolos confiables utilizan una técnica fundamental, conocida como acuse de recibo positivo con retransmisión.

- Verdadero
- Falso

## 2. Indique la opción correcta

El mecanismo que utiliza TCP para que la entrega de datagramas pueda ordenarse en el destino es el siguiente: cada segmento transmitido por TCP tiene su propio número de secuencia privado. El espacio de número de secuencia tiene una extensión de 32 bits, para asegurar que los duplicados antiguos hayan desaparecido.

- Verdadero
- Falso

## 3. Indique la opción correcta

La función de la Bandera SYN en la cabecera TCP se utiliza para el establecimiento de conexiones. Solicita al TCP del receptor que sincronice los números de secuencia para establecer el circuito virtual.

- Verdadero
- Falso

## 4. Indique la opción correcta

En la cabecera TCP la función de la ventana es contener el número de bytes que están en tránsito en la red sin confirmación.

- Verdadero
- Falso

## 5. Indique la opción correcta

Las funciones que caracteriza a TCP como un servicio de entrega confiable es:

- Orientación de flujo.
- Conexión de circuito virtual.
- Flujo no estructurado.
- Todas las anteriores.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Orientación de flujo

en el host destino pasa al receptor la misma secuencia de bytes que le pase el transmisor en el host origen.

Conexión de circuito virtual

verifica que la transferencia esté autorizada y que los dos extremos estén listos.

Flujo no  
estructurado

el servicio TCP/IP no está obligado a formar flujos estructurados de datos. se consigue agregando confirmaciones de recepción de los mensajes.

Confiabilidad

# SP10 / H4: Mecanismos de establecimiento y fin de conexión

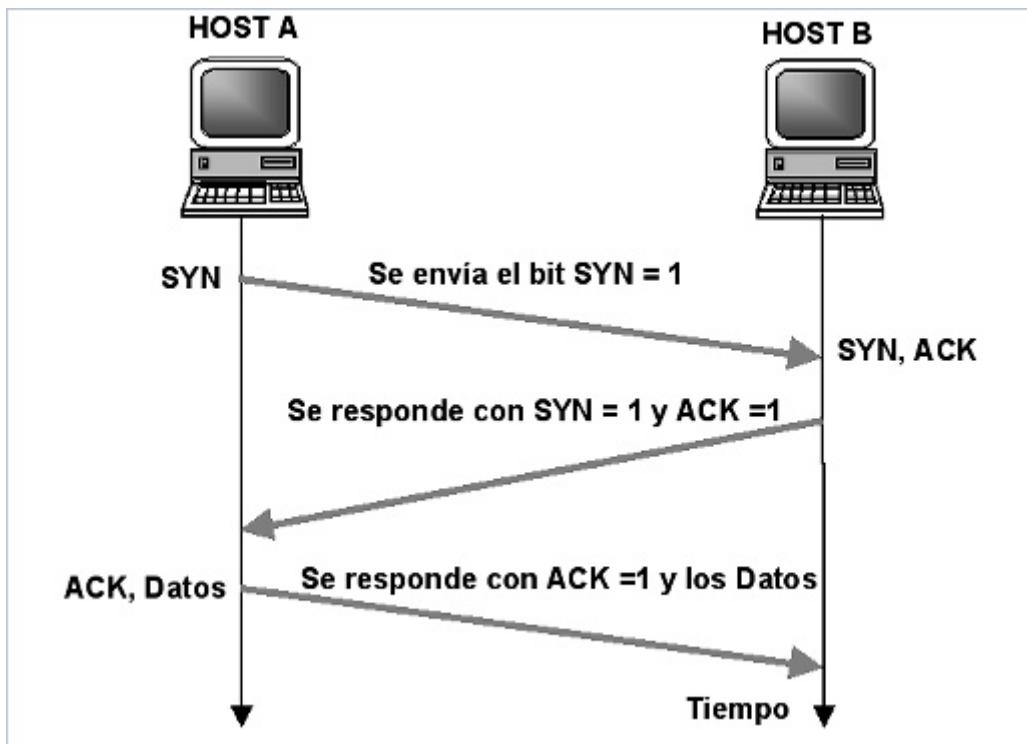
## Negociación a tres vías

TCP es un protocolo orientado a conexión. Éste establece una conexión lógica extremo a extremo entre dos host. La información de control, llamado "*handshake*", es intercambiada entre los puntos finales para establecer un diálogo antes de transmitir los datos. TCP indica la función de control de un segmento colocando el bit SYN en el campo "Flag" en la palabra 4 del encabezamiento del segmento.

El tipo de *handshake* usado por TCP es llamado "*handshake a tres vías*" debido a que son intercambiados tres segmentos. La figura siguiente muestra la simplicidad del "*handshake a tres vías*".

El Host "A" comienza la conexión enviando un segmento al Host "B" con el bit SYN "Número de Secuencia de Sincronización" (SYN = Syn-chronize Sequence Number) en 1 (on).

Este segmento comunica al Host "B", que el Host "A" desea establecer una conexión y comunica a "B" que el número de secuencia del Host "A" puede usar como número de comienzo este segmento (el número de secuencia es usado para mantener los datos en el orden apropiado).



El Host "B" responde a "A" con un segmento que tiene los bits de "Reconocimiento" (ACK = Acknow-ledgement) y el bit SYN puestos en 1 (on). El segmento B reconoce la recepción del segmento A e informa a "A" con cual "Número de Secuencia" comenzar el Host "B".

Finalmente, el Host "A" envía un segmento que reconoce la recepción del segmento B y transfiere los primeros datos.

Luego de este intercambio, el TCP del Host "A" tiene una evidencia positiva de que el TCP remoto está activo

y listo para recibir datos. Tan pronto como la conexión es establecida, los datos pueden ser transferidos.

Cuando los módulos cooperativos han concluido la transferencia de datos, pueden intercambiar un "handshake a tres vías" con los segmentos conteniendo el bit de "No más datos" (llamado el bit FIN) para cerrar la conexión. Este es el intercambio extremo a extremo de datos que provee la conexión lógica entre los dos sistemas.

TCP ve a los datos que envía como un "tren continuo de bytes", no como paquetes independientes. Además, TCP toma cuidado de mantener la secuencia en la cual los bytes son enviados y recibidos. Los campos "Número de Secuencia" y el "Número de Reconocimiento" en el encabezamiento del segmento TCP mantienen la pista de los bytes.

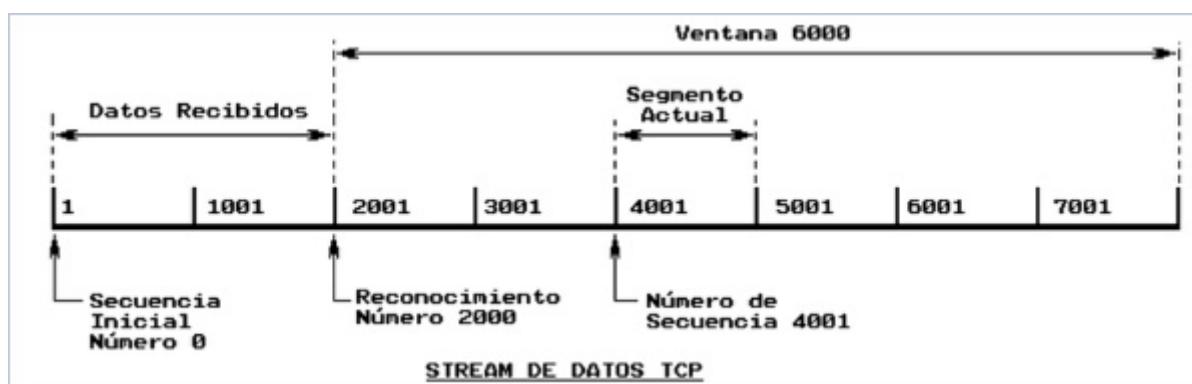
El TCP estándar no requiere que cada sistema comience numerando los bytes con algún número específico; cada sistema elige el número que puede usar como punto de comienzo.

Para mantener la pista del tren de bytes correctamente, cada extremo de la conexión sincroniza el sistema de numeración de bytes intercambiando el bit SYN durante los segmentos de handshake. El campo "Número de Secuencia" en el segmento SYN contiene el "Número de Secuencia Inicial" (ISN = *Initial Sequence Number*), el cual es el punto de comienzo para el sistema de numeración de bytes. Aunque no es requerido por el protocolo estándar, el ISN es usualmente 0 (cero).

Cada byte de datos es numerado secuencialmente a partir del ISN, de modo que el primer byte real de datos enviado tiene un número de secuencia "ISN + 1" (usualmente 1). El Número de Secuencia en el encabezamiento del segmento de datos identifica la posición secuencial en el tren de datos del primer byte de datos en el segmento. Por ejemplo, si el primer byte en el tren de datos tiene número de secuencia 1 (ISN = 0) y han sido transferidos anteriormente 4000 bytes de datos, entonces el primer byte de datos en el segmento actual es el byte 4001 y el Número de Secuencia debiera ser 4001.

El segmento Reconocimiento (ACK) realiza dos funciones: "reconocimiento positivo" y "control de flujo". El reconocimiento comunica al emisor cuántos datos han sido recibidos y cuántos más puede aceptar el receptor. El Número de Reconocimiento es el número de secuencia del último byte recibido en el extremo remoto. El estándar no requiere un reconocimiento individual para todos los paquetes. El número de reconocimiento es un reconocimiento positivo de todos los bytes hasta ese número. Por ejemplo, si el primer byte enviado fue numerado como 1 y han sido exitosamente recibidos 2000 bytes, el Número de Reconocimiento debiera ser 2000.

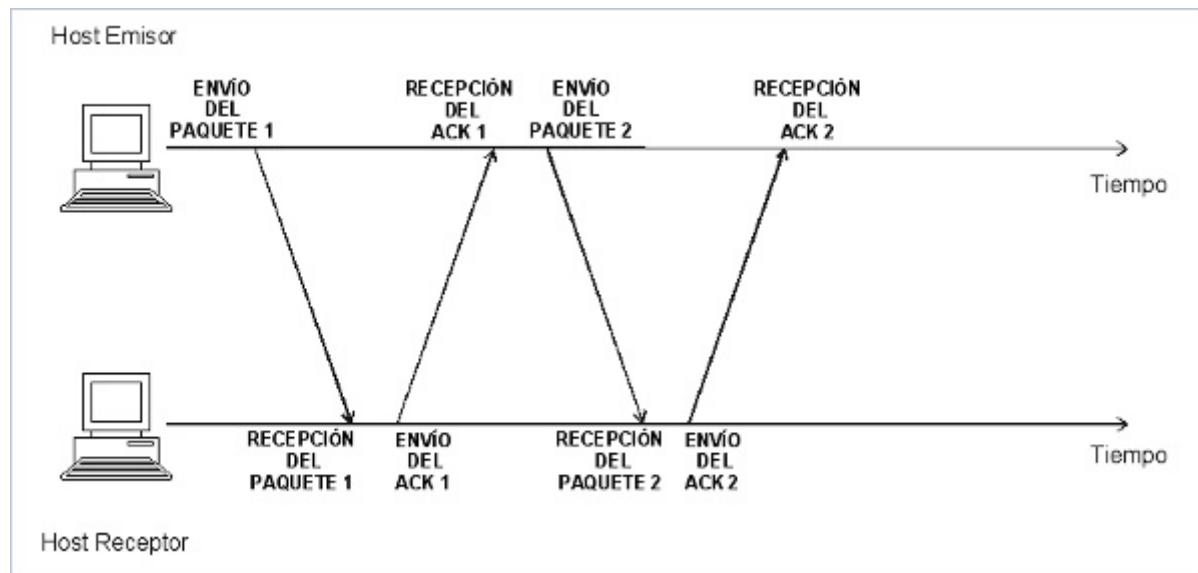
La figura siguiente muestra un tren de datos TCP (Bytes) que comienza con un "Número de Secuencia Inicial" de 0.



El sistema receptor ha recibido y reconocido 2000 bytes, de modo que el Número de Reconocimiento actual

es 2000. El receptor también tiene suficiente espacio de buffer para otros 6000 bytes, lo que puede advertirse por la ventana 6000.

El emisor está enviando actualmente un segmento de 1000 bytes, comenzando con el Número de Secuencia 4001. El emisor no ha recibido reconocimientos para los bytes 2001, pero continua enviando datos mientras está dentro de la ventana. Si el emisor completa la ventana y no recibe reconocimientos de los datos enviados previamente, éste puede, luego de un tiempo apropiado (time-out) enviar los datos comenzando nuevamente desde el primer byte no reconocido. En la figura que a continuación vemos, la retransmisión puede comenzar desde el byte 2001, si no se han recibido nuevos reconocimientos. Este procedimiento asegura que los datos son efectivamente recibidos en el extremo remoto de la red.





¿Te animás a medir cuánto aprendiste?

**1. Indique la opción correcta**

El tipo de handshake usado por TCP es llamado "handshake a tres vías", debido a que son intercambiados tres segmentos.

- Verdadero
- Falso

**2. Indique la opción correcta**

La conexión TCP comienza enviando un segmento con el bit SYN en 1.

- Verdadero
- Falso

**3. Indique la opción correcta**

La conexión TCP termina enviando un segmento con el bit FIN en 0.

- Verdadero
- Falso

**4. Indique la opción correcta**

TCP ve a los datos que envía como "paquetes independientes" y no como "un tren continuo de bytes".

- Verdadero
- Falso

**5. Indique la opción correcta**

El segmento Reconocimiento (ACK) permite realizar la siguiente función:

- Reconocimiento positivo.
- Control de flujo.
- Todas las anteriores.
- Ninguna de las anteriores.

**6. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Handshake	es el numero de secuencia inicial o punto de comienzo para el sistema de numeración de bytes.
ISN	es el número de secuencia de sincronización con el que un host comienza la conexión.
ACK	es la información de control intercambiada entre los puntos finales.
SYN	es el segmento de reconocimiento que realiza reconocimiento positivo y control de flujo.

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

El tipo de handshake usado por TCP es llamado "handshake a tres vías", debido a que son intercambiados tres segmentos.

- Verdadero
- Falso

## 2. Indique la opción correcta

La conexión TCP comienza enviando un segmento con el bit SYN en 1.

- Verdadero
- Falso

## 3. Indique la opción correcta

La conexión TCP termina enviando un segmento con el bit FIN en 0.

- Verdadero
- Falso

## 4. Indique la opción correcta

TCP ve a los datos que envía como "paquetes independientes" y no como "un tren continuo de bytes".

- Verdadero
- Falso

## 5. Indique la opción correcta

El segmento Reconocimiento (ACK) permite realizar la siguiente función:

- Reconocimiento positivo.
- Control de flujo.
- Todas las anteriores.
- Ninguna de las anteriores.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Handshake

es la información de control intercambiada entre los puntos finales.

ISN

es el numero de secuencia inicial o punto de comienzo para el sistema de numeración de bytes.

ACK

es el segmento de reconocimiento que realiza reconocimiento positivo y control de flujo.

SYN

es el número de secuencia de sincronización con el que un host comienza la conexión.

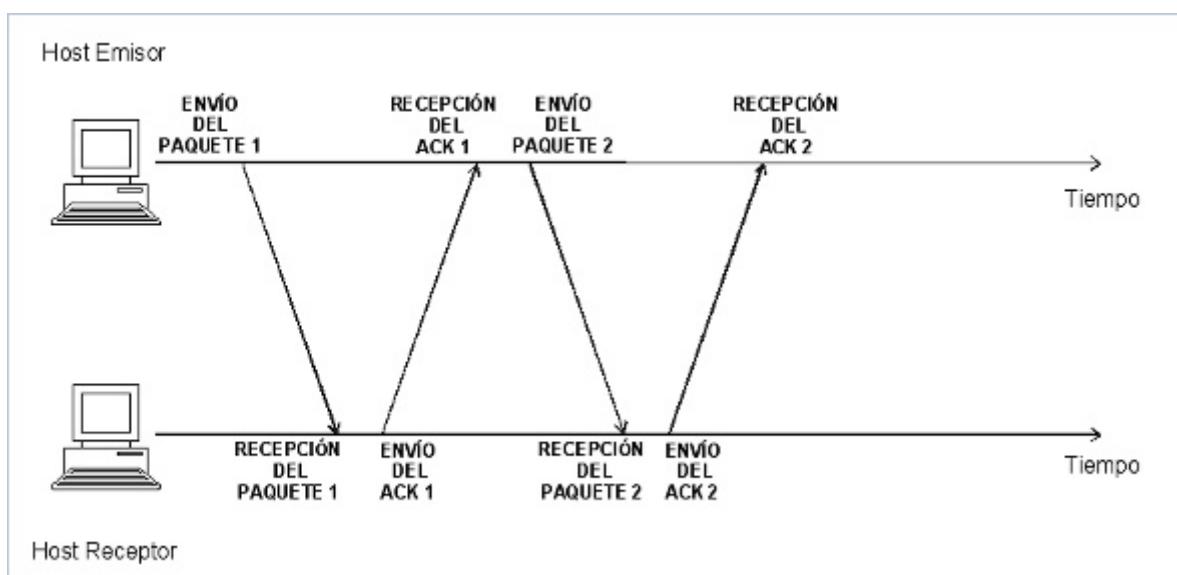
# SP10 / H5: Mecanismos para control de flujo

## Las ventanas deslizables

Si bien se produce en los dos sentidos no se produce en ambos sentidos al mismo tiempo. En la figura se observa que el emisor envía un paquete y se queda esperando el acuse de recibo (ACK) correspondiente a ese paquete, el receptor lo recibe y devuelve el acuse de recibo; recién cuando el emisor recibe este acuse de recibo, se encuentra en condiciones de enviar el próximo paquete. Obviamente que un sistema de este tipo consigue dos objetivos. Confiabilidad y control de flujo (ya que el flujo de datos es controlado por los acuses de recibo).

Sin embargo, debemos admitir que un sistema de este tipo no aprovecha muy bien el ancho de banda del medio de transmisión (si bien ya sabe que el ancho de banda está referido a la gama de frecuencias que un medio permite que lo atraviesen; en este contexto se refiere más que nada a la velocidad de transferencia, es decir, a la cantidad de bits por segundo que se pueden enviar por el medio de transmisión), ya que en cualquier instante de tiempo sólo un mensaje estará en tránsito: ya sea un paquete enviado por el emisor o un acuse de recibo enviado por el receptor.

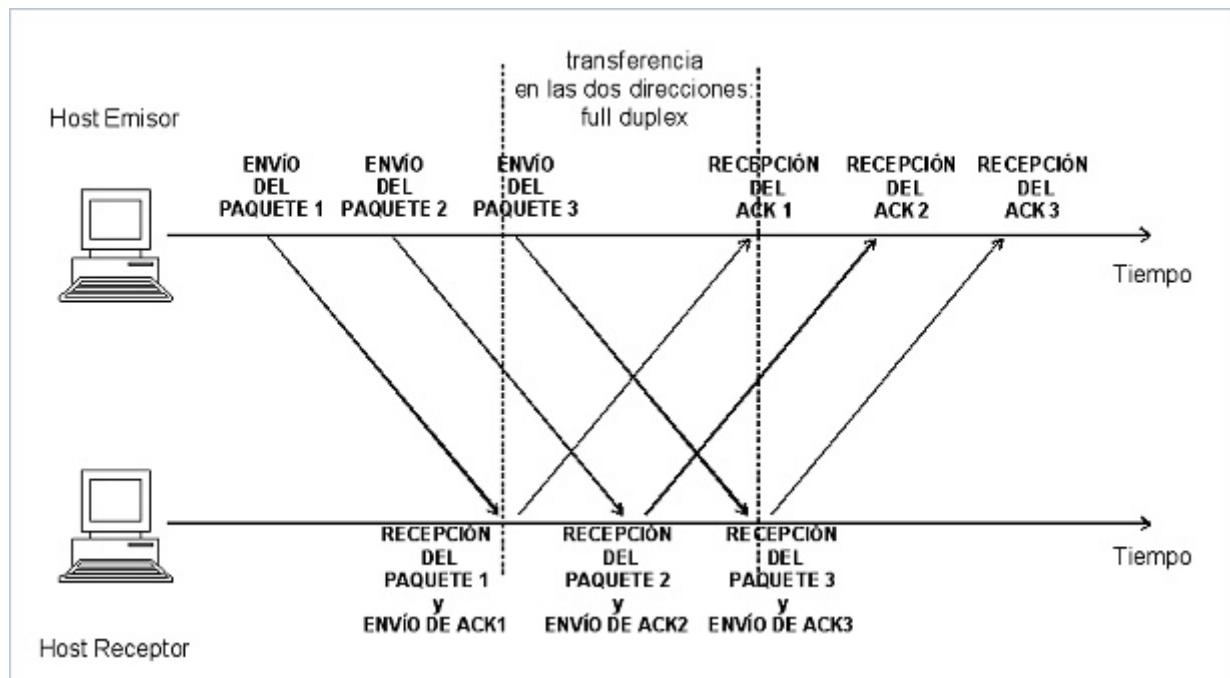
Como podrá darse cuenta fácilmente, esta no es la forma real en que se implementan las comunicaciones bajo TCP/IP.



Puede observar en la figura la comunicación con acuses de recibo (ACK)

Para mejorar el aprovechamiento del ancho de banda del medio hay que permitir que se produzca un flujo de bits en ambos sentidos del medio en forma simultánea, lo que se denomina comunicación full duplex.

En vez de exigir al emisor que envíe de a un segmento por vez y que permanezca en espera hasta recibir el correspondiente acuse de recibo, podemos flexibilizar esta regla y permitir que el emisor emita más de un paquete y que luego permanezca en espera de sus acuses de recibo, como se grafica en la siguiente figura:



Puede observarse en la figura una ventana deslizante de 3 paquetes

En la figura anterior se ha mostrado el caso en el cual se permite al emisor enviar 3 paquetes antes de recibir acuse de recibo. Como se puede observar en la zona delimitada por las líneas verticales de puntos, existe un intervalo de tiempo en el cual las comunicaciones fluyen en ambos sentidos. Esto hace un mejor aprovechamiento de la capacidad de transmisión del medio. A este tipo de procedimiento, se lo denomina de ventana deslizante.

Es muy importante tener en cuenta que el TCP del lado del emisor recibe el mensaje de la aplicación como un flujo de Bytes y que de esa forma espera recibir el mensaje la aplicación del lado del receptor. El hecho de que el TCP del emisor organice dichos bytes en segmentos se debe primordialmente a que, si bien hacia la capa de aplicación TCP debe verse como un servicio orientado a la conexión, la realidad es que las capas inferiores sólo ofrecen un servicio no orientado a la conexión. En el concepto de ventana deslizante se basa el control del flujo de Bytes de TCP.

## Buffers y control de flujo

Un punto importante para tener en cuenta es que tanto el emisor como el receptor cuentan con buffers donde almacenan los datos de entrada. En el caso del emisor, allí se almacenan los Bytes del mensaje de la aplicación; en el caso del receptor, se almacenan los bytes que llegan en los paquetes remitidos.

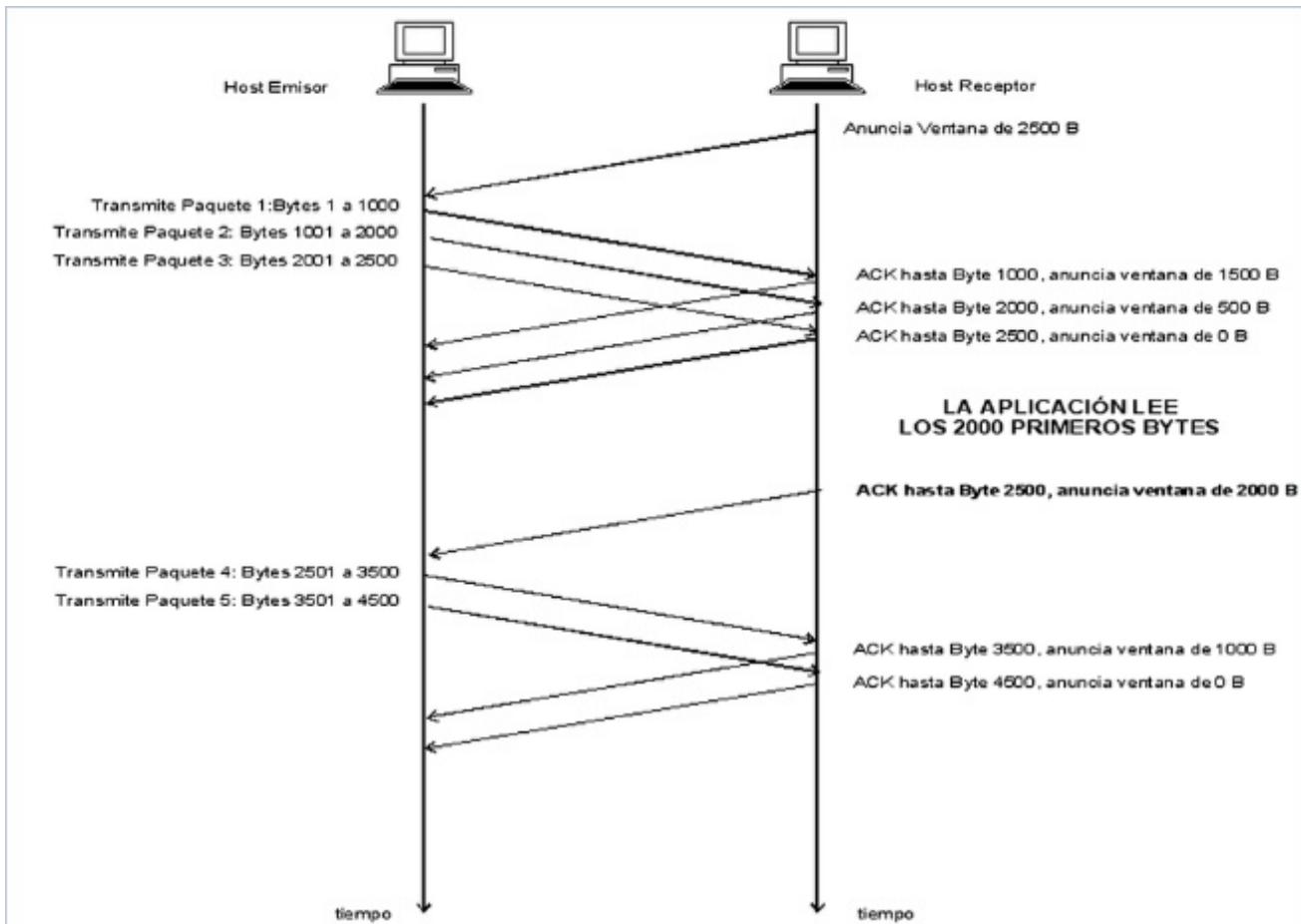
En el caso del emisor, la aplicación remite los bytes al buffer del TCP en el emisor, el cual los retiene hasta que está habilitado para enviarlos.

En el caso del receptor, almacena en los buffers los bytes que le van llegando, hasta que pueda procesarlos y enviarlos a la aplicación en el receptor. En este último punto es muy importante comprender que el hecho de que el TCP del receptor reciba los paquetes, no significa que éstos hayan sido procesados y enviados a la aplicación, lo cual indica que estos buffers pueden saturarse.

En el momento en el cual se establece la comunicación, ambos protocolos TCP se remiten el tamaño de sus

respectivos buffers. Esto es muy importante ya que, por ejemplo, el emisor se entera de cuál es la máxima cantidad de Bytes que puede enviar, o mejor dicho que el receptor puede acumular. De la misma forma, cada vez que el receptor envía un acuse de recibo al receptor, le indica cuál es el tamaño del buffer que le queda disponible, el cual no es otro que el tamaño de la ventana disponible.

Veamos un ejemplo, el cual se grafica en la figura que sigue:



Supongamos que el emisor está limitado a enviar paquetes de hasta 1000 Bytes, cosa que puede ocurrir -por ejemplo- por el tamaño de la MTU. Agreguemos el supuesto de que la aplicación emisor está dispuesta a enviar una buena cantidad de Bytes, digamos unas decenas de miles. Supongamos también, que el receptor tiene un buffer de 2500 Bytes.

Como habíamos comentado, al establecer la conexión el receptor anunció el tamaño de su buffer, que coincide con el tamaño de la ventana inicial, en este caso dos mil quinientos Bytes.

El TCP del emisor prepara, entonces, tres paquetes para enviar los primero dos mil quinientos Bytes, dado que está limitado a un tamaño de paquete de 1000 Bytes formará: 2 paquetes de 1000 Bytes y un tercero de 500 Bytes, sin esperar ninguna acuse de recibo envía los tres paquetes.

A medida que el receptor recibe cada uno de estos paquetes envía al emisor un acuse de recibo indicando hasta qué número de bytes ha recibido y, al mismo tiempo, anunciando el tamaño de ventana que le queda disponible. Tengamos en cuenta algo muy importante: cada acuse de recibo puede remitirse sólo si se han recibido todos los Bytes anteriores (es decir, no puede enviar un ACK 2 si no ha recibido el paquete 1).

Supongamos que la aplicación en el receptor que está esperando los Bytes no los comienza a leer hasta que no ha sido recibido el tercer paquete; en este caso, en el momento de recibir el tercer paquete, el TCP del receptor anuncia una ventana de tamaño 0 Bytes.

Esto obliga al emisor a esperar hasta recibir un nuevo acuse de recibo con una cantidad positiva de Bytes en el tamaño de la ventana.

Una vez que la aplicación en el receptor ha leído, por ejemplo, los primeros dos mil Bytes recibidos, y de esta forma ha descargado dos mil Bytes del *buffer* del TCP, éste remite un mensaje con acuse de recibo donde anuncia una ventana de dos mil Bytes.

A partir de este momento, el proceso se repite.

En el ejemplo se ha mencionado que, luego de recibir un anuncio de ventana de 0 Bytes, el emisor queda en un estado latente a la espera de recibir un nuevo acuse de recibo con un valor de ventana positivo; esto es cierto en general, aunque hay dos excepciones:

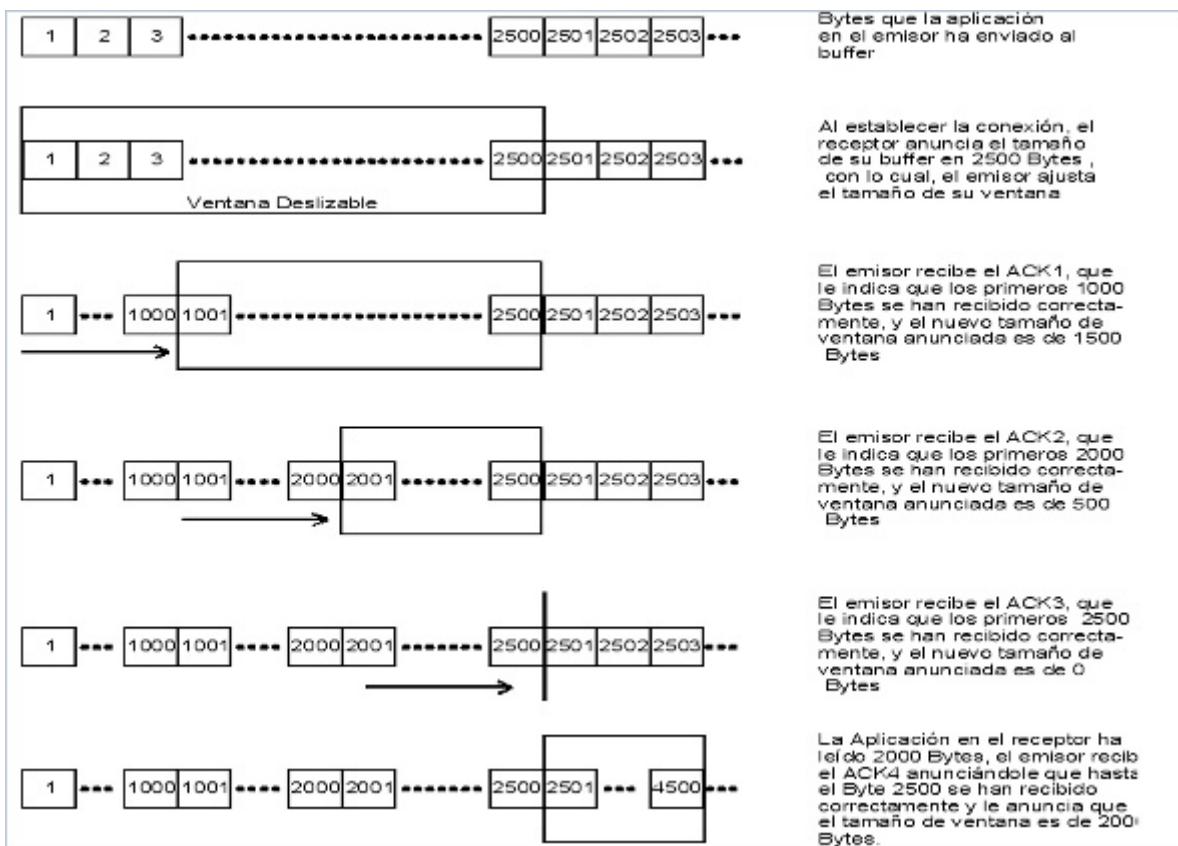
**Primero:** supongamos que el receptor, luego de remitir un acuse de recibo con un valor de ventana nulo ha enviado un acuse de recibo con un valor de ventana positivo, pero que éste se ha partido (lamentablemente los acuses de recibo también pueden perderse). En ese caso, el emisor quedaría a la espera eternamente. Para solucionar este problema, existe la posibilidad de que el emisor puede enviar un paquete de un Byte para hacer que el receptor anuncie el siguiente valor de Byte esperado y el tamaño de la ventana.

**Segundo:** también está habilitada en el protocolo la posibilidad de remitir datos urgentes, esto habitualmente es utilizado para dar fin a una aplicación remota en el host receptor, como suele ocurrir cuando se está utilizando Telnet y, por alguna razón, la aplicación en el receptor no responde.

## ¿Por qué se llamará Ventana Deslizable?

El porqué de la mencionada denominación se pondrá de manifiesto cuando vea la siguiente figura, referida al ejemplo anterior:

Ejemplo de ventana deslizable en el Emisor:



## Dos problemas que afectan dramáticamente al rendimiento, y sus soluciones

Existen dos problemas, muy similares: uno, del lado del emisor y el otro, del lado del receptor, que pueden disminuir fuertemente el rendimiento de una transmisión TCP.

Antes que nada analicemos un poco en el rendimiento de una comunicación TCP/IP.

Supongamos que deseamos enviar un solo Byte, TCP agregará un encabezado (aunque aún no hemos mostrado su formato, éste es de aproximadamente veinte Bytes), con lo cual el segmento TCP será de 21 Bytes. TCP envía el segmento a IP, el cual agrega también su encabezado, el cual puede ser de unos veinte Bytes, dando por resultado un paquete IP de cuarenta y un Bytes.

Observe que de estos 41 Bytes, sólo se desea remitir 1, los demás forman parte del protocolo. Agreguemos a esto el acuse de recibo, el cual es también de cuarenta Bytes (el acuse de recibo no es otra cosa más que un segmento TCP, el cual también se encapsula en un paquete IP).

¡Es decir que para enviar un solo Byte de información hemos utilizado en total 81 Bytes!

Sin hacer un análisis muy profundo, es evidente que el método no está obteniendo un buen rendimiento.

Es obvio que se necesita que los paquetes IP enviados desde el emisor viajen con una cierta cantidad importante de Bytes. La pregunta es, ¿cuántos Bytes debe esperar tener en buffer el emisor antes de remitir un segmento TCP?

Una solución a esta pregunta viene dada por el algoritmo de Nagle \* 20.1 : este algoritmo permite el envío de un nuevo segmento, si han entrado suficientes Bytes para llenar la mitad de la ventana anunciada en el último

acuse de recibo, o el valor máximo de segmento permitido.

### **El síndrome de la ventana tonta**

El segundo caso es muy similar a éste, pero en el lado del receptor y se denomina síndrome de la ventana tonta.

¿Qué pasa si la aplicación en el receptor es muy lenta para leer los Bytes que están en el buffer TCP del receptor?

Pensemos en un caso extremo: una vez que se ha llenado el buffer en el receptor, planteemos que la aplicación es capaz de leer un solo Byte, en el próximo acuse de recibo enviará un valor de ventana positivo de sólo un Byte. Esto obligaría al emisor a remitir un único Byte en el próximo paquete.

En este caso, la solución fue propuesta por Clark.

Evidentemente esta solución debe conseguir que el receptor no envíe acuses de recibo si tiene un espacio disponible en buffer muy pequeño, lo cual lo obligaría a anunciar una ventana también pequeña.

Nuevamente, la pregunta clave es ¿cuánto debe esperar el TCP del receptor para enviar un acuse de recibo?

Como es de esperar, la respuesta es muy similar a la del problema anterior: el receptor no debe enviar una actualización de ventana hasta que pueda manejar el tamaño máximo de segmento que anunció al establecer la conexión o que su buffer esté vacío hasta la mitad, lo que sea más pequeño.

# REFERENCIAS 20

## 20.1 : Algoritmo de Nagle

El Algoritmo de Nagle se trata de un procedimiento que supone una mejora y aumento de eficiencia de las redes de comunicación basadas en Transmission Control Protocol (TCP). El algoritmo de Nagle es un método heurístico para evitar enviar paquetes IP particularmente pequeños, también denominados pequeogramas (del inglés tinygrams). El algoritmo de Nagle intenta evitar la congestión que estos paquetes pueden ocasionar en la red reteniendo por poco tiempo la transmisión de datos TCP en algunas circunstancias.

Fuente:[https://es.wikipedia.org/wiki/Algoritmo\\_de\\_Nagle](https://es.wikipedia.org/wiki/Algoritmo_de_Nagle)

---



¿Estás listo para un desafío?

**1. Indique la opción correcta**

El control de flujo en TCP se realiza mediante mecanismos de Ventanas Deslizables.

- Verdadero
- Falso

**2. Indique la opción correcta**

En TCP Se llama Ventana Deslizable a la cantidad de bytes que pueden estar en la red sin confirmación.

- Verdadero
- Falso

**3. Indique la opción correcta**

Para mejorar el aprovechamiento del ancho de banda hay que permitir que se produzca un flujo de bits en ambos sentidos en forma simultánea.

- Verdadero
- Falso

**4. Indique la opción correcta**

Cada vez que el receptor envía un acuse de recibo al receptor, le indica cuál es el tamaño del buffer que le queda disponible, el cual no es otro que el tamaño de la ventana disponible.

- Verdadero
- Falso

**5. Indique la opción correcta**

Existe un intervalo de tiempo en el que las comunicaciones fluyen en ambos sentidos. Esto hace a un mejor aprovechamiento de la capacidad de transmisión del medio. A este tipo de procedimiento se lo denomina:

- Banda Base.
- Banda Base.

- o Orientación de flujo.
- o Ventana deslizante.

#### 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Control de flujo

es el espacio de almacenamiento temporal que tiene tanto el emisor como el receptor.

Buffer

es una solución al problema del envío de paquetes muy pequeños.

Algoritmo de Nagle

es lo que sucede si la aplicación del receptor es muy lenta para leer los Bytes en el buffer TCP.

Síndrome de la ventana tonta

es el procedimiento mediante el cual se indica cual es el tamaño de la ventana disponible.

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

El control de flujo en TCP se realiza mediante mecanismos de Ventanas Deslizables.

Verdadero

Falso

## 2. Indique la opción correcta

En TCP Se llama Ventana Deslizable a la cantidad de bytes que pueden estar en la red sin confirmación.

Verdadero

Falso

## 3. Indique la opción correcta

Para mejorar el aprovechamiento del ancho de banda hay que permitir que se produzca un flujo de bits en ambos sentidos en forma simultánea.

Verdadero

Falso

## 4. Indique la opción correcta

Cada vez que el receptor envía un acuse de recibo al receptor, le indica cuál es el tamaño del buffer que le queda disponible, el cual no es otro que el tamaño de la ventana disponible.

Verdadero

Falso

## 5. Indique la opción correcta

Existe un intervalo de tiempo en el que las comunicaciones fluyen en ambos sentidos. Esto hace a un mejor aprovechamiento de la capacidad de transmisión del medio. A este tipo de procedimiento se lo denomina:

Banda Base.

Banda Base.

Orientación de flujo.

X Ventana deslizante.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Control de flujo

es el procedimiento mediante el cual se indica cual es el tamaño de la ventana disponible.

Buffer

es el espacio de almacenamiento temporal que tiene tanto el emisor como el receptor.

Algoritmo de Nagle

es una solución al problema del envío de paquetes muy pequeños.

Síndrome de la  
ventana tonta

es lo que sucede si la aplicación del receptor es muy lenta para leer los Bytes en el buffer TCP.

# SP10 / H6: El modelo cliente-servidor

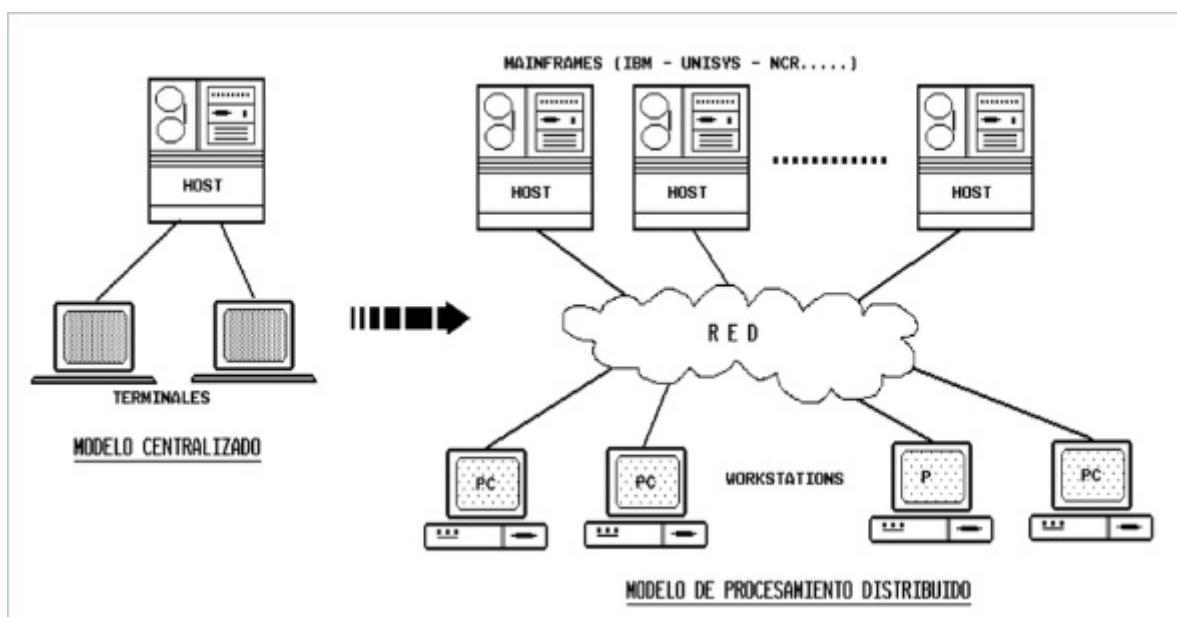
Cliente/Servidor es una arquitectura para implementar aplicaciones funcionalmente separadas en procesos distintos. Estas funciones pueden ubicarse en el mismo procesador o distribuirse en múltiples procesadores en una red. La ubicación de funciones es transparente al usuario.

Bajo esta definición, cliente/servidor se refiere principalmente al software del sistema y al de aplicación, residentes en clientes y servidores.

En esencia, cliente/servidor es una arquitectura para construir aplicaciones distribuidas y proveer flexibilidad para que los creadores de aplicaciones puedan distribuir sus elementos a través de los sistemas.

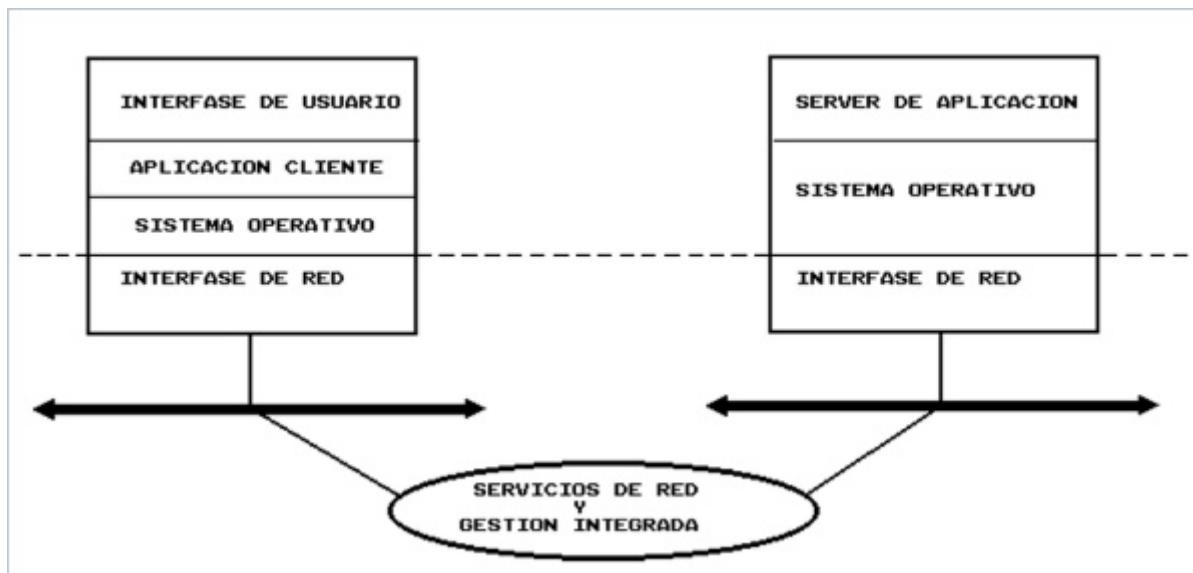
- Cliente: una estación de trabajo o computadora conectada a una red que se usa para acceder a los recursos de la red.
- Servidor: una máquina que proporciona a los usuarios enorme capacidad de almacenamiento en disco, bases de datos o conexiones a una red. Los servidores pueden ser mainframes, minicomputadoras, grandes estaciones de trabajo o dispositivos de LAN. Más de un servidor puede suministrar servicios a los clientes.

La figura siguiente compara una arquitectura tradicional con la arquitectura cliente/servidor. En la misma puede apreciarse con claridad el concepto de la arquitectura y su poder de procesamiento, y por otro lado el importante papel que juega la red de comunicaciones.



## Relación entre Cliente/Servidor y Procesamiento Distribuido

Cliente/Servidor provee una arquitectura para maximizar el uso del procesamiento y el diseño de aplicaciones distribuidas, mientras que Procesamiento Distribuido es la infraestructura fundamental que asegura la conexión existente y confiable de las aplicaciones cliente/servidor. Una efectiva arquitectura de red provee el transporte esencial para la distribución de aplicaciones.



Una infraestructura distribuida implica tener acceso a herramientas y paquetes de desarrollo de software que soporten los elementos de red de gestión.

Una estructura cliente/servidor no tiene por qué estar necesariamente fundamentada en sistemas "abiertos". Siempre que la estructura pueda soportar una o más aplicaciones distribuidas, puede emplear, generalmente, tanto elementos "abiertos" como "propietarios".

## Infraestructura Cliente/Servidor

Dentro de esta definición, identificamos dos elementos específicos:

- Una arquitectura de red efectiva, que asegure conectividad física y lógica altamente confiable para los sistemas y usuarios interconectados.
- Un entorno de gestión integrado que garantice el control y la disponibilidad de sistemas, redes y aplicaciones dentro de la infraestructura cliente/servidor y distribuido.

## Arquitectura de red

Una efectiva arquitectura de red es la base sobre la cual se implementa cliente/servidor y las aplicaciones distribuidas.

Las organizaciones no pueden construir aplicaciones distribuidas si sus redes carecen de capacidad suficiente, no son confiables o no soportan todos los sistemas o aplicaciones apropiadas. El desarrollo de una arquitectura efectiva de red tendrá que tener en cuenta tres niveles:

- Infraestructura física
- Conectividad lógica
- Servicios residentes de red

## Infraestructura física

Involucra el despliegue de una red física que cumpla con los requerimientos de comunicaciones. Los puntos principales por considerar incluyen capacidad y ancho de banda, soporte de sistemas, facilidad de instalación y administración, requerimientos de LAN vs. WAN y efectividad en función de los costos. El concepto de interconexión LAN central surge como la estructura física predominante para el Procesamiento Distribuido. En este esquema, todos los sistemas (PCs, Workstation, servidores, etc.) están conectados a una LAN. Esta LAN se sustenta en tecnología estándar (*Ethernet*, *To-ken Ring* ó *FDDI*) y en una arquitectura de concentrador y cableado estructurado. Todas las LAN separadas se enlazan entre sí a través de una familia de plataformas de interconexión confiable y flexible. Finalmente, la estructura física incluye servicios WAN (públicos o privados).

## Conectividad Lógica

Se construye sobre el enlace entre sistemas de una infraestructura física. Una vez que se cuenta con enlaces físicos seguros deberán tener capacidad para iniciar, recibir y entender la comunicación con otros sistemas de red. Hay una variedad de opciones de estándares de conectividad lógica incompatibles, tales como SNA, TCP/IP, OSI entre otros. Cada uno de estos protocolos usualmente requiere equipos diferentes para la red física.

## Servicios de Red

Aún cuando se cuente con estándares establecidos para conectividad entre sistemas y aplicaciones, las compañías necesitan determinar cuáles son los servicios residentes en la red para soportar las aplicaciones distribuidas. Estos servicios residentes proveen un conjunto de gestiones comunes a los que pueden acudir los usuarios. Estos servicios abarcan una amplia variedad de funciones que incluyen: gestión de directorios, mensajería electrónica, temporización, sincronización, transferencia de archivos y seguridad. El área de la arquitectura de red ofrece un buen ejemplo acerca de cómo puede variar la conformación de la infraestructura cliente/servidor, dependiendo del alcance de las aplicaciones. El número de usuarios y la complejidad de las aplicaciones cumple un rol principal en la determinación del nivel de funcionalidad apropiado y, por consiguiente, el costo de una arquitectura de red distribuida.

El modelo cliente/servidor puede parecer extremadamente simple. La visión centrada en el usuario y muchas de las características más comunes ocultan la verdadera complejidad y los costos de soportar un acceso a la información en forma amistosa y abierta.

Si bien el beneficio directo está en la utilización de la capacidad de procesamiento disponible, los mayores beneficios del modelo cliente/servidor están en el acceso abierto y fácil a la información.

Estas necesidades y beneficios no son únicos a la arquitectura cliente/servidor. En realidad son los mismos temas que han guiado a la industria de la información desde sus comienzos.

El punto en cuestión es, entonces, cómo pueden la funcionalidad, flexibilidad, integración, conectividad y accesibilidad ser incorporadas a la red y al entorno a un costo óptimo.

La arquitectura cliente/servidor está basada en el procesamiento cooperativo. En términos sencillos, el procesamiento cooperativo es una sola aplicación dividida en tareas. Estas tareas son luego ejecutadas en dos o más plataformas que funcionan en forma independiente.

El término cliente/servidor está asociado al mundo de las PCs en una red de Área Local, que a su vez está vinculada a uno o más servidores.

El modelo implica procesamiento cooperativo de los requerimientos de los clientes al server, que procesa los mismos y retorna los resultados al cliente.

# Procesamiento cliente/servidor

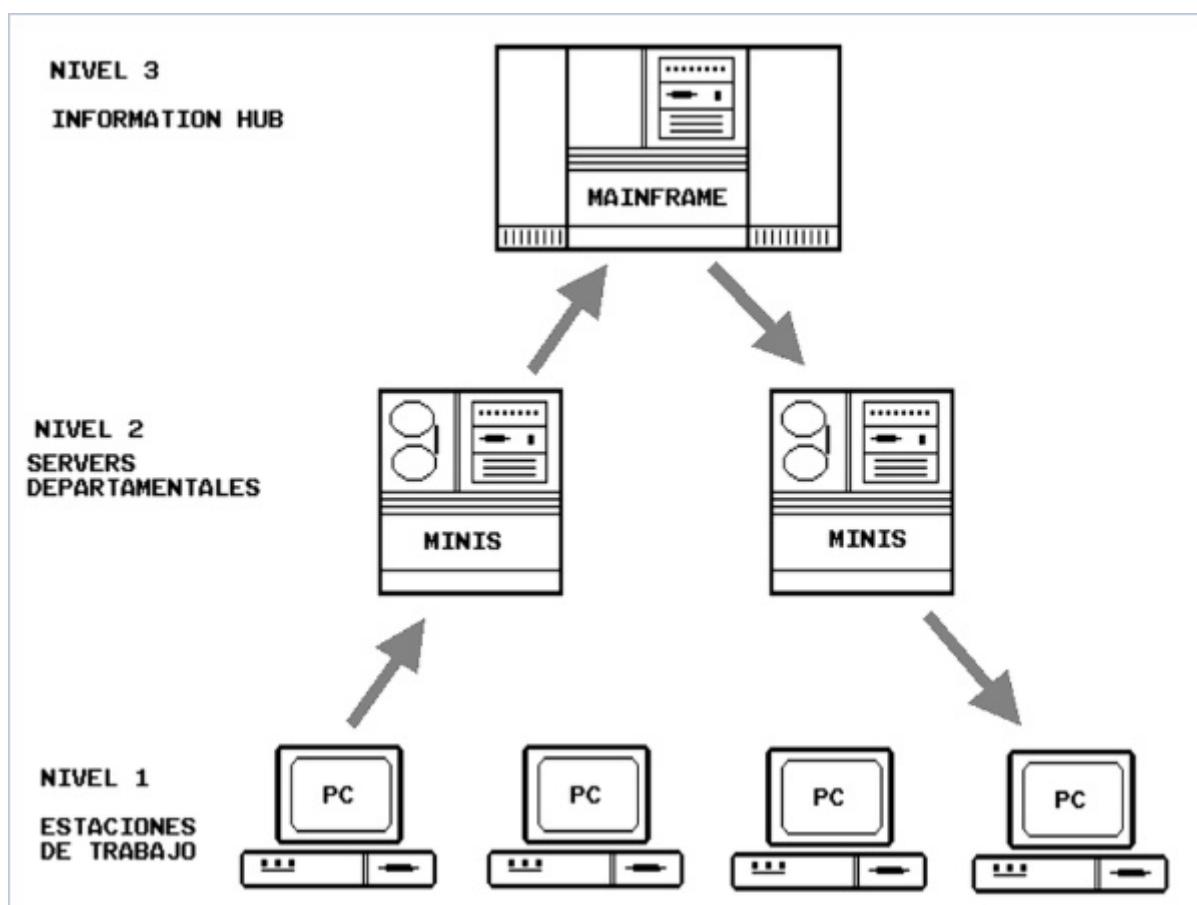
Las computadoras personales pueden ser conectadas a un dispositivo que permita compartir recursos. Los archivos en un disco rígido y las impresoras son ejemplos típicos.

En dicho contexto, todo el procesamiento es realizado en las PCs individuales y sólo ciertas funciones (por ejemplo impresión y E/S de archivos) son distribuidas. Entonces, un archivo entero debe ser enviado a una PC que emitió un requerimiento de lectura sobre dicho archivo. Si un archivo debe ser actualizado, el archivo entero es trabajado por la PC que emitió el requerimiento de actualización. Este tipo es el implementado por Novell NetWare.

Al mismo tiempo, las workstations también fueron cambiando. Éstas se fueron convirtiendo en clientes de los servers. La principal razón para el cambio fue que en un entorno de LAN de gran dimensión, compartir servicios de archivos e impresión representaba sólo una fracción de una aplicación típica. La parte más significativa de la funcionalidad de una aplicación era compartida por los usuarios. Entonces, una parte del procesamiento de las aplicaciones fue distribuido a un nuevo servidor, que recibe requerimiento de las aplicaciones corriendo en las workstations (clientes) y los procesa para cada uno de sus clientes.

En este modelo, el procesamiento de aplicaciones se divide entre el cliente y el servidor.

El procesamiento es iniciado y controlado en forma parcial por el servicio cliente, pero no en una forma maestro esclavo. Tanto el server como el cliente cooperan para ejecutar una aplicación.



La figura anterior muestra cómo pueden escalonarse las aplicaciones, desde los clientes a el/los servidores.

## Procesamiento peer-to-peer

El modelo cliente/servidor distingue entre clientes que requieren servicios y servidores que proveen servicios a los requerimientos. En el procesamiento peer-to-peer, todos los sistemas participantes son iguales y pueden emitir requerimientos y proveer servicios hacia y desde cada uno de ellos.

Esta arquitectura representa el punto culminante en la distribución de procesamiento de aplicaciones. El procesamiento es desarrollado allí donde los recursos de computación están disponibles. Un solo sistema en el procesamiento peer-to-peer puede actuar como cliente de otros servers y como servidor para otros clientes (incluyéndose el mismo). En suma, en el procesamiento peer-to-peer, un servidor puede distribuir la carga de tareas entre los servers disponibles y optimizar dicha distribución basada en servers y características de la red.

Idealmente, un entorno peer-to-peer de estas características provee procesamiento cooperativo entre aplicaciones que pueden pertenecer a plataformas de hardware y software muy diversas. Uno de los objetivos del entorno peer-to-peer es el de soportar bases de datos en red, en las cuales los usuarios pueden moverse en entornos de cómputos heterogéneos.

## Objetivos del modelo Cliente/Servidor

Podemos considerar las siguientes ventajas:

- Permite a las empresas utilizar la tecnología en forma más eficiente. Las estaciones ofrecen un poder de computación considerable, que anteriormente era disponible sólo en mainframes, a un costo muy reducido respecto de estos últimos.
- Permite que el procesamiento resida en forma cercana a la fuente de datos que está siendo procesada. El tráfico de la red y el tiempo de respuesta pueden ser reducidos en forma considerable.
- Facilita el uso de interfaces gráficas disponibles en las *workstations*.
- Permite y alienta la aceptación de sistemas abiertos. El hecho de que clientes y servidores puedan correr en diferentes plataformas de *hardware* y *software* permite al usuario final la elección de mayores y mejores alternativas de implementación.

Las desventajas para tener en consideración del modelo son:

- Si una porción significativa de la lógica de aplicación es llevada a un servidor, el mismo puede convertirse en un cuello de botella, de la misma forma que un mainframe en una arquitectura maestro esclavo. Los recursos limitados del server serán cada vez más requeridos a medida que crezca el número de usuarios. Es importante, entonces, notar que la centralización de los datos debería residir en sistemas con la capacidad de proveer los servicios necesarios a los usuarios.

Las aplicaciones distribuidas son más complejas que las aplicaciones no distribuidas, tanto en diseño como manejo operacional.

## Sistemas Cliente/Servidor

Una de las principales funciones de una red es la de compartir recursos. Muchas veces esta distribución se

lleva a cabo por programas distintos, ejecutándose en computadoras diferentes. Uno de los programas, llamado "servidor", proporciona un recurso en particular. El otro programa, llamado "cliente", utiliza ese recurso.

En redes LAN, donde todo está muy cerca y visible, es muy común utilizar la palabra "servidor" para referirse a la computadora que ejecuta justamente esta función. En la Internet, generalmente el hardware no se ve y los términos "cliente" y "servidor" hacen referencia a los programas que solicitan y proporcionan servicios.

Lo interesante de esto es que los programas cliente y servidor no necesariamente deben ejecutarse sobre la misma computadora. Por el contrario, lo más frecuente es que ambos programas residan en computadoras diferentes.

Por ejemplo, podríamos acceder desde una PC en la ciudad de Córdoba, a un sistema de noticias de Nueva York. En este caso, en nuestra PC se ejecuta el programa cliente, por ejemplo el *Internet Explorer*, o el *Google Chrome*, mientras que el servidor se ejecuta en la otra punta del globo terrestre, probablemente en una supercomputadora de la agencia de noticias.

El *Internet Explorer* o el *Google Chrome* incluyen programas cliente de HTTP. Cuando conecta con una computadora mediante cualquiera de estos programas, lo que está haciendo es solicitarle que le envíe a usted una página Web. En este caso, usted hace de cliente y la computadora que le remite la páginas Web hace de servidor; claro que para ello debe tener cargado un programa servidor HTTP.

Los programas populares de gestión de e-mail, como el *Outlook Express*, o el *Eudora* son programas cliente de e-mail. Cuando quiere bajar su e-mail, lo que hace es enviar una solicitud a un programa servidor de e-mail, que posee su proveedor de servicios de Internet. Dicho programa le remite sus e-mails.

Como usted habrá notado, por lo general, una aplicación en red constará de dos programas independientes: un programa cliente y otros servidor. Sin embargo, se puede diseñar un solo programa que cumpla ambas funciones. De hecho, algunos programas servidor que no pueden satisfacer una solicitud de servicio actúan, en ese momento, como programas cliente y piden información a otros servidor (un ejemplo clásico es el Sistema de Nombres de Dominios de Internet DNS que usa programas servidor de nombres para buscar direcciones en Internet).

Todos los servicios Internet hacen uso de la "Relación Cliente/Servidor". Por lo tanto, aprender a navegar en Internet, es aprender a usar cada uno de los "programas Clientes" disponibles. Por ello, para usar Internet hay que entender:

1. Cómo ejecutar un programa cliente.
2. Cómo decirle al programa cliente qué servidor utilizar.
3. Qué instrucciones se pueden utilizar con cada tipo de cliente.

El usuario debe saber ejecutar el programa cliente y decirle lo que tiene que hacer. El trabajo del programa cliente es conectar con el servidor adecuado y asegurarse de que sus instrucciones son enviadas correctamente. Cada tipo de cliente de Internet tiene sus propias reglas e instrucciones.

En resumen, el modelo de programación cliente-servidor divide una aplicación de red en dos lados: el cliente y el servidor. Por definición, el lado cliente solicita información o servicios al lado servidor. Éste responde a las solicitudes del cliente.

El hecho de que se utilice el modelo cliente-servidor, tiene profundas implicancias en la asignación de los puertos.

En general, podemos decir que en el host del lado cliente la asignación del puerto a una aplicación determinada puede ser arbitraria y no es del todo relevante; en cambio, las aplicaciones del lado servidor deben estar

asociadas a puertos bien conocidos, como los que figuran entre los anteriores (o, por lo menos que sean bien conocidos por quienes deben acceder como clientes).

Esto es así porque cuando el cliente envía una solicitud al servidor, debe saber de antemano a qué puerto enviarla; cuando envíe la solicitud mediante UDP, en él pondrá su dirección de puerto cliente, haciéndola conocer de esta forma al programa servidor; por eso es que puede ser cualquiera.

Otro hecho muy importante: la aplicación del lado servidor debe estar previamente activa, en un estado latente, es decir "escuchando" y esperando posibles solicitudes de clientes.

Esto brinda cierta vulnerabilidad al modelo cliente-servidor: pensemos en cómo actúan, en algunos casos, los hackers.

Un programa utilizado por ellos muy habitualmente sigue la siguiente lógica: como en su computadora no posee habitualmente un programa servidor Telnet (recuerde que mediante Telnet usted puede enviar una secuencia de teclas a otra computadora, lo cual virtualmente le da el control de esa otra computadora), le envía, por ejemplo, un e-mail con un programa adjunto habitualmente escondido; cuando abre dicho archivo, lo que en realidad hace en un segundo plano es activar un programa ejecutable que instala un servidor Telnet en su computadora. Esto significa que a partir de este momento usted está en condiciones de brindar a otras computadoras servicios Telnet.

Cuando inicie una sesión de red, su recientemente adquirido servidor Telnet se activará, y abrirá el puerto 23 (en la herramienta siguiente de esta SP verá una selección de puertos UDP y TCP más utilizados), el cual estará absolutamente dispuesto a brindar dichos servicios a cualquier cliente que se lo solicite.

Si a este programa, el hacker adiciona una función extra, por ejemplo envía un datagrama cualquiera a la computadora de él, éste podrá saber en qué momento estamos conectados y, además, conocerá nuestra dirección IP (la cual se remite en el datagrama). A partir de ese momento, el hacker puede usar su programa cliente Telnet para enviarle solicitudes al programa servidor Telnet que instaló en su computadora. Las conclusiones son obvias: él compartirá el control de su computadora.

¿Cómo podría hacer para protegerse de un ataque de este tipo?

Sin duda, la respuesta es no aceptar *e-mails* de "desconocidos", o por lo menos no activar los datos adjuntos.

Ahora piense como administrador de red (es decir póngase en esta posición: por más que envíe un memorando a todos los usuarios de su red ordenando taxativamente que no abran los *e-mails* de desconocidos (sabe que no le harán caso), y responda la pregunta anterior.

Por último, compliquemosla un poco más: piense como un hacker ¿cómo actuaría en ese caso?



¡Vamos a comprobar cuánto aprendiste!

**1. Indique la opción correcta**

En un modelo Cliente/Servidor, se conoce como "cliente" a una estación de trabajo conectada a una red que se usa para acceder a los recursos de la red.

- Verdadero
- Falso

**2. Indique la opción correcta**

En un modelo Cliente/Servidor, se conoce como "servidor" a aquella máquina que proporciona servicios a los clientes, tales como capacidad de almacenamiento en disco, bases de datos, procesamiento de aplicaciones o conexiones de red.

- Verdadero
- Falso

**3. Indique la opción correcta**

Cliente/Servidor es una arquitectura para implementar aplicaciones que funcionan separadas en procesos distintos.

- Verdadero
- Falso

**4. Indique la opción correcta**

Una Infraestructura Cliente/Servidor define:

- Una arquitectura de red efectiva, que asegure conectividad física altamente confiable.
- Un entorno de gestión integrado que garantice el control y la disponibilidad.
- Todas las anteriores.
- Ninguna de las anteriores.

**5. Indique la opción correcta**

El modelo Cliente/Servidor tiene la siguiente ventaja:

- Si una porción significativa de la lógica de aplicación esta en un servidor, el mismo puede convertirse en un cuello de botella.
- Las aplicaciones distribuidas son mas complejas que las aplicaciones no distribuidas.
- Todas las anteriores.
- Ninguna de las anteriores.

#### 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Arquitectura de red

involucra el despliegue de una red física que cumple con los requerimientos de comunicaciones.

Infraestructura física

proveen un conjunto de gestiones comunes a las que pueden acceder los usuarios.

Conectividad lógica

es la que se construye sobre el enlace entre sistemas de infraestructura física.

Servicios de red

es la base sobre la cual se implementa Cliente/Servidor y las aplicaciones distribuidas.

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

En un modelo Cliente/Servidor, se conoce como "cliente" a una estación de trabajo conectada a una red que se usa para acceder a los recursos de la red.

- Verdadero
- Falso

## 2. Indique la opción correcta

En un modelo Cliente/Servidor, se conoce como "servidor" a aquella máquina que proporciona servicios a los clientes, tales como capacidad de almacenamiento en disco, bases de datos, procesamiento de aplicaciones o conexiones de red.

- Verdadero
- Falso

## 3. Indique la opción correcta

Cliente/Servidor es una arquitectura para implementar aplicaciones que funcionan separadas en procesos distintos.

- Verdadero
- Falso

## 4. Indique la opción correcta

Una Infraestructura Cliente/Servidor define:

- Una arquitectura de red efectiva, que asegure conectividad física altamente confiable.
- Un entorno de gestión integrado que garantice el control y la disponibilidad.
- Todas las anteriores.
- Ninguna de las anteriores.

## 5. Indique la opción correcta

El modelo Cliente/Servidor tiene la siguiente ventaja:

- Si una porción significativa de la lógica de aplicación esta en un servidor, el mismo puede convertirse en un cuello de botella.
- Las aplicaciones distribuidas son mas complejas que las aplicaciones no distribuidas.
- Todas las anteriores.
- Ninguna de las anteriores.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Arquitectura de red

es la base sobre la cual se implementa Cliente/Servidor y las aplicaciones distribuidas.

Infraestructura física

involucra el despliegue de una red física que cumple con los requerimientos de comunicaciones.

Conectividad lógica

es la que se construye sobre el enlace entre sistemas de infraestructura física. proveen un conjunto de gestiones comunes a las que pueden acceder los usuarios.

Servicios de red

# SP10 / H7: Protocolos, Puertos (Ports) y Conectores (Sockets)

TCP es también responsable de la entrega de datos recibidos desde IP, a la aplicación correcta. La aplicación a la cual el dato está dirigida, se identifica por un número de 16 bit llamado "Número de Puerto" (Port Number), que veremos más adelante.

Los "Puertos Origen" (Source Port) y "Puertos Destinos" (Destination Port), están contenidos en la primera palabra del encabezamiento del segmento.

Una tarea importante del servicio de la Capa de Transporte es pasar correctamente datos a y desde la Capa de Aplicación.

Una vez que los datos son encaminados a través de la red y entregados a un host específico, éste debe ser entregado al usuario o proceso correcto. Como los datos se mueven hacia arriba o hacia abajo de las capas TCP/IP, es necesario un mecanismo para entrega de datos al protocolo específico en cada capa. El sistema debe poder combinar datos de muchas aplicaciones dentro de algunos protocolos de transporte, y desde el protocolo de transporte en el protocolo Internet.

La combinación de muchas fuentes de datos en un único tren de datos se llama "multiplexación". Los datos que arriban de una red deben ser "demultiplexados", o sea, divididos para su entrega a múltiples procesos. Para realizar esto, IP usa "números de protocolos" a fin de identificar los protocolos de transporte y los protocolos de transporte utilizan "números de puertos" para identificar las aplicaciones.

Algunos números de protocolos y puertos están reservados para identificar "servicios bien conocidos" (*well-known services*). Los "*well-known services*" son protocolos estándar de red, tales como FTP y TEL-NET, que son comúnmente usados por todas las redes.

El número de protocolo y el número de puerto asignados a los *well-known services* están documentados en el "*Assigned Number RFC*". Los sistemas Linux definen números de protocolos y puertos en dos archivos de textos.

## Números de protocolos

El número de protocolo es un único byte en la tercera palabra del encabezado del datagrama. El valor identifica el protocolo en la capa superior a la Internet (Capa de Transmisión) al cual deben ser pasados los datos.

En Linux, el número de protocolos está definido en `/etc/protocol`. Este archivo es una simple tabla que contiene el nombre y número del protocolo asociado. El formato de la tabla es una entrada única por línea, y consiste en un nombre de protocolo, separado por espacios en blanco del número de protocolo. El número de protocolo está separado por espacios en blanco del "alias" del nombre del protocolo. Los comentarios comienzan con `#`. Un archivo `/etc/protocol` se muestra a continuación:

```
% cat /etc/protocol
#
# @(#)protocols 1.8 88/02/07 SMI
#
# Internet (IP) protocols #
ip 0 IP #internet protocol, pseudo protocol number
icmp 1 ICMP #internet control message protocol
igmp 2 IGMP #internet group multicast protocol
gpp 3 GGP #gateway-gateway protocol
```

```
tcp 6 TCP #transmission control protocol  
pup 12 PUP #PARC universal packet protocol  
ud 17 UDP #user datagram protocol
```

El listado mostrado más arriba es el contenido del archivo /etc/protocol de un Host. Este listado no está completo, ya que existe una cantidad bastante más numerosa de "Números de Protocolos". No obstante, un sistema sólo necesita incluir el número de los protocolos que se usan normalmente.

Cuando un datagrama llega y la dirección destino es igual a la dirección c local, la Capa Internet conoce que el datagrama tiene que ser entregado a uno de los protocolos superiores. Para decidir cuál protocolo debe recibir el datagrama, IP examina el número de protocolo del datagrama. Si al usar la tabla, ve que el número de protocolo es 6, lo entrega a TCP. Si comprueba que el número de protocolo es el 17, lo entrega a UDP. Tanto TCP como UDP son dos servicios de la capa de transporte, pero todos los protocolos listados usan servicios de entregas de datagramas IP directamente.

## Números de puertos

Después que IP pasa el mensaje entrante al protocolo de transporte, éste pasa los datos al proceso de aplicación correcto. El proceso de aplicación, también llamado "servicio de red" (network service) está identificado por un número de puerto (port number), el cual tiene un valor de 16 bit. El "Número de Puerto Origen" (Source Port Number), identifica al proceso que envía el dato y el "Número de Puerto Destino" (Destination Port Number), identifica al proceso que recibe el dato. Ambos están contenidos en la primera palabra del encabezamiento de cada segmento TCP y cada paquete UDP.

Los números de puertos menores a 256 están reservados para "well-known services" (tales como FTP y TELNET) y están definidos en el "Assigned Number RFC".

Los números de puertos desde el 256 al 1024 son usados por "Servicios específicos", originalmente desarrollados para los sistemas UNIX.

El número de puerto no es único entre los protocolos de capa de transporte; el número sólo es único dentro de un protocolo de transporte específico. En otras palabras, TCP y UDP pueden ambos asignar el mismo número de puerto. Es la combinación de Número de Protocolo y Número de Puerto el que identifica biunívocamente al proceso a quien deben entregarse los datos.

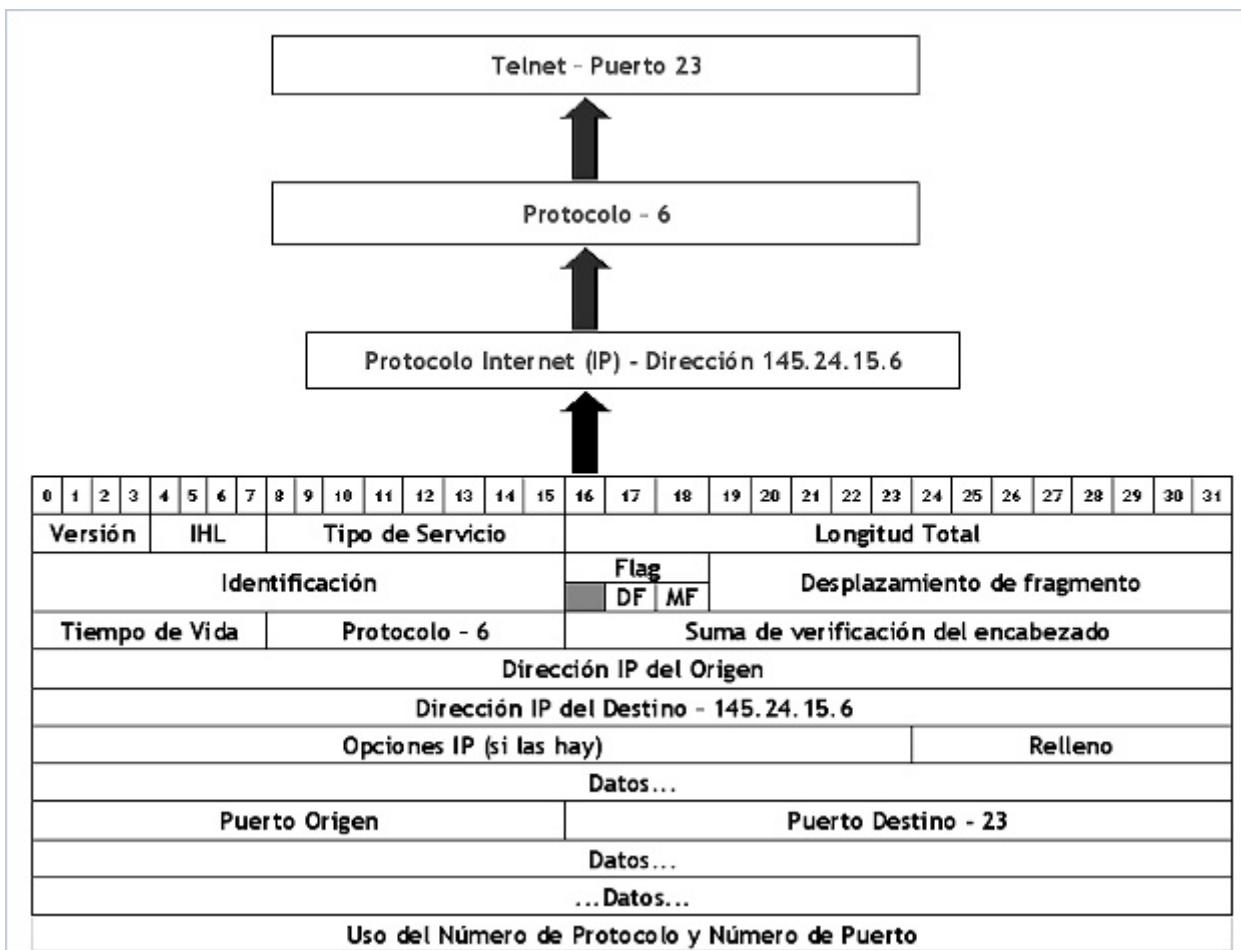
Un archivo /etc/services parcial se muestra más abajo. El formato de este archivo es muy similar al /etc/protocols. Cada entrada de línea comienza con el nombre oficial del servicio, separado por espacios en blanco del apareamiento "número de puerto/protocolo" asociado con el servicio. El número de puerto está apareado al número de protocolo debido a que diferentes protocolos de transporte pueden usar el mismo número de puerto. Puede ser provisto un listado opcional de "alias" para el nombre de servicio oficial después del par "número de puerto/número de protocolo".

```
host1  
% cat /etc/services  
#  
# @(#)services 1.12 88/02/07 SMI  
#  
# Network services, Internet style  
#
```

```
echo 7/udp
echo 7/tcp
systat 11/tcp
netstat 15/tcp
ftp-data 20/tcp
ftp 21/tcp
telnet 23/tcp
smtp 25/tcp mail
time 37/tcp timeserver
time 37/udp timeserver
name 42/udp nameserver
whois 43/tcp nickname
domain 53/tcp
domain 53/udp
hostnames 101/tcp hostname
#
# Host specific function
#
tftp 69/udp
rje 77/tcp
finge 79/tcp
link 87/tcp ttylink
supdup 95/tcp # Pos Office
pop-2 109/tcp
uucp-path 117/tcp
nntp 119/tcp usenet # Network News Transfer
ntp 123/tcp # Network Time Protocol
#
# UNIX specific services
#
exec 512/tcp
login 513/tcp
shell 514/tcp cmd # no password used
biff 512/udp comsat
who 513/udp whod
shell 514/tcp cmd # no password used
syslog 514/udp
talk 517/udp
```

route 520/udp router routed

La figura siguiente muestra este proceso de entrega.



Esta tabla, combinada con la tabla /etc./protocols, provee toda la información necesaria para entregar los datos a la aplicación correcta. Un datagrama llega a destino, basado en la dirección destino de la quinta palabra del encabezamiento del datagrama. IP usa el número de protocolo en la tercera palabra del encabezamiento del datagrama, para entregar los datos del datagrama al protocolo de la capa de transporte apropiado.

La primera palabra de los datos entregados al protocolo de transporte contiene el número de puerto destino, que comunica al protocolo de transporte, la aplicación a la cual pasar los datos.

## Conectores (Sockets)

Los "Puertos bien conocidos" (Well-known ports) son números de puertos estandarizados, que permiten a los computadores remotos conocer cuál puerto conectar para un servicio de red particular. Esto simplifica el proceso de conexión debido a que el emisor y receptor conocen de antemano qué datos están relacionados a un proceso específico, y pueden usar un número de puerto determinado. Por ejemplo, todos los sistemas que ofrecen TELNET, tienen el puerto 23.

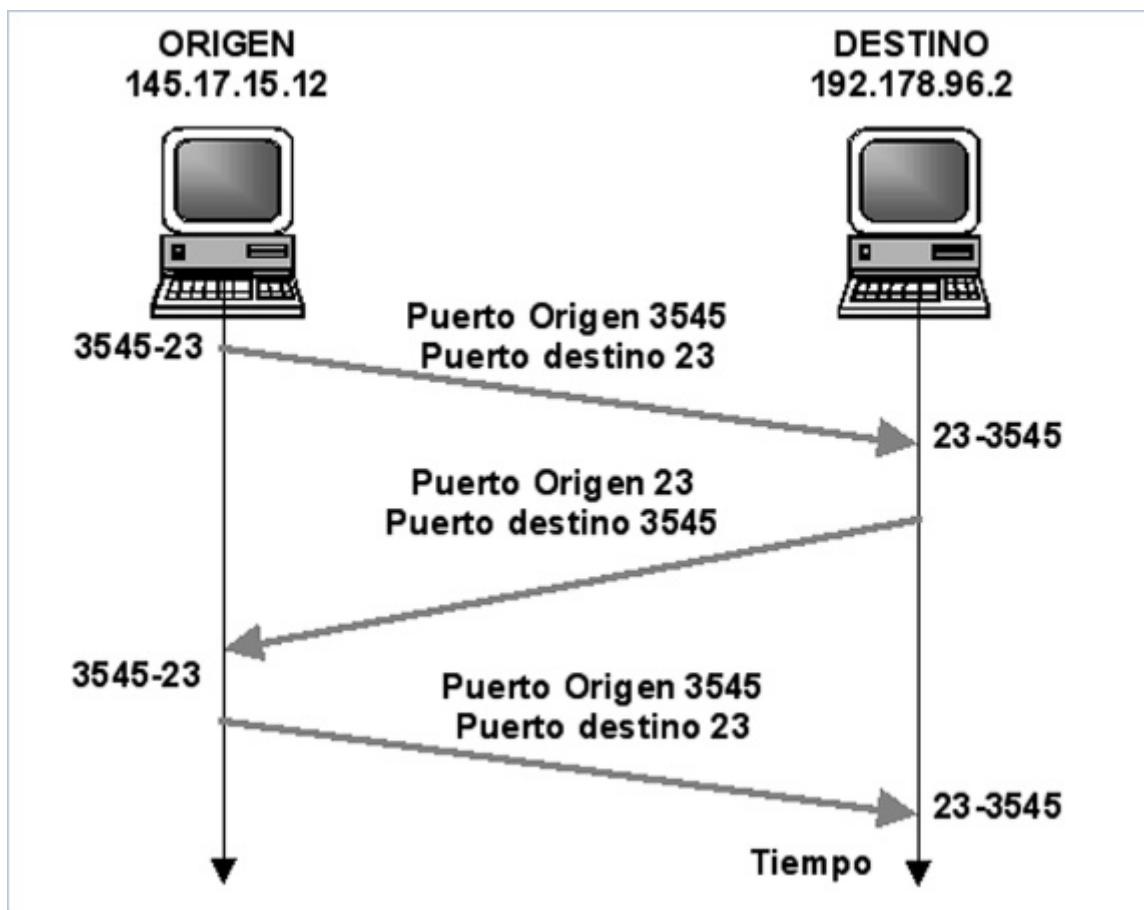
Existe un segundo tipo de puerto, llamado un "puerto dinámicamente asignado" (dynamically allocated port).

Como el nombre indica, un puerto dinámicamente asignado es un puerto no preasignado. Ellos son establecidos por los procesos cuando los necesitan. El sistema asegura que no asigan el mismo número de puerto y que el número asignado esté por encima del rango de los números de puerto estándar.

Los puertos dinámicamente asignados proveen la flexibilidad necesaria para soportar usuarios múltiples. Si un usuario TELNET es asignado al puerto 23 para el puerto origen y destino, ¿qué número de puerto será asignado al segundo usuario TELNET concurrente?

Para identificar únicamente cada una de las conexiones, el puerto origen es individualizado por un número de puerto dinámicamente asignado, y el número del well-known ports es usado por el puerto destino.

La figura siguiente muestra el intercambio de números de puertos durante el handshake TCP.



En el ejemplo de TELNET, al primer usuario le es dado un número de puerto aleatorio y, al puerto destino, el número 23 (TELNET). Al segundo usuario le es dado un número de puerto aleatorio distinto y el mismo número de puerto destino. Éste es el par de número de puerto, origen y destino, que identifica únicamente cada una de las conexiones de red.

El host destino conoce el puerto origen, debido a que es provisto en los encabezamiento de los segmentos TCP y los paquetes UDP. Ambos host conocen los puertos destinos porque es un well-known ports.

El host origen genera aleatoriamente un puerto origen, en este ejemplo el 3545. Éste envía un segmento con un puerto origen 3545 y un puerto destino 23. El host destino recibe el segmento y responde usando 23 como puerto origen y 3545 como puerto destino.

La combinación de una dirección IP y un número de puerto es llamada un "conector" (socket).

Un socket identifica un único proceso de red dentro de toda la Internet. Algunas veces, los términos "socket" y "port number" son usados indistintamente. En realidad, los "well-known services", son frecuentemente referidos como "well-known sockets".

En nuestro contexto, socket es la combinación de una dirección IP y un número de puerto. Un par de sockets, uno para el host receptor y uno para el host emisor, definen la conexión para los protocolos orientados a conexión como el TCP.

En la figura anterior puede verse la asignación dinámica de puerto y *well-known ports*. Un usuario en el host 145.17.15.12 (host origen) usa TELNET para conectarse al host 192.178.96.2.

El usuario es dinámicamente asignado a un único número de puerto, 3545. La conexión es hecha al servicio TELNET en el host remoto, el cual es, de acuerdo con el estándar asignado al *well-known ports* 23.

El socket, en el lado origen de la conexión, es "145.17.15.12.3545" (dirección IP 145.17.15.12 más el número de puerto 3545). Para el lado destino de la conexión, el socket es "192.178.96.2.23" (dirección IP 192.178.12.2 más puerto 23).

El puerto del socket destino es conocido por ambos sistemas, dado que es un *well-known ports*. El puerto del socket origen es conocido, porque el host fuente informó al host destino el socket fuente cuando fue hecho el requerimiento de conexión. El par de socket es, por consiguiente, conocido por ambos computadores (origen y destino).

La combinación de los dos sockets identifica únicamente esta conexión; no hay otra conexión en Internet con este par de socket.

## Los puertos UDP y TCP

Por último, y a modo de apéndice, se agrega la siguiente lista de los primeros 256 puertos asignados por IANA, el organismo competente que realiza tales asignaciones.

Dado que es muy bueno poder consultar el listado completo de los puertos asignados, le sugiero que los obtenga directamente de IANA en el siguiente *enlace*: *Puertos asignados por IANA*  
<http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml>

El listado completo de la lista de puertos ocuparía aproximadamente 130 páginas, por lo cual no tiene sentido insertarlo en este texto.

Los puertos están divididos en tres rangos:

Puertos Bien Conocidos: desde el 0 hasta el 1023

Puertos Registrados: desde el 1024 hasta el 49151

Puertos Dinámicos y/o Privados: desde el 49152 hasta el 65535

### Puertos bien conocidos

Los puertos conocidos son asignados por la IANA y en la mayoría de los sistemas sólo pueden ser utilizados por el sistema (o root) los procesos o programas ejecutados por usuarios con privilegios de administrador.

Los puertos se utilizan en el protocolo TCP [RFC793] para nombrar a los extremos de las conexiones lógicas. Se definen puertos de referencia con el fin de proporcionar servicios. La lista de Puertos Bien Conocidos especifica el puerto que utiliza el proceso de servidor como puerto de contacto.

En la medida de lo posible, estas mismas asignaciones de puerto se utilizan con UDP [RFC768].

Los puertos asignados usan una pequeña porción de los números de puerto posibles. Durante muchos años, los puertos asignados estaban en el rango 0-255. Posteriormente, el rango de puertos bien conocidos administrados por la IANA se ha ampliado para el rango de 0-1023 (anteriormente a 1992, el rango de 256 a 1023 se usaba para servidores específicos de UNIX)

A continuación se muestran, de los Puertos Bien Conocidos, una selección de los más utilizados

Keyword	Decimal	Description	References
echo	7/tcp	Echo	
echo	7/udp	Echo	
ftp-data	20/tcp	File Transfer [Default Data]	
ftp-data	20/udp	File Transfer [Default Data]	
ftp	21/tcp	File Transfer [Control]	
ftp	21/udp	File Transfer [Control]	
telnet	23/tcp	Telnet	
telnet	23/udp	Telnet	
smtp	25/tcp	Simple Mail Transfer	
smtp	25/udp	Simple Mail Transfer	
name	42/tcp	Host Name Server	
name	42/udp	Host Name Server	
nameserver	42/tcp	Host Name Server	
nameserver	42/udp	Host Name Server	
nicname	43/tcp	Who Is	
nicname	43/udp	Who Is	
domain	53/tcp	Domain Name Server	
domain	53/udp	Domain Name Server	
hostname	101/tcp	NIC Host Name Server	
hostname	101/udp	NIC Host Name Server	
pop3	110/tcp	Post Office Protocol - Version 3	
pop3	110/udp	Post Office Protocol - Version 3	
ntp	123/tcp	Network Time Protocol	
ntp	123/udp	Network Time Protocol	
snmp	161/tcp	SNMP	
snmp	161/udp	SNMP	
snmptrap	162/tcp	SNMPTRAP	
snmptrap	162/udp	SNMPTRAP	



¿Te animás a medir cuánto aprendiste?

**1. Indique la opción correcta**

Los Puertos Bien Conocidos (well-known services) son protocolos estándar de red, tales como FTP y TELNET que son, comúnmente, usados por todas las redes.

- Verdadero
- Falso

**2. Indique la opción correcta**

Los "Puertos Origen" y "Destino", están contenidos en la tercera palabra del encabezamiento del segmento.

- Verdadero
- Falso

**3. Indique la opción correcta**

Una aplicación identifica que un mensaje es para ella mediante:

- El número MAC.
- El número IP.
- El número de puerto.
- El nombre de la Aplicación.

**4. Indique la opción correcta**

¿Cómo se llaman los puertos y servicios reservados?

- Puertos Bien Conocidos.
- Puertos Registrados.
- Puertos Dinámicos.
- Puertos Privados.

**5. Indique la opción correcta**

¿Cómo se identifican los Puertos Bien Conocidos?

- Porque son los números de puertos menores a 256.
- Porque son los números de puertos menores a 1023.
- Porque son los números de puertos menores a 49151.
- Porque son los números de puertos menores a 65535.

#### 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Número de protocolo	es un único byte que identifica el protocolo en la Capa de Transmisión al cual deben ser pasados los datos.
Número de puerto	es un número de 16 bits (2bytes) que identifica el proceso de la aplicación que envía/recibe los datos.
Socket	es la combinación de una dirección IP y un número de puerto.

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Los Puertos Bien Conocidos (well-known services) son protocolos estándar de red, tales como FTP y TELNET que son, comúnmente, usados por todas las redes.

- Verdadero
- Falso

## 2. Indique la opción correcta

Los "Puertos Origen" y "Destino", están contenidos en la tercera palabra del encabezamiento del segmento.

- Verdadero
- Falso

## 3. Indique la opción correcta

Una aplicación identifica que un mensaje es para ella mediante:

- El número MAC.
- El número IP.
- El número de puerto.
- El nombre de la Aplicación.

## 4. Indique la opción correcta

¿Cómo se llaman los puertos y servicios reservados?

- Puertos Bien Conocidos.
- Puertos Registrados.
- Puertos Dinámicos.
- Puertos Privados.

## 5. Indique la opción correcta

¿Cómo se identifican los Puertos Bien Conocidos?

- Porque son los números de puertos menores a 256.
- Porque son los números de puertos menores a 1023.
- Porque son los números de puertos menores a 49151.
- Porque son los números de puertos menores a 65535.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Número de protocolo

es un único byte que identifica el protocolo en la Capa de Transmisión al cual deben ser pasados los datos.

Número de puerto

es un número de 16 bits (2bytes) que identifica el proceso de la aplicación que envía/recibe los datos.

Socket

es la combinación de una dirección IP y un número de puerto.

# SP10 / Ejercicio resuelto

El problema concreto en el Hospital es el siguiente:

En un sector del mismo, el tercer piso, se encuentra el Departamento Historias Clínicas, con un servidor que es consultado permanentemente por todos los profesionales que están atendiendo pacientes, y el Departamento Docencia, que cuenta con una sala de conferencias donde diariamente los médicos residentes asisten a capacitación y se realizan teleconferencias donde especialistas de otros países no solo dan catedra sino también se muestran casos prácticos que incluyen intervenciones quirúrgicas on-line.

Como podrá sospechar, cada vez que hay una teleconferencia colapsa la subred del tercer piso y los profesionales que están atendiendo en los consultorios tienen que soportar amargas esperas para poder acceder al servidor de historias clínicas.

En la subred de referencia, utilizamos un software analizador de protocolos para obtener una captura de datos de 1000 paquetes. A continuación vemos un cuadro resumen con la siguiente información:

Protocol	Percentage	Bytes	Packets
Ethernet Type 2	0,000%	0	0
IP	0,000%	0	0
TCP	47,822%	121.652	352
NetBIOS	1,366%	3.476	9
+SessMsg	39,409%	100.251	572
Sess Req	0,153%	390	3
Pos Ses Rsp	0,050%	128	2
HTTP	10,242%	26.054	33
HTTP Proxy	0,201%	512	8
Lotus Notes	0,042%	108	1
UDP	0,684%	1.739	19
ICMP	0,000%	0	0
Dest Unreach	0,029%	74	1

En ella se aprecia la cantidad de paquetes y bytes por protocolo, como así también el porcentaje de cada uno de ellos.

Flags: 0x00  
Status: 0x21 Sliced  
Packet Length: 1082 Slice Length: 96  
Timestamp: 08:00:01.629929 04/04/2003

#### Ethernet Header

Destination: 00:50:8B:55:EE:00 ← Dirección MAC destino  
Source: 00:50:54:FF:12:82 ← Dirección MAC origen  
Protocol Type: 0x0800 IP ← Tipo de Protocolo de Capa de Red (IP)

#### IP Header - Internet Protocol Datagram

Version: 4  
Header Length: 5 (20 bytes)  
Precedence: 0  
Type of Service: %0000  
Unused: %0  
Total Length: 1064  
Identifier: 32765  
Fragmentation Flags: %010 Do Not Fragment  
Fragment Offset: 0 (0 bytes)  
Time To Live: 46  
IP Type: 0x06 TCP  
Header Checksum: 0xBA35  
Source IP Address: 200.62.58.48  
Dest. IP Address: 10.250.1.53  
No Internet Datagram Options

**TCP - Transport Control Protocol**

Source Port: 80 World Wide Web HTTP

Destination Port: 42880

Sequence Number: 1212667050

Ack Number: 872678475

Offset: 5

Reserved: %000000

Code: %010000

Ack is valid

Window: 49280

Checksum: 0x98B4

Urgent Pointer: 0

No TCP Options

Checksum: 0x98B4

Urgent Pointer: 0

No TCP Options

**HTTP - HyperText Transfer Protocol**

.... ... 09 09 09 09 20 20 0D 0A

... .... <td c 09 09 09 20 20 09 09 09 09 20 20 3C 74 64 20 63  
lass="generalT 6C 61 73 73 3D 22 67 65 6E 65 72 61 6C 54

HTTP Data:

ext9 65 78 74 39

Vemos que el mayor porcentaje de los paquetes utiliza TCP

**Propuesta de mejora:**

1. Configurar las aplicaciones de Docencia para que en sus Aplicaciones de Teleconferencia utilicen el protocolo UDP en vez de TCP.

2. Dividir el tráfico de Historias Clínicas y Docencia en dos subredes distintas separándolas con un Router.

## SP10 / Ejercicio por resolver

En la empresa donde Ud. trabaja utilice un software analizador de paquetes para hacer una captura de 65534 paquetes.

En la misma deberá distinguir lo siguiente:

- Tipos de tramas y paquetes capturados.
- Tipos de direcciones MAC (direcciones físicas).
- Tipos de direcciones de red (direcciones lógicas).
- Tamaño de los paquetes.
- Tipos de protocolos involucrados.

Se pide:

1. Realice un grafico por cantidad y tipo de paquetes.
2. Indique qué tipos de protocolos circulan en la red donde fueron capturados los paquetes
3. Identifique si es posible alguna mejora que pudiera realizar para mejorar el tráfico y propóngala a su profesor/tutor



¿Estás listo para un desafío?

**1. Indique la opción correcta**

La primera palabra de la cabecera UDP indica los números de puertos origen y destino.

- Verdadero
- Falso

**2. Indique la opción correcta**

UDP es capaz de gestionar mensajes de reportes de error mediante ICMP.

- Verdadero
- Falso

**3. Indique la opción correcta**

La cuarta palabra de la Cabecera TCP tiene un conjunto de Flag o banderas de 1 bit cada una: URG, ACK, PSH, RST, SYN y FIN

- Verdadero
- Falso

**4. Indique la opción correcta**

El número de secuencia (ISN) en el encabezamiento del segmento de datos identifica la posición secuencial en el tren de datos del primer byte de datos en el segmento.

- Verdadero
- Falso

**5. Indique la opción correcta**

Una estación de trabajo conectada a una red que se usa para acceder a los recursos de la red es conocida como:

- Servidor.
- Cliente.
- Host.

- Estación de trabajo igualitaria.

**6. Indique la opción correcta**

Aquella máquina que proporciona servicios a los clientes, tales como capacidad de almacenamiento en disco, bases de datos, procesamiento de aplicaciones o conexiones de red.

- Cliente.
- Servidor.
- Host.
- Nodo.

**7. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

SYN	es un intercambio de segmentos, el usado por TCP es llamado "a tres vías".
Handshake	es un bit que indica si la conexión TCP termina utilizando un 1.
FIN	es una Bandera en la cabecera TCP que se utiliza para el establecimiento de conexiones.
Ventana Deslizable	es la cantidad de bytes que pueden estar en la red sin confirmación.

**8. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

La capa de Transporte	direcciona los mensajes a las distintas aplicaciones mediante los protocolos UDP y TCP.
TCP y UDP	establecen conexiones entre aplicaciones y permiten que varias aplicaciones utilicen simultáneamente los servicios IP.
UDP	provee servicio de entrega segura de datos con detección y corrección de errores extremo a extremo.
TCP	provee servicio de entrega de datagramas poco seguro, no orientado a conexión.

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

La primera palabra de la cabecera UDP indica los números de puertos origen y destino.

- Verdadero
- Falso

## 2. Indique la opción correcta

UDP es capaz de gestionar mensajes de reportes de error mediante ICMP.

- Verdadero
- Falso

## 3. Indique la opción correcta

La cuarta palabra de la Cabecera TCP tiene un conjunto de Flag o banderas de 1 bit cada una: URG, ACK, PSH, RST, SYN y FIN

- Verdadero
- Falso

## 4. Indique la opción correcta

El número de secuencia (ISN) en el encabezamiento del segmento de datos identifica la posición secuencial en el tren de datos del primer byte de datos en el segmento.

- Verdadero
- Falso

## 5. Indique la opción correcta

Una estación de trabajo conectada a una red que se usa para acceder a los recursos de la red es conocida como:

- Servidor.
- Cliente.
- Host.
- Estación de trabajo igualitaria.

## 6. Indique la opción correcta

Aquella máquina que proporciona servicios a los clientes, tales como capacidad de almacenamiento en disco, bases de datos, procesamiento de aplicaciones o conexiones de red.

- Cliente.
- Servidor.
- Host.
- Nodo.

## 7. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

SYN	es una Bandera en la cabecera TCP que se utiliza para el establecimiento de conexiones.
Handshake	es un intercambio de segmentos, el usado por TCP es llamado "a tres vías".
FIN	es un bit que indica si la conexión TCP termina utilizando un 1.
Ventana	es la cantidad de bytes que pueden estar
Deslizable	en la red sin confirmación.

#### 8. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

La capa de Transporte	direcciona los mensajes a las distintas aplicaciones mediante los protocolos UDP y TCP.
TCP y UDP	establecen conexiones entre aplicaciones y permiten que varias aplicaciones utilicen simultáneamente los servicios IP.
UDP	provee servicio de entrega de datagramas poco seguro, no orientado a conexión.
TCP	provee servicio de entrega segura de datos con detección y corrección de errores extremo a extremo.

# Situación profesional 11: ¿Qué dispositivos de conectividad utilizaremos?

## La capa de Aplicación y los dispositivos de networking

¿Qué dispositivos deberán tenerse en cuenta para que la red funcione correctamente?

Ha llegado a adquirir los conocimientos necesarios para completar la instalación de una red. Para ello no sólo son imprescindibles los cables, sino que debe instalar distintos dispositivos para lograr la conectividad de toda la red. ¿Dónde se conectarán las computadoras?, ¿cómo se realiza la conexión entre las distintas redes?, ¿cómo se accede a Internet? Estas y otras preguntas tendrán su explicación al estudiar los distintos tipos de dispositivos que la industria pone a disposición para lograr la conectividad de la red. Comprenderá el uso, funciones y características de un Hub, de un Switch y de un Router, como así también qué son y cómo afectan a las redes las colisiones y los broadcast, y la forma de limitar o minimizarlos.

# SP11 / H1: Dispositivos de conectividad: Capas 1 y 2: Repetidor, Hub, NIC, Bridge y Switch

## Los dispositivos de conectividad en las redes

Los dispositivos de conectividad (o medios de *networking*) son elementos físicos por los cuales pasan las señales de transmisión (cables, microondas, radioenlaces, etc.). La cantidad de datos que viajan en la red dependen de los materiales que constituyen los medios. Estos medios permiten conectar las distintas estaciones de trabajo para formar redes de datos.

Como vimos en la SP1 Herramienta 3 (Clasificación de las redes) según su tamaño y alcance, según el área que abarcan, las redes más típicas son: LAN, MAN y WAN.

De este tipo de redes, resumimos las características destacables a los fines de explicar luego los elementos típicos de conectividad:

- Redes LAN
  - Son redes de bajo nivel de errores.
  - Cubren áreas pequeñas.
  - Tienen alta disponibilidad.
  - Medios de comunicación propietarios.

En este tipo de redes utilizamos *Hubs*, *Bridges*, *Switches* y *Routers* (que se explican en profundidad mas adelante). Estos dispositivos están diseñados para conectar dispositivos adyacentes, proveen conectividad todo tiempo, son controlados en forma privada y proveen acceso múltiple a medios de gran velocidad de transferencia.

- Redes MAN
  - Son redes de bajo nivel de errores.
  - Cubren áreas del tamaño de una ciudad o parte de una ciudad.
  - Tienen alta disponibilidad.

En este tipo de redes utilizamos tecnologías intermedias entre LAN y WAN.

- Redes WAN
  - Son redes de nivel de errores más altos que las LAN.
  - Cubren áreas extensas (una provincia, un país, el mundo entero).
  - Tienen baja a media disponibilidad.
  - Medios de comunicación arrendados (compartidos).

En este tipo de redes utilizamos Servidores de Comunicaciones y Routers . Estos dispositivos están diseñados para conectar dispositivos separados por grandes distancias, proveen conectividad full y part time, proveen control de acceso a servicios públicos, tienen velocidades de transferencia relativamente más bajas que las LAN y proveen acceso a interfaces seriales.

En los orígenes, cuando las redes LAN solo compartían archivos e impresoras, los problemas eran la incompatibilidad del hardware y del software utilizado. Lo que funcionaba bien dentro de la LAN, no necesariamente lo hacía tan bien fuera de ella.

Cuando se crea el Modelo OSI (1984) como marco de referencia conceptual, se estandariza de qué manera

debe circular la información a través de los medios, lo que permite lograr la conectividad de las redes.

Las ventajas que provee el Modelo OSI son:

- Reducción de la complejidad.
- Estandarización de las interfaces.
- Facilidad de ingeniería modular.
- Asegurar interoperabilidad de tecnologías.
- Simplificar la enseñanza y aprendizaje.

En el Modelo OSI, pueden haber diferencias entre las distintas arquitecturas de redes que se implementan, pero la arquitectura de capas facilita la integración a través de la modularización: a medida que la información desciende hacia la capa física, pierde el "lenguaje humano" y va "tomando el lenguaje de las computadoras" (binario).

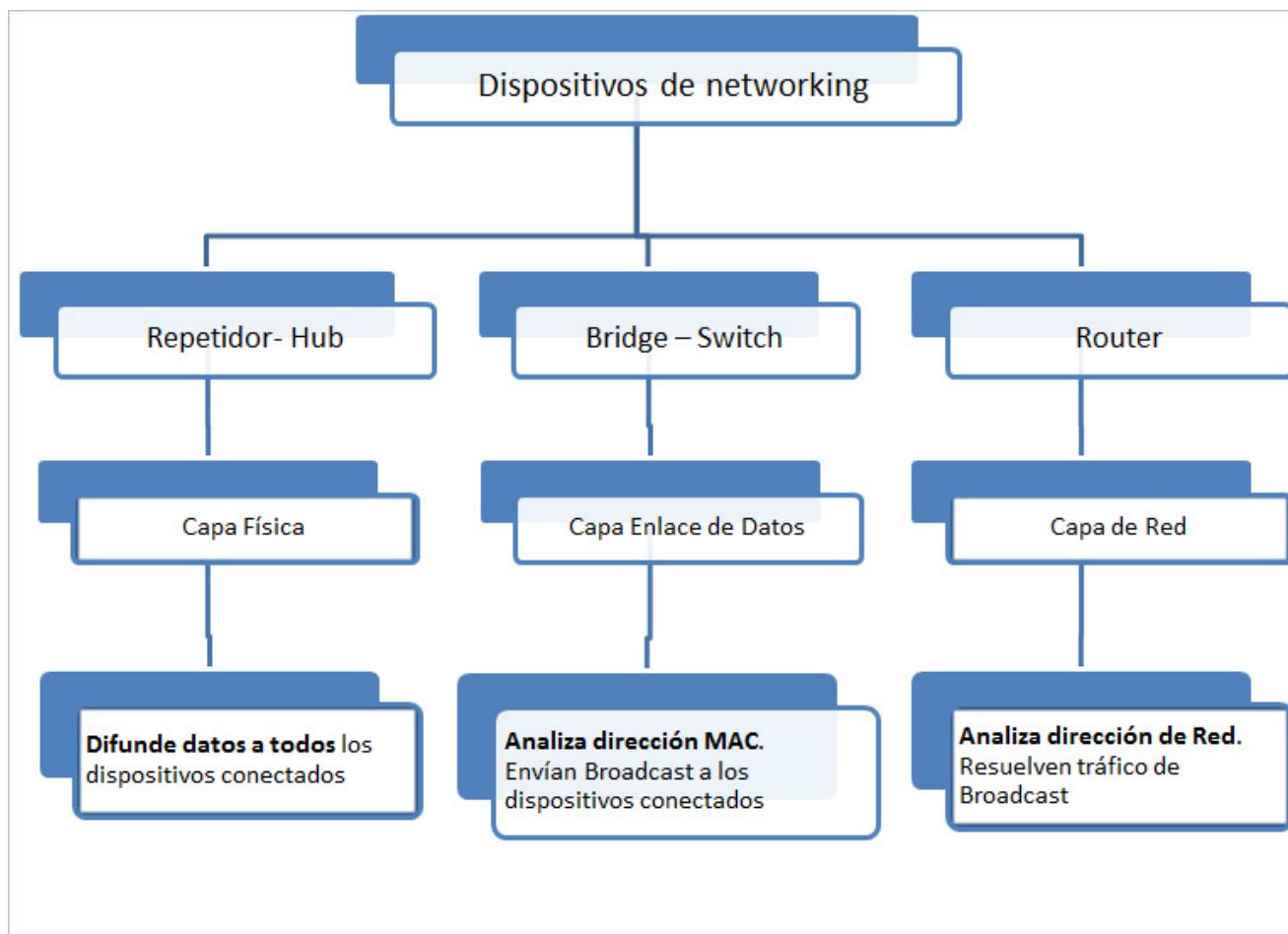
**Toda red tiene:**

- Una estructura.
- Un funcionamiento que permite la comunicación origen - destino.

La comunicación se da en forma de datos o paquetes de datos. Tanto el origen como el destino son computadoras. El proceso en que viajan los datos se conoce como "Encapsulamiento" y a medida que los datos descienden, se les van agregando encabezamientos. Esos encabezamientos son la forma en que las distintas capas del Modelo OSI se comunican entre sí. Ahora bien, esos "encabezados" son interpretados por distintos dispositivos que realizan las distintas tareas indicadas en el Modelo OSI. Por esto, cuando analicemos los dispositivos, lo haremos siempre teniendo como referencia al Modelo OSI.

Por ejemplo: cuando decimos a qué computadora dentro de la red se deben enviar los datos deberá analizarse la "dirección física", (o dirección MAC), que en el caso de Ethernet se graba en la misma Placa de Red (NIC) en el proceso de fabricación. Otros dispositivos utilizan estas direcciones para crear y actualizar "tablas de enrutamiento" y "estructuras de datos". De esta manera, cuando las direcciones de la trama y de la NIC coinciden, esta última copia la trama y la pasa a las capas superiores para completar el proceso de comunicación.

En la figura siguiente vemos un mapa conceptual donde podemos observar sintéticamente algunas diferencias principales (más adelante se explicarán los detalles):



"Mapa conceptual" | Autor

Los dispositivos de conectividad se utilizan para conectar redes. Cuando estas redes crecen en tamaño y complejidad, se utilizan distintos dispositivos para conectarlas, pero todos comparten alguno o más propósitos comunes:

Propósitos comunes:

- Conectar un mayor número de nodos a la red.
- Alargar las distancias que cubre la red.
- Localizar el tráfico de la red.
- Fusionar redes existentes.
- Aislar problemas de red, de modo de facilitar su diagnóstico.
- Brindar seguridad y confiabilidad.

## Relación entre dispositivos y capas

En figura siguiente pueden verse conceptualmente los distintos dispositivos de networking, en que capa funcionan y una descripción general de las tareas que realizan.

OSI	Dispositivo	Descripción General
3 a 7	<b>IDS</b>	Sistema de detección de intrusos encargado de detectar los posibles intrusos que intentan obtener acceso no autorizado a través de la red o en un servidor.
3 a 7	<b>Firewall</b>	Dispositivo de comunicaciones utilizado para proteger una red de otras clasificadas como de menor nivel de seguridad.
3	<b>Router</b>	Efectúa el ruteo a nivel de red, interconectando segmentos de distintas redes. Divide dominios de colisión y de broadcast.
2	<b>Switch</b>	Similar al puente pero posee N interfaces y adicionalmente, posee capacidad de memorizar / priorizar tráfico. Interconecta segmentos de la misma red.
2	<b>Bridge</b>	Dispositivo utilizado para segmentar redes, permite filtrar tráfico identificándolo por su dirección física. Utilizado para conectar redes LAN de distinta topología a corta distancia y dividir dominios de colisión.
2	<b>NIC</b>	Elemento que permite a los dispositivos conectarse a una red. Almacena las direcciones físicas y gestiona el acceso al medio.
1	<b>Hub</b>	Dispositivo de comunicaciones utilizado para reconstruir y repetir señales a nivel físico en todos los puertos. Es también llamado Repetidor Multipuerto
1	<b>Repetidor</b>	Dispositivo de comunicaciones utilizado para reconstruir y repetir señales a nivel físico.

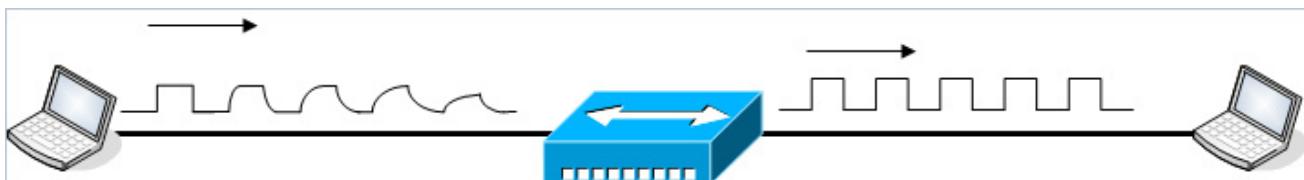
"Dispositivos y Capas" | Autor

Veremos a continuación las características principales de estos dispositivos. Para organizarnos, lo haremos por niveles o capas donde operan:

## Dispositivos de Capa 1

### Repetidor

Los repetidores retransmiten la señal que reciben. Regeneran y retemporizan las señales, lo que permite que éstas se propaguen a mayor distancia. Solamente se encargan de los paquetes a nivel de bits (señales eléctricas) por lo que son entonces dispositivos de la capa 1.



"Repetidor" | Autor

Los repetidores son actualmente menos comunes que en el pasado, ya que hoy en día los hubs ofrecen, además de las características típicas de los repetidores, las ventajas de la concentración y conectividad.

Sus características pueden resumirse en los siguientes puntos:

- Operan en la Capa Física (capa 1 del Modelo OSI).
- Permiten aumentar el número de nodos conectados a una red.
- Permiten aumentar la extensión de la red.

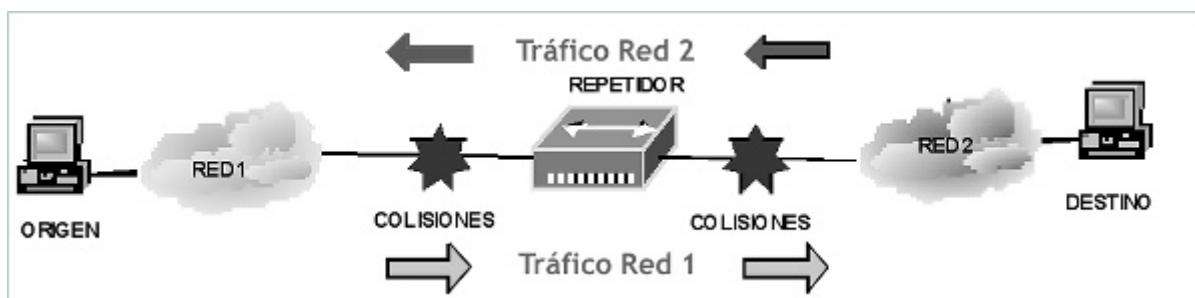
Funciones:

- Regenerar la señal.
- Amplificar la señal.

Estas funciones se logran dando una nueva forma y volviendo a temporizar las señales antes de reenviarlas a través de la red.

Para que las señales no sean irreconocibles a los dispositivos que las reciben, ya sea a causa del ruido, o de las atenuaciones debido a las distancias y a las limitaciones de los medios físicas, los repetidores toman las señales debilitadas, las limpian, las amplifican y las reenvían para que continúen su camino en la red.

Desventaja: el uso de repetidores no filtra el tráfico de la red, por lo tanto extiende el dominio de colisión de la misma (se explica más adelante, en "Concentrador del tipo hub o repetidor multipuerto" lo que significa un "dominio de colisión"). Por ahora, observe la figura:

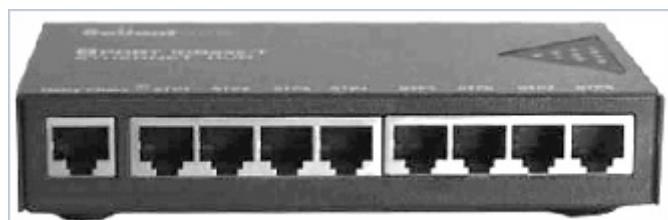


## Hub o Repetidor Multipuerto

El Hub es un repetidor que, al contener múltiples puertos para el conexionado de los cables, también se los conoce como "Repetidor Multipuerto". Los repetidores multipuerto combinan las propiedades de amplificación y de retemporización de los repetidores con la conectividad. Para conectar cada estación a la red, las LAN pueden utilizar HUB. Estos dispositivos son "concentradores de cables" y además cumplen la función de repetir la señal que ingresa por uno de sus puertos al resto de los puertos.

Los hubs son dispositivos de red que sólo manejan bits y son dispositivos de la Capa 1

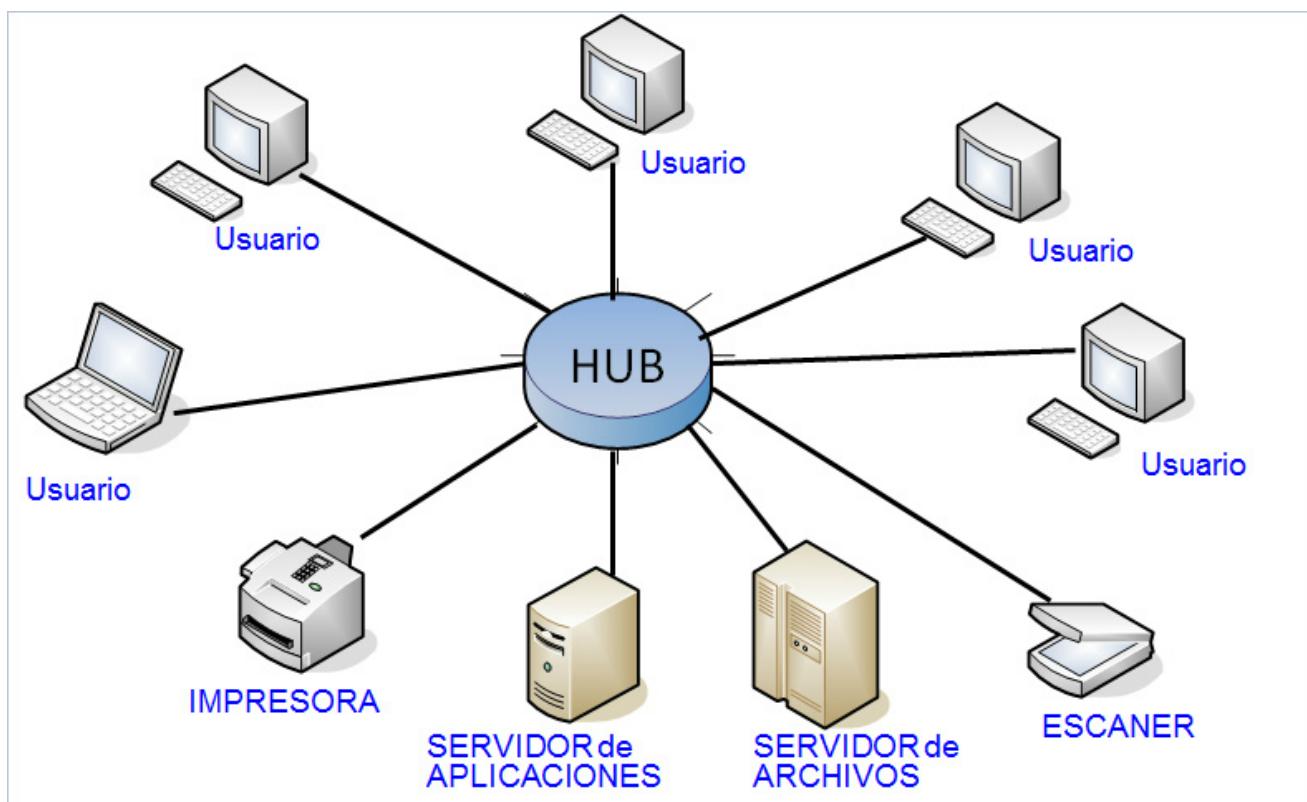
Puede constituir el centro de red en una topología estrella Ethernet



Se podría conectar conectar una estación de trabajo al Hub como muestra la siguiente figura:



Con lo que, conceptualmente se puede conformar una red de la siguiente manera:



"Hub" | Autor

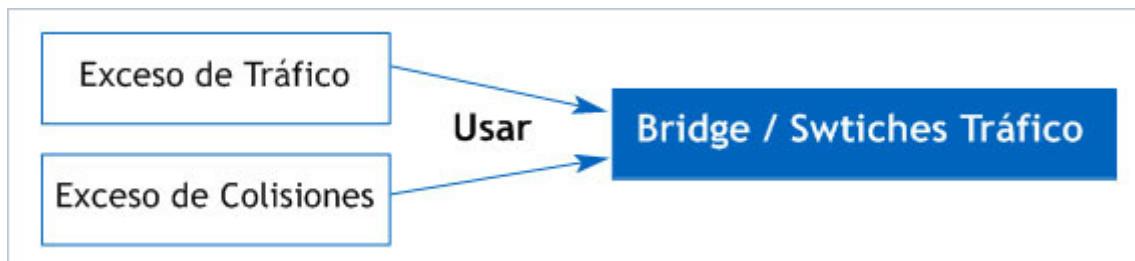
Puede utilizar esta forma rápida de conexión solo como solución de coyuntura, pues, para armar una red deberíamos seguir las reglas del cableado estructurado, ya vistas en las SP anteriores (del host a la roseta, de ésta al patch panel, de este al concentrador, cableado horizontal, vertical, etc)..

## Problemas del exceso de tráfico:

Cuando hay un solo medio (cable) y diferentes segmentos conectados por dispositivos que no filtran tráfico (repetidores o hubs), puede suceder que más de un usuario intente enviar datos a través de la red al mismo tiempo. Esto se da, por ejemplo, en Ethernet, cuyo Acceso al Medio, como ya vimos, es CSMA/CD.

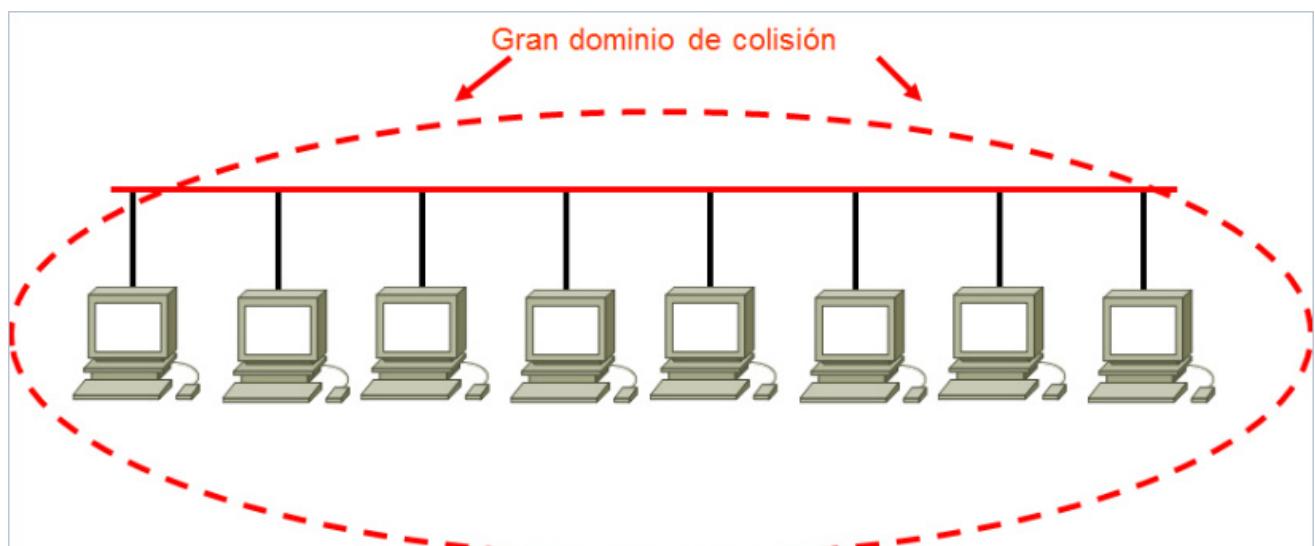
Según Ethernet, si más de un nodo intenta transmitir al mismo tiempo, se producirá una colisión. En este caso, los datos se dañan entre sí, siendo imposible distinguir los datos de ambos mensajes.

**Dominio de colisión:** El área donde se producen colisiones se llama "Dominio de Colisión".



En el caso de una colisión, la tarjeta NIC emite una "postergación" basadas en un algoritmo, lo que provoca un retardo diferente en cada dispositivo. Esto minimiza las colisiones, pero no las elimina.

Si existen muchas computadoras en la red y/o el tráfico es "pesado", se reiterarán las colisiones provocando repetidas postergaciones y demoras en el tráfico. Incluso, en un caso extremo puede provocar la inoperatividad total de la red.

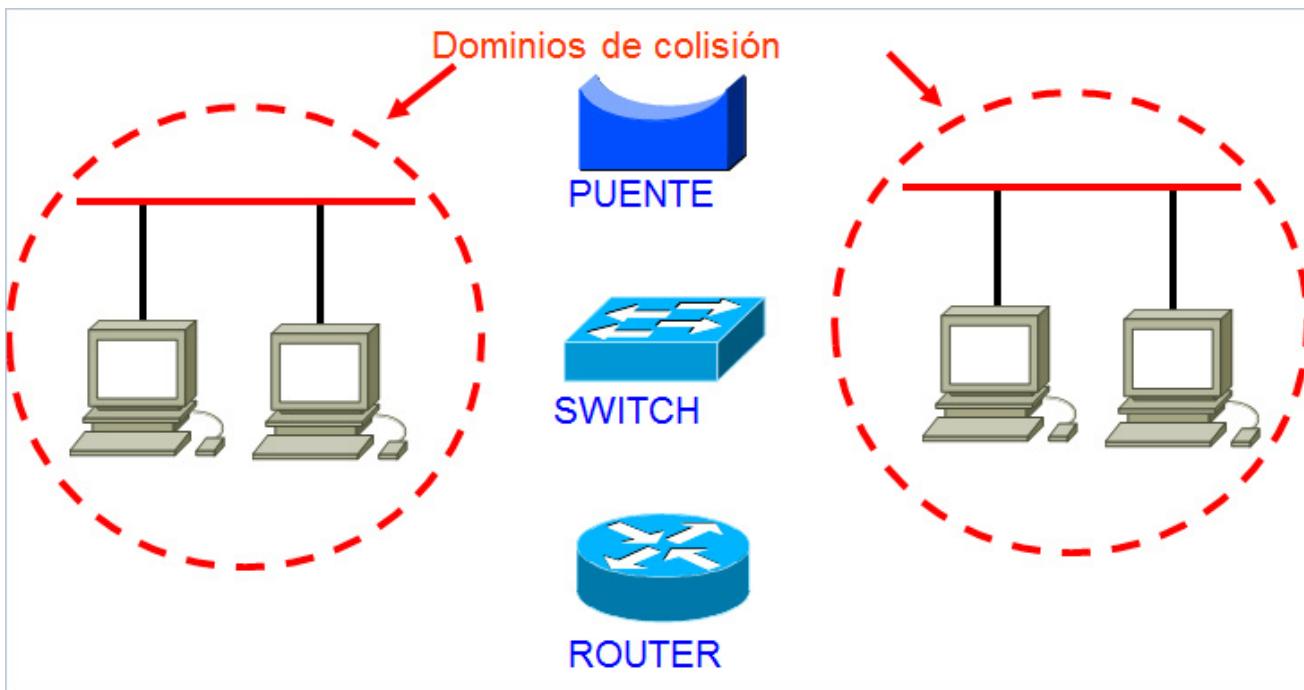


"Gran dominio de colisión" | Autor

Desventajas de estos dispositivos:

- No puede filtrar tráfico de red.
- Los bits que llegan a un puerto salen a todos los puertos (excepto por el puerto donde entraron).
- Los datos son transferidos a todos los segmentos de LAN (independientemente de si es necesario que deban llegar allí o no).

Solución al problema de las colisiones y exceso de tráfico innecesario: si tiene exceso de tráfico o exceso de colisiones, utilice Puentes/Switches y/o Routers (se explican más adelante, en los dispositivos de capa 2 y capa 3)

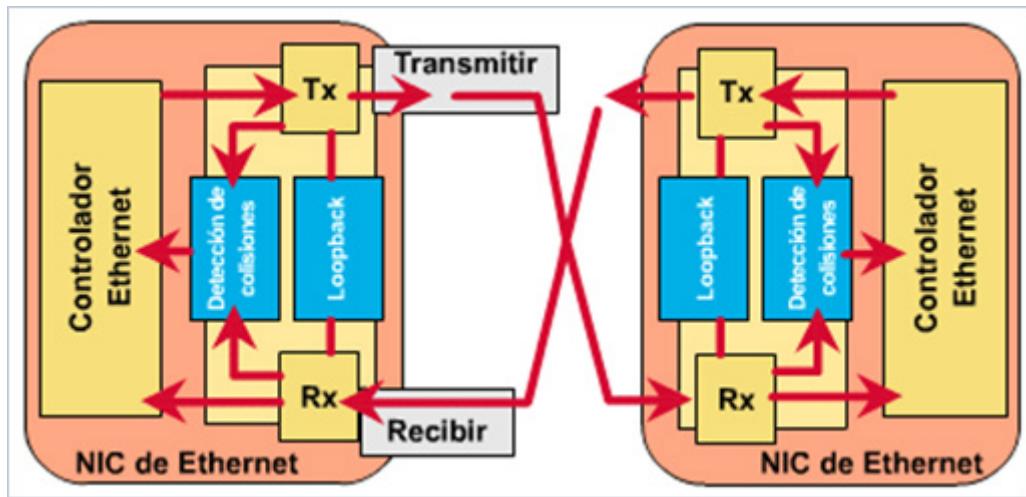


"Segmentación" | Autor

## Dispositivos de Capa 2

### NIC (Network Interface Card): La tarjetas de red

Es la tarjeta que conecta cada dispositivo con los medios de red. Se conecta a una motherboard y suministra los puertos para la conexión. Esta tarjeta puede estar diseñada como una tarjeta Ethernet, una tarjeta Token Ring o una tarjeta FDDI.



"Nic" | Autor

Permite las conexiones físicas entre las estaciones de trabajo y la red. Las tarjetas de red requieren una IRQ, una dirección E/S y direcciones de memoria. Para el caso de las redes Ethernet trae de fábrica la dirección física o MAC que actúa en la Capa de Enlace de Datos del Modelo OSI.



"NIC" | Autor

En la LAN, cada estación de trabajo y los servidores tienen al menos una tarjeta NIC. Está diseñada para enchufar dentro de una de las ranuras de expansión del motherboard.

## Funciones de la tarjeta de red:

- Brindar un punto de conexión para los medios de networking.
- Formar tramas de datos y enviarlos a través de los medios y transformarlos en información que las estaciones de trabajo puedan comprender.
- Implementar el acceso ordenado a los medios de red compartidos.

La elección del medio físico puede condicionar la elección de la tarjeta NIC. Algunas tienen circuitos para varios tipos de conexión. Las siguientes son las **características a tener en cuenta** en el momento de elegir el tipo de tarjeta de red a utilizar:

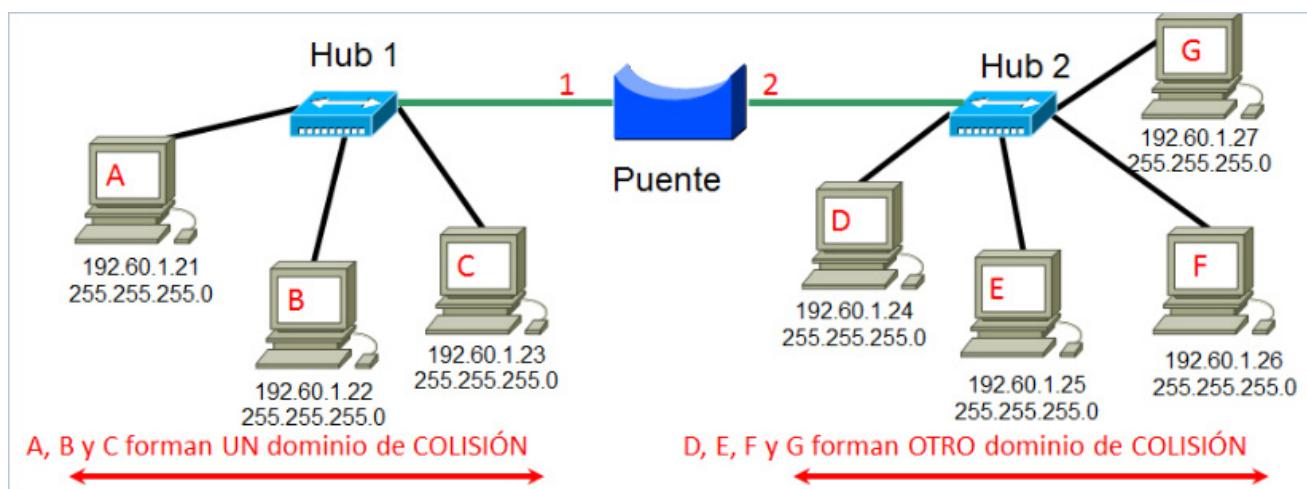
- El tipo de red (*Ethernet, Token Ring, FDDI* u otro)
- El tipo de medios (UTP, Coaxial, Fibra Óptica, Wireless)
- El tipo de bus de sistema (PCI, PCIe, USB)

## Bridge (Puente)

Dispositivo de networking que conecta segmentos de red. Arma una tabla con las direcciones físicas que aprende de los equipos que tiene conectados en cada puerta. Toma decisiones con respecto a si debe transferir señales al otro segmento en función de las direcciones físicas aprendidas.

Por lo tanto: mejora el desempeño de una red al eliminar el tráfico innecesario y minimiza las colisiones.

Se usa para dividir grandes dominios de colisión. Divide a la red en segmentos más pequeños y reduce la cantidad de tráfico entre los segmentos, como se ilustra en la figura siguiente:



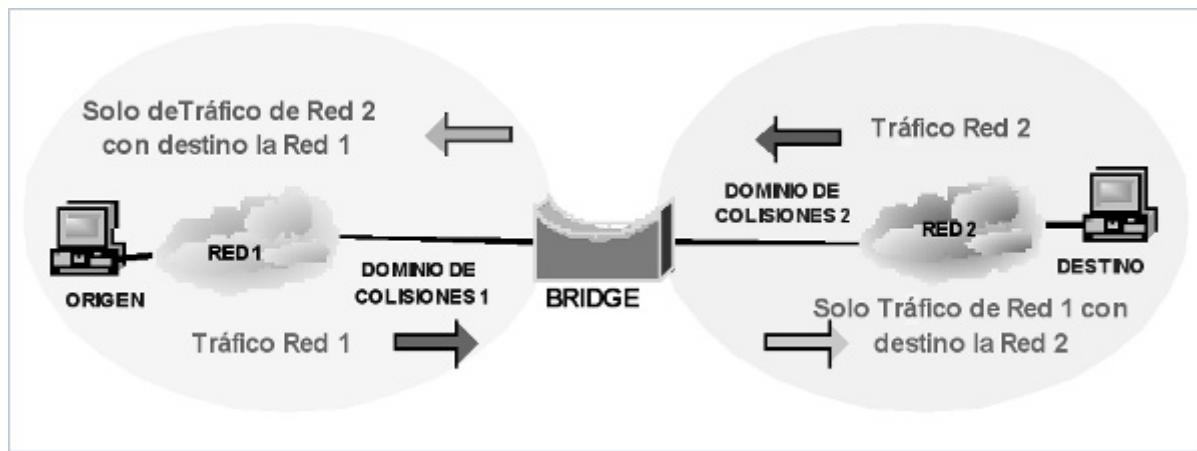
"Puente" | Autor

Sus características pueden resumirse en los siguientes puntos:

- Actúan en la Capa de Enlace del Modelo OSI.
- Filtran datos según la dirección MAC de destino.
- Pasan tramas entre segmentos redes que operan bajo protocolos diferentes como por ejemplo:

**Ethernet ↔ Token Ring**

- No se preocupan de los protocolos.



#### Ventajas de los Puentes (Bridges):

- Operan en la Capa de Enlace de Datos (capa 2 del Modelo OSI).
- Eliminan el tráfico innecesario.
- Minimizan las colisiones, dividiendo las redes en segmentos y filtrando el tráfico en base a la dirección MAC.

#### ¿Cómo filtran los Puentes (Bridges)?

Los puentes o bridges filtran el tráfico construyendo tablas con las direcciones MAC de todas las redes conectadas a él.

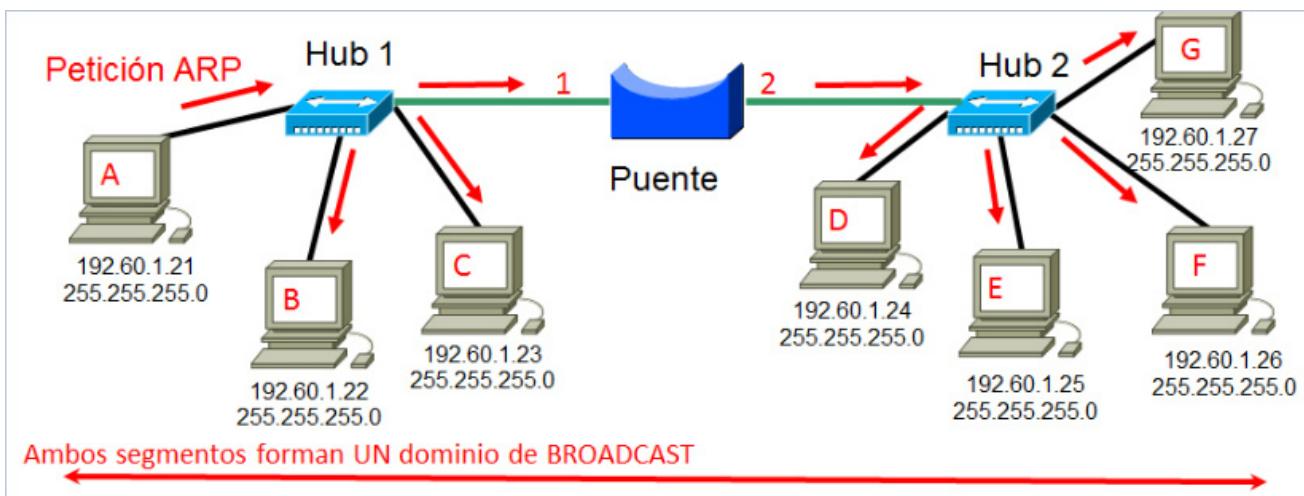
Toma la dirección MAC destino y la compara con sus tablas; si determina que esta dirección proviene del mismo segmento de red que el de origen, no la envía a los otros segmentos de red. En caso contrario, lo envía al segmento de red que corresponda. De esta manera eliminan el tráfico innecesario.

#### Desventajas de los Puentes (o problemas que no pueden resolver los Bridges):

- Trabajan mejor cuando el tráfico de un segmento a otro de la red no es demasiado grande. Cuando el tráfico es pesado, el bridge puede ser un cuello de botella y hacer más lenta la comunicación.
- Los bridges extienden los broadcasts.

#### Que son los broadcasts?

Recuerde cuando vimos ARP, cuando un dispositivo de red quiere llegar a otro pero no conoce la dirección de destino. En ese caso, el origen envía un broadcast. El broadcast se envía a todos los dispositivos de la red. Estos deben prestar atención a dichos broadcast.



"Broadcast" | Autor

Qué problema originan los broadcasts?

Si se envían demasiados broadcast, se puede producir una "tormenta de broadcast". Una tormenta de broadcast puede retrasar la información más allá de los límites de tiempo, causar demoras en el tráfico y hacer que la red no pueda operar a un nivel óptimo. En casos extremos una tormenta de broadcast puede bloquear a toda la red.

## Switch

El Switch es un bridge multipuerto, dispositivo de red que filtra y envía tramas en base a la dirección de destino de cada trama. Permite establecer una conexión cuando resulte necesario, y terminarla cuando ya no haya sesión que soportar.

Los switches, también denominados switches de LAN, por lo general reemplazan los hubs y funcionan con la infraestructura de cableado existente, de manera que su instalación puede realizarse con un mínimo de problemas en las redes de cableado estructurado anteriores.

### Lan Switching o Comutación LAN

La comutación es una tecnología que alivia la congestión, en las LAN Ethernet, reduciendo el tráfico y aumentando el ancho de banda.

La comutación LAN compensa la escasez de ancho de banda y los cuellos de botella de la red, como los que aparecen entre varias estaciones y un servidor de archivos remoto. Un switch puede segmentar una LAN en micro segmentos de un solo host. Esto crea dominios libres de colisión a partir de un dominio de colisión grande.

Aunque el switch elimina los dominios de colisión, todos los hosts conectados al switch siguen estando en el mismo dominio de broadcast. Por lo tanto, todos los nodos conectados a través del switch pueden ver un broadcast desde un solo nodo.

La Ethernet comutada se basa en una red donde cada nodo está directamente conectado a uno de sus puertos o a un segmento conectado a uno de los puertos del switch. Esto crea una conexión de ancho de banda de 10/100 Mbps entre cada nodo y cada segmento del switch. Una estación conectada directamente a un switch Ethernet representa su propio dominio de colisión y accede a los 10/100 Mbps completos.

Una LAN que utiliza una topología Ethernet conmutada crea una red que se comporta como si tuviera solamente dos nodos: el nodo emisor y el nodo receptor. Estos dos nodos comparten el ancho de banda entre sí, lo que significa que casi todo el ancho de banda está disponible para la transmisión de datos. Debido a que una LAN Ethernet conmutada utiliza con tanta eficiencia el ancho de banda, proporciona un rendimiento mayor que el de una LAN Ethernet conectada mediante puentes o hub. En la implementación de Ethernet conmutada, el ancho de banda disponible puede alcanzar aproximadamente el 100%.

La conmutación aumenta el ancho de banda disponible en una red, creando segmentos de red dedicados (es decir, conexiones punto a punto) y conectando dichos segmentos en una red virtual dentro del switch. Este circuito de red virtual existe solamente cuando dos nodos necesitan comunicarse. Es por ello que se llama circuito virtual: existe solamente cuando se necesita y se establece dentro del switch.

Una desventaja de los switches es que son más caros que los hub. Sin embargo, muchas empresas implementan la tecnología de conmutación paulatinamente, conectando los hub a switches hasta que llegue el momento en que se puedan reemplazar los hub.

## Operaciones básicas del switch

La conmutación es una tecnología que reduce la congestión en las LAN Ethernet, Token Ring y FDDI disminuyendo el tráfico y aumentando el ancho de banda. Los switches LAN se utilizan frecuentemente para reemplazar hub compartidos. Están diseñados para funcionar con infraestructuras de cable ya existentes, de manera que se pueden instalar sin provocar disturbios en el tráfico de red existente.

Actualmente, en la comunicación de datos, todos los equipos de conmutación realizan dos operaciones básicas:

- Comutación de tramas: esto ocurre cuando una trama llega a un puerto de entrada y se transmite a un puerto de salida.
- Mantenimiento de las operaciones de conmutación: un switch desarrolla y mantiene las tablas de conmutación.

El término "*bridging*" se refiere a la tecnología en la cual un dispositivo conocido como puente conecta dos o más segmentos de la LAN. Un puente transmite datagramas de un segmento a otros segmentos. Cuando un puente se activa y empieza a operar, examina la dirección MAC de los datagramas entrantes y crea una tabla de destinos conocidos. Si el puente sabe que el destino de un datagrama se encuentra en el mismo segmento que el origen, descarta el datagrama ya que no hay necesidad de transmitirlo.

Si el puente sabe que el destino se encuentra en otro segmento, transmite el datagrama a ese segmento solamente.

Si el puente no conoce el segmento destino, transmite el datagrama a todos los segmentos salvo el segmento origen (técnica conocida como inundación). La ventaja principal de la técnica de "*bridging*" es que limita el tráfico a ciertos segmentos de red.

Tanto puentes como switches conectan los segmentos LAN y utilizan una tabla de direcciones MAC para determinar el segmento al que se debe transmitir un datagrama y reducen el tráfico.

Los switches son más funcionales que los puentes en las redes actuales porque operan a una velocidad mucho más alta que los puentes y soportan nuevas funcionalidades, como por ejemplo las LAN Virtuales (VLAN).

## Comutación de Capa 2 y 3

Existen dos métodos de conmutación de tramas:

- Comutación a nivel de Capa 2.
- Comutación a nivel de Capa 3.

La conmutación es el proceso de tomar una trama que llega por una interfaz y enviarla a través de otra interfaz. Los routers utilizan la conmutación de Capa 3 para enrutar un paquete; los switches (switches de Capa 2) utilizan la conmutación de Capa 2 para enviar tramas.

La diferencia entre la conmutación de Capa 2 y Capa 3 es el tipo de información que se encuentra dentro de la trama y que se utiliza para determinar la interfaz de salida correcta.

- Con la conmutación de Capa 2, las tramas se comutan tomando como base la información de la dirección MAC.
- Con la conmutación de Capa 3, las tramas se comutan tomando como base la información de la capa de red.

La conmutación de Capa 2 no mira dentro de un paquete para obtener información de la capa de red como lo hace la conmutación de Capa 3.

La conmutación de capa 2 busca una dirección MAC destino dentro de una trama. Envía la información a la interfaz apropiada, si conoce la ubicación de la dirección destino. La conmutación de capa 2 crea y mantiene una tabla de conmutación que ayuda a ubicar las direcciones MAC que pertenecen a cada puerto o interfaz.

Si el switch de capa 2 no sabe dónde enviar la trama, realiza el broadcast de la trama desde todos sus puertos hacia la red a fin de saber cuál es el destino correcto. Una vez que vuelve la trama de respuesta, el switch aprende la ubicación de la nueva dirección y agrega la información a la tabla de conmutación.

Las direcciones de Capa 2 utilizan un espacio de dirección plano con direcciones universalmente únicas.

La conmutación de Capa 3 opera a nivel de la capa de red. Examina la información del paquete y envía los paquetes tomando como base las direcciones destino de la capa de red. La conmutación de Capa 3 también soporta la funcionalidad del router.

En la mayoría de los casos, el administrador de red determina las direcciones de Capa 3. Los protocolos como IP, IPX y AppleTalk utilizan el direccionamiento de Capa 3. Al crear direcciones de Capa 3, un administrador de red crea áreas locales que actúan como unidades de direccionamiento únicas (similares a las calles, ciudades, estados y países) y asigna un número a cada entidad local. Si los usuarios se mudan a otro edificio, sus estaciones finales obtienen nuevas direcciones de Capa 3, pero sus direcciones de Capa 2 permanecen iguales. Por ejemplo, una persona que se cambia de domicilio, cambiará su dirección postal, pero mantendrá su número de documento (DNI).

Como los routers operan a nivel de Capa 3 del modelo de referencia OSI, pueden adoptar y crear una estructura de direccionamiento jerárquico. Por lo tanto, una red enrutada puede unir una estructura de direccionamiento lógico a una infraestructura física, por ejemplo, a través de subredes TCP/IP.

El flujo de tráfico en una red conmutada (es decir, plana) es, por lo tanto, inherentemente diferente del flujo de tráfico en una red enrutada (es decir, jerárquica). Las redes jerárquicas permiten un flujo de tráfico más flexible que las redes planas, ya que pueden usar la jerarquía de red para determinar las rutas óptimas y contener los dominios de broadcast.

## Microsegmentación

El poder creciente de los procesadores, los requisitos cliente/servidor y las aplicaciones multimediales han creado y aumentado la necesidad de un ancho de banda mayor en los entornos compartidos tradicionales. Estos requisitos indican a los diseñadores de red que deben reemplazar los hub en los centros de cableado por

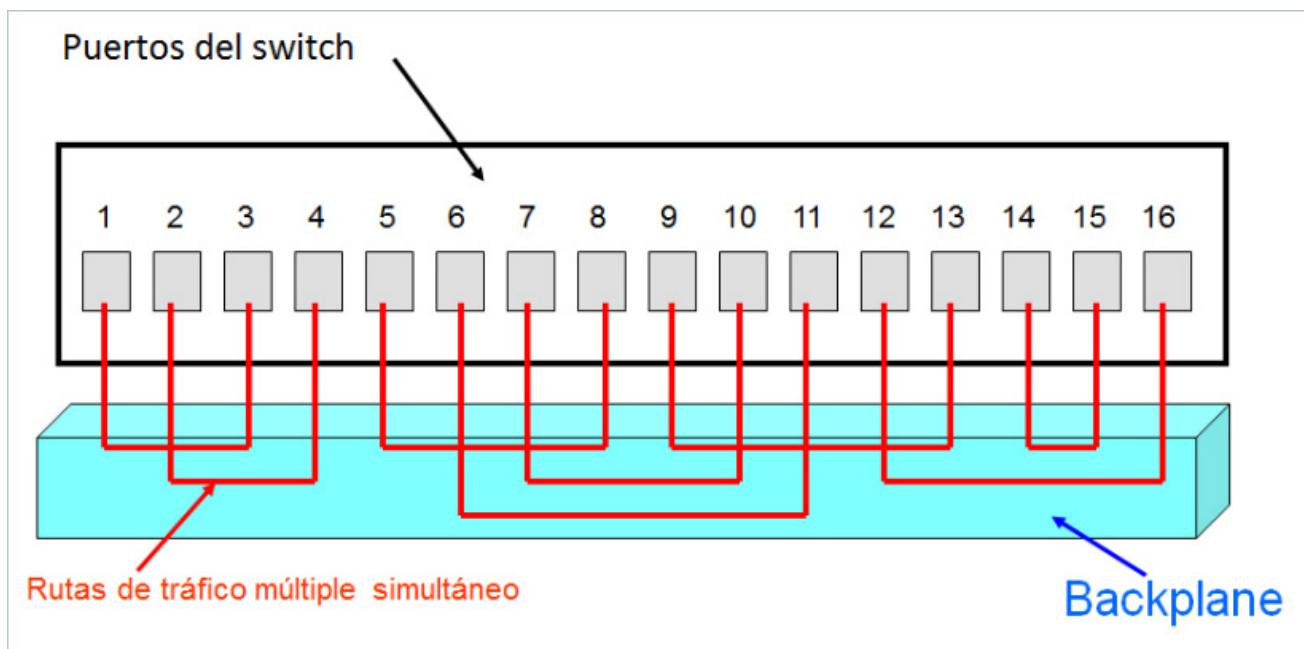
switches.

Como en el caso de los puentes, los switches conectan segmentos de la LAN, usan una tabla de direcciones MAC para determinar el segmento en el que es necesario transmitir un datagrama y reducen el tráfico.

Los switches operan a velocidades mucho más altas que los puentes y pueden soportar nuevas funcionalidades como, por ejemplo, las LAN virtuales.

Un switch Ethernet brinda muchas ventajas como, por ejemplo, permitir que varios usuarios se comuniquen en paralelo a través del uso de circuitos virtuales y segmentos de red dedicados en un entorno libre de colisiones. Esto aumenta el ancho de banda disponible en el medio compartido.

Los switches de Capa 2 utilizan microsegmentación para satisfacer las demandas de mayor ancho de banda y un mejor rendimiento.



"Microsegmentación" | Autor

Se puede pensar en cada puerto de switch como un micropuente; este proceso se llama microsegmentación.

De este modo, cada puerto de switch funciona como un puente individual y otorga el ancho de banda total del medio a cada host.

De forma similar a los puentes o bridges, los switches envían e inundan el tráfico en base a las direcciones MAC.

## ¿Cómo conoce las direcciones un Switch?

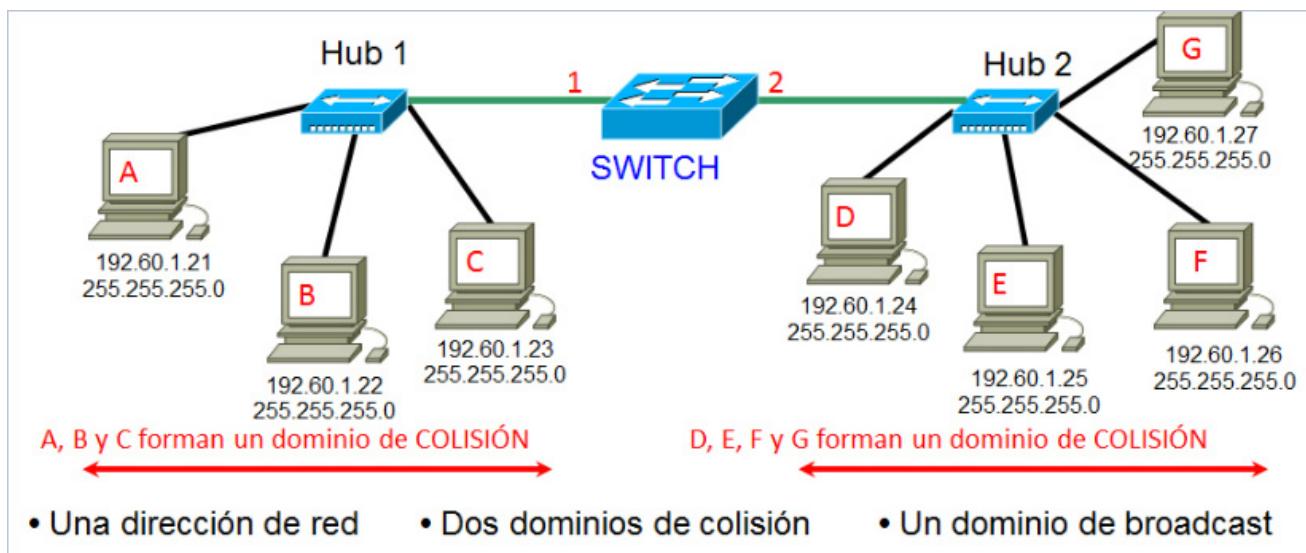
Un switch Ethernet puede aprender la dirección de cada dispositivo de la red leyendo la dirección origen de cada paquete transmitido y anotando el puerto donde la trama se introdujo en el switch.

Las direcciones se aprenden de forma dinámica. Esto significa que, a medida que se leen las nuevas direcciones, éstas se aprenden y se almacenan en la memoria. Cuando se lee un origen que no se encuentra en la memoria, se aprende y almacena para su uso futuro.

Cada vez que una dirección se almacena, se le agrega un **timeout** \*21.1. Esto permite almacenar las direcciones durante un período de tiempo determinado. Cada vez que se hace referencia a una dirección, recibe un nuevo timeout . Las direcciones a las cuales no se hace referencia durante un determinado período de tiempo, se eliminan de la lista. Al eliminar direcciones antiguas, se logra mantener una base de datos de envío precisa y funcional.

## Segmentación con Switch

Si utilizamos el switch de la siguiente forma:



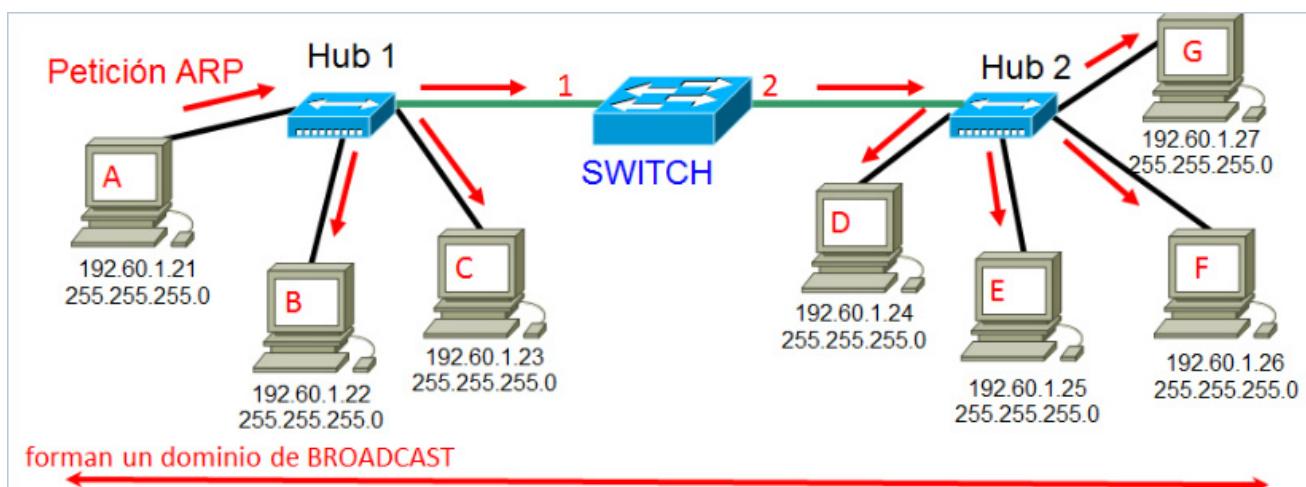
"Segmentación con switch" | Autor

El Switch aprende las direcciones MAC para cada puerto o boca de conexión

En este esquema, si A y B se comunican, D,E,F, y G no se enteran

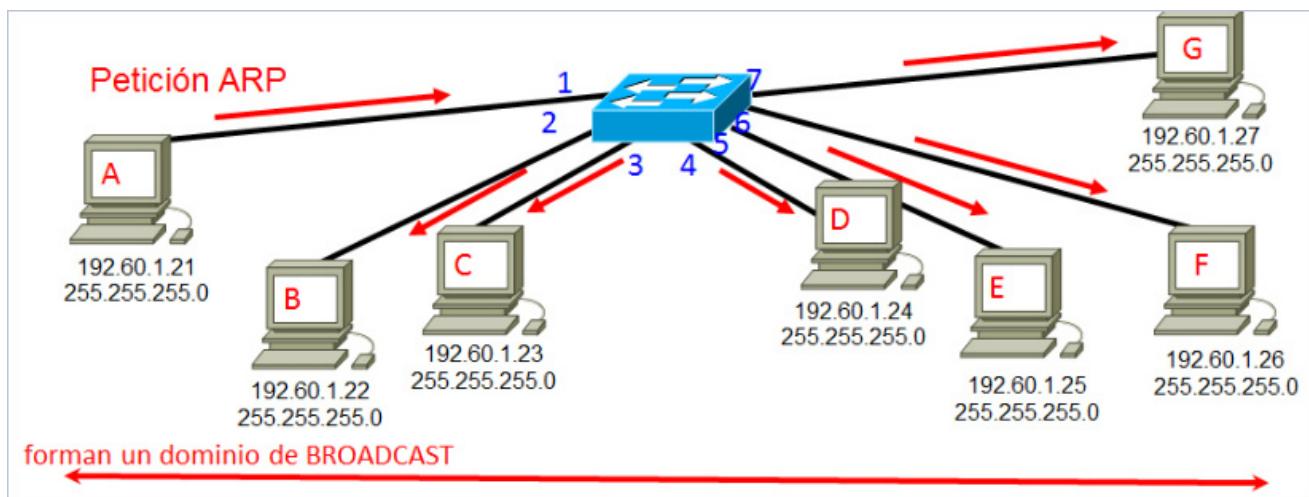
Se ha logrado dividir el dominio de colisión en dos más pequeños

Pero qué pasaría si se generara una petición ARP?



Si se genera una petición ARP, esta se propaga a toda la red, pues todos los equipos forman un solo dominio de broadcast. En redes grandes se puede generar lo que llamamos "tormenta de broadcast".

Otra forma de conectar el Switch es prescindiendo de los hubs:



De esta forma no eliminamos el problema del broadcast, pero si reducimos al máximo posible las colisiones, pues se generan tantos dominios de colisión como puertos o bocas de conexión tenga el Switch.

## Ventajas de LAN switching

Los switches ofrecen muchas ventajas.

- Habilita el acceso dedicado entre origen y destino: permiten que varios usuarios puedan comunicarse utilizando segmentos de red dedicados.
- Soporta múltiples comunicaciones simultáneas: permiten que varios usuarios puedan comunicarse en paralelo usando circuitos virtuales.
- Elimina las colisiones y aumenta la capacidad: en un entorno sin colisiones se maximiza la velocidad de transferencia disponible en el medio compartido.

Además, el desplazamiento hacia un entorno LAN commutado es muy económico ya que se puede volver a utilizar el hardware y el cableado existentes.

El poder del switch combinado con el software para la configuración de las LAN, otorga a los administradores de red gran flexibilidad para el manejo de la red.

## Desventajas

Como hemos visto, un Switch mejora la velocidad de transferencia separando los dominios de colisión y enviando de forma selectiva el tráfico a los segmentos correspondientes de una red.

Aunque el switch de LAN reduce el tamaño de los dominios de colisión, todos los hosts conectados al switch se encuentran todavía en el mismo dominio de broadcast, por lo tanto, un broadcast desde un nodo será visto por todos los demás nodos conectados a través del switch de LAN.

Una solución sería separar físicamente las redes. Pero... ¿Cómo podemos hacer que los datos viajen entre dos redes?

Colocando dispositivos de Capa 3 para permitir que los datos entre redes y/o subredes puedan enrutarse.

# REFERENCIAS 21

## 21.1 : Timeout

Significa una marca horaria, vencido el tiempo asignado, el algoritmo tomará una decisión.

---



¡Vamos a comprobar cuánto aprendiste!

**1. Indique la opción correcta**

Los dispositivos de networking se usan para conectar redes.

- Verdadero
- Falso

**2. Indique la opción correcta**

A los Hubs también se los conoce como Repetidores Multipuerto.

- Verdadero
- Falso

**3. Indique la opción correcta**

Todas las redes tienen en común:

- Una estructura.
- Un funcionamiento que permite la comunicación origen - destino.
- Todas las anteriores.
- Ninguna de las anteriores.

**4. Indique la opción correcta**

Un Repetidor:

- Opera en la Capa Física (capa 1 del Modelo OSI).
- Permite aumentar el número de nodos conectados a una red.
- Permiten aumentar la extensión de la red.
- Todas las anteriores.

**5. Indique la opción correcta**

Un Repetidor realiza la función de:

- Regenerar la señal.
- Amplificar la señal.

- Todas las anteriores.
- Ninguna de las anteriores.

#### 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Bridge	permite a los dispositivos conectarse a una red. Almacena las direcciones físicas y gestiona el acceso al medio.
NIC	reconstruye y repite señales a nivel físico en todos los puertos. Es también llamado Repetidor Multipuerto.
Hub	segmenta redes y permite filtrar tráfico identificándolo por su dirección física. Divide dominios de colisión.
Repetidor	reconstruye y repite señales a nivel físico.

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Los dispositivos de networking se usan para conectar redes.

Verdadero

Falso

## 2. Indique la opción correcta

A los Hubs también se los conoce como Repetidores Multipuerto.

Verdadero

Falso

## 3. Indique la opción correcta

Todas las redes tienen en común:

Una estructura.

Un funcionamiento que permite la comunicación origen - destino.

Todas las anteriores.

Ninguna de las anteriores.

## 4. Indique la opción correcta

Un Repetidor:

Opera en la Capa Física (capa 1 del Modelo OSI).

Permite aumentar el número de nodos conectados a una red.

Permiten aumentar la extensión de la red.

Todas las anteriores.

## 5. Indique la opción correcta

Un Repetidor realiza la función de:

Regenerar la señal.

Amplificar la señal.

Todas las anteriores.

Ninguna de las anteriores.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Bridge

segmenta redes y permite filtrar tráfico  
identificándolo por su dirección física. Divide  
dominios de colisión.

NIC

permite a los dispositivos conectarse a una red.  
Almacena las direcciones físicas y gestiona el  
acceso al medio.

Hub

reconstruye y repite señales a nivel físico en  
todos los puertos. Es también llamado  
Repetidor Multipuerto.

Repetidor

reconstruye y repite señales a nivel físico.

# SP11 / H2: Dispositivos de Conectividad: Capas 3 a 7: Router, Firewall e IDS

## Dispositivos de Capa 3

### Router

El Router es un dispositivo de networking que se usa para conectar distintas redes. Permite pasar paquetes de datos entre redes en base al direccionamiento de Capa 3 del Modelo OSI.

### Diferencias entre Switch y Router

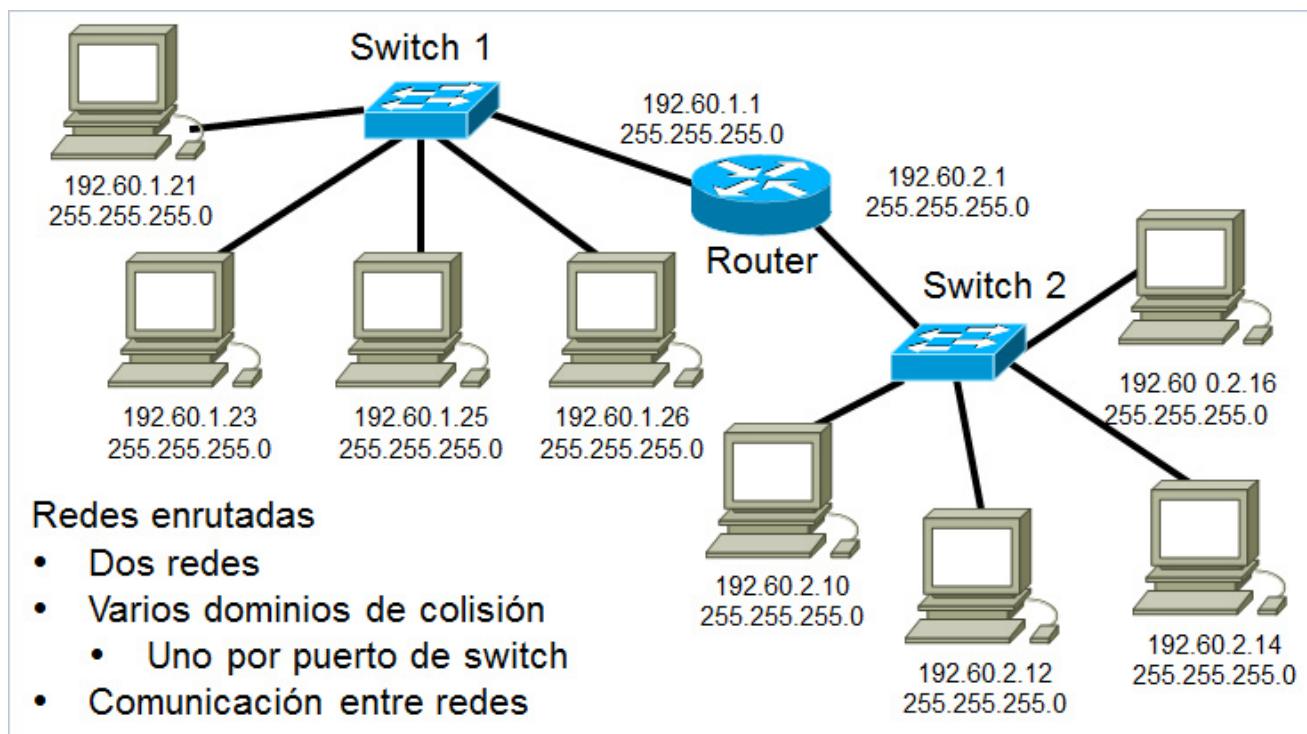
Se resumen en la siguiente tabla:

Switch	Router
Actúa en la capa de <b>Enlace</b>	Actúa en la capa de <b>Red</b>
Utiliza direcciones <b>MAC</b>	Utiliza direcciones <b>IP</b>
Longitud de la dirección: <b>48 bits</b>	Longitud de la dirección: <b>32 bits</b>
Las direcciones MAC están <b>dentro de la NIC</b>	Se implementa sobre el <b>software</b>
Direcciones asignadas por el <b>fabricante</b> de la NIC	Direcciones asignadas por <b>administrador</b>
Esquema de direccionamiento <b>plano</b>	Esquema de direccionamiento <b>jerárquico</b>
Conecta diferentes <b>redes/subredes</b>	Conecta diferentes <b>segmentos de red</b>

"Diferencias entre Switch y Router" | Autor

### Segmentación con Router

Vemos ahora una forma habitual de conexión para aprovechar la capacidad de un Router:



"Segmentación con Router" | Autor

En este esquema se pueden observar dos dominios de broadcast separados, porque el router no envía broadcasts de la capa 2, como peticiones ARP.

Cada interfaz en el router se conecta a una red separada, de manera que la inserción de un router en una LAN separa dominios de colisión y de broadcast, porque, como ya dijimos, los routers no envían broadcasts.

El router puede ejecutar la selección de mejor ruta. El router se puede usar para conectar distintos medios de networking y distintas tecnologías de LAN simultáneamente.

Los routers pueden conectar las LAN que ejecutan distintos protocolos (IP; IPX; AppleTalk) y pueden tener conexiones seriales con las WAN.

## Funcionamiento de los Routers

Los routers se usan para conectar dos o más redes. Cada red debe tener un número de red único que está incorporado en la dirección IP asignada a cada dispositivo conectado a la red. Los routers pueden tener más de una dirección IP, una por cada red conectada.

Al llegar al router, éste realiza las siguientes funciones:

- Separa el encabezado de enlace de datos que lleva la trama.
- El router examina la capa 3 para determinar la red de destino.
- El router consulta su tabla de enrutamiento, para determinar por cuál de sus puertos enviará el paquete para que lleguen a la red de destino.
- Antes de enviar los datos a través del puerto correspondiente, encapsula los datos en la correspondiente trama de enlace de datos.

## ¿Cuándo un dispositivo busca los servicios de un router?

Un dispositivo de red, no puede enviar una solicitud ARP a un dispositivo de otra red. Por lo tanto, si el origen está en una red distinta a la de destino y si el origen desconoce la dirección MAC destino, deberá utilizar los servicios de un router.

De esta forma, los routers actúan como gateway por defecto. El origen encapsula los datos teniendo como dirección destino la MAC del router. El origen usa la IP destino y no la del router.

Si el router ubica la dirección IP y MAC de destino mapeadas y sabe que la red destino está conectada a uno de sus puertos, encapsula los datos con la nueva dirección MAC y los envía al destino correcto.

Si no puede ubicar la IP destino en sus tablas, el router ubica la dirección MAC de otro router que pueda cumplir con esa función y envía los datos a él. De esta forma, los Router se organizan para dar una respuesta ARP al dispositivo que originó la solicitud.

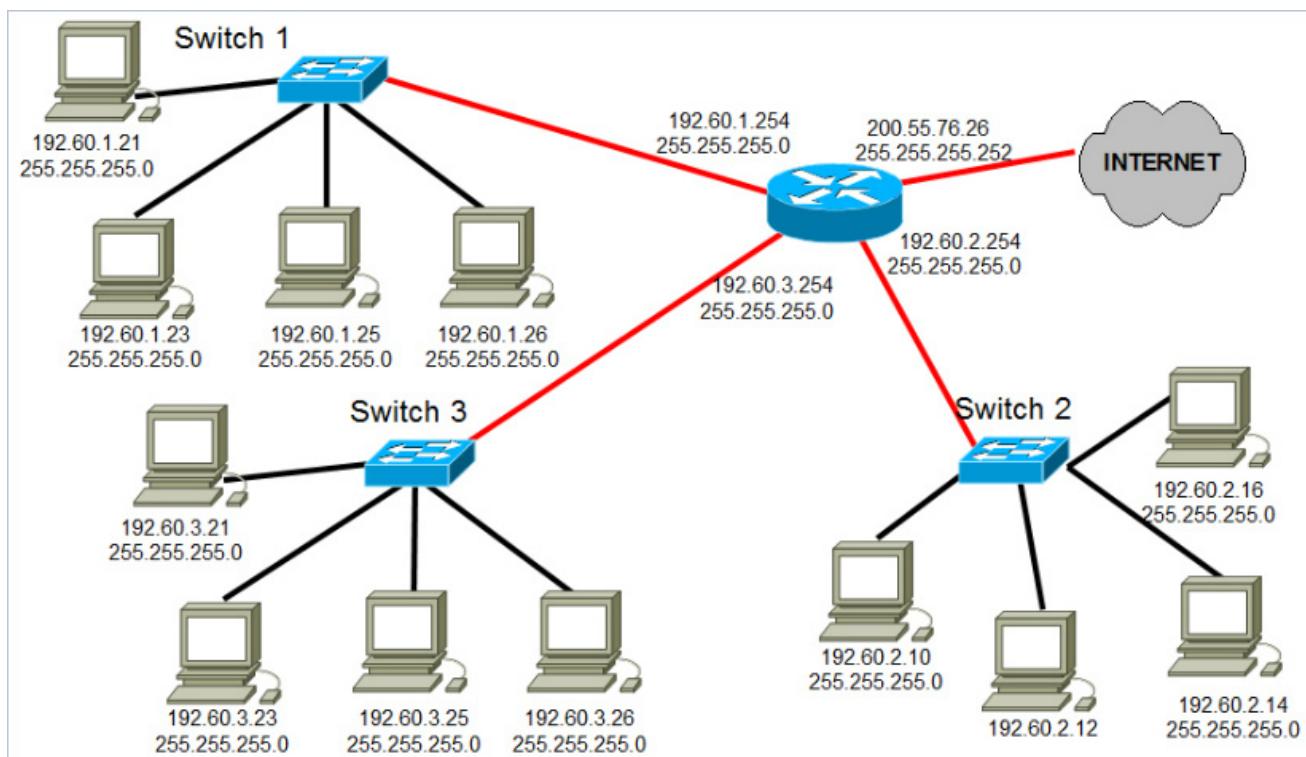
Además, los Routers llevan tablas ARP que mapean direcciones MAC de todas las redes a las cuales están conectados.

## ¿Qué problemas resuelven los routers?

Resuelven el problema del excesivo tráfico de broadcast, ya que no envían tramas a menos que se les indique. El enrutamiento que realizan los Routers ayuda a contener los broadcast.

## Segmentación con Router y conexión a Internet

Vemos a continuación otra forma habitual de conexión para aprovechar la capacidad de un Router:

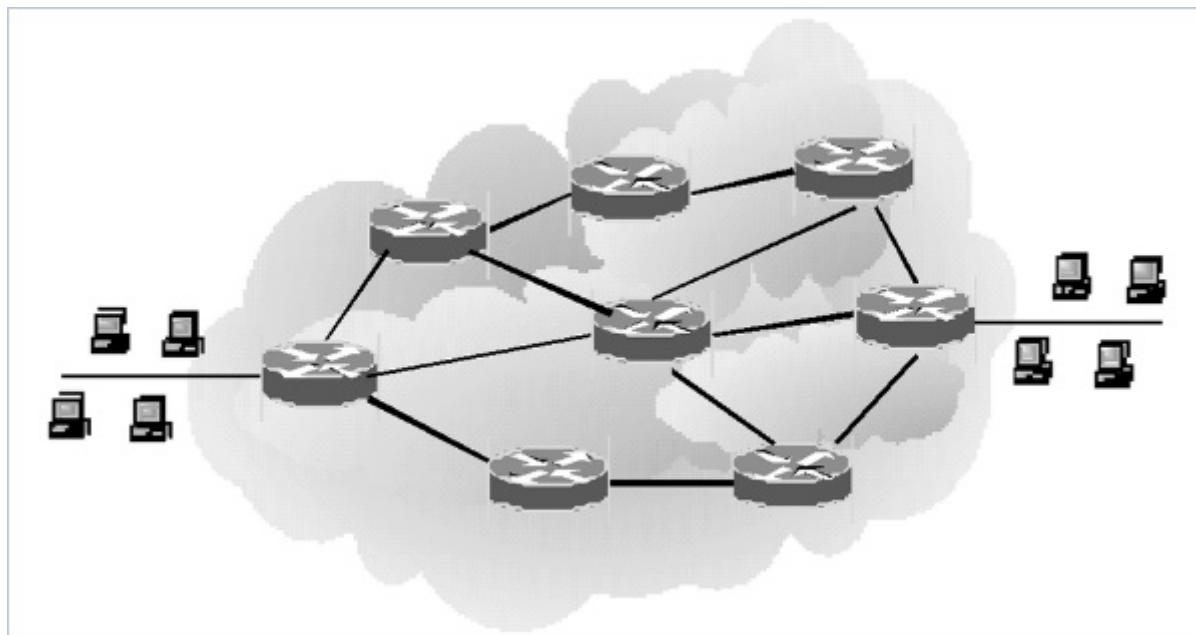


"Segmentación con Router conectado a Internet" | Autor

Esperamos que esta figura le sea de utilidad para pensar el esquema de conexión de sus futuras redes. Complemente con lo aprendido en las SP anteriores, tanto en lo referente a Redes y Subredes, Clases, Máscaras, Cableado Horizontal, Vertical, Backbone y otros conceptos que ya está en condiciones de integrar.

## Red de Routers

En una red de routers, como por ejemplo en una gran red LAN, como así también en redes MAN o WAN, se aprovecha la capacidad de los Routers para tomar decisiones "inteligentes" sobre cuál es la mejor ruta para entregar los datos a través de las redes.

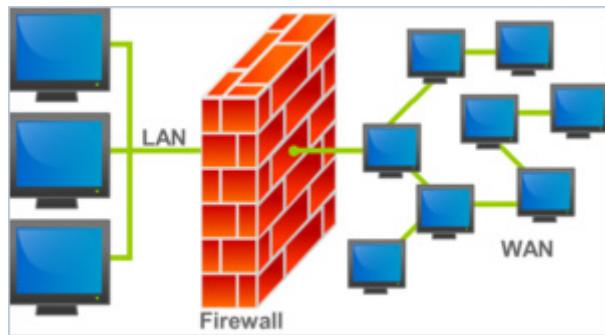


Para determinar la ruta a seguir, utilizan una o más métricas para decidir la ruta óptima por la cual se enviará el tráfico de red. Envían paquetes de una red a otra en base a la información de la capa de red.

## Dispositivos de Capa 3 a 7

### Firewall

Un Firewall (cortafuegos) o servidor de seguridad, puede ser un dispositivo de hardware o también un software. Se utiliza para ayudar a mantener una red segura. Su objetivo principal es controlar el tráfico de red entrante y saliente mediante el análisis de los paquetes de datos.



"Firewall" | <http://upload.wikimedia.org/wikipedia/commons/thumb/5/5b/Firewall.png/300px-Firewall.png>

En base a este análisis determina si se debe permitir o no atravesarlo, sobre la base de un conjunto de reglas predeterminado.

El Firewall de una red construye a nivel lógico un muro entre la red interna o equipo que protege y el resto de las redes.

Por lo general las otras redes son externas como Internet, que no se presupone segura y de confianza.



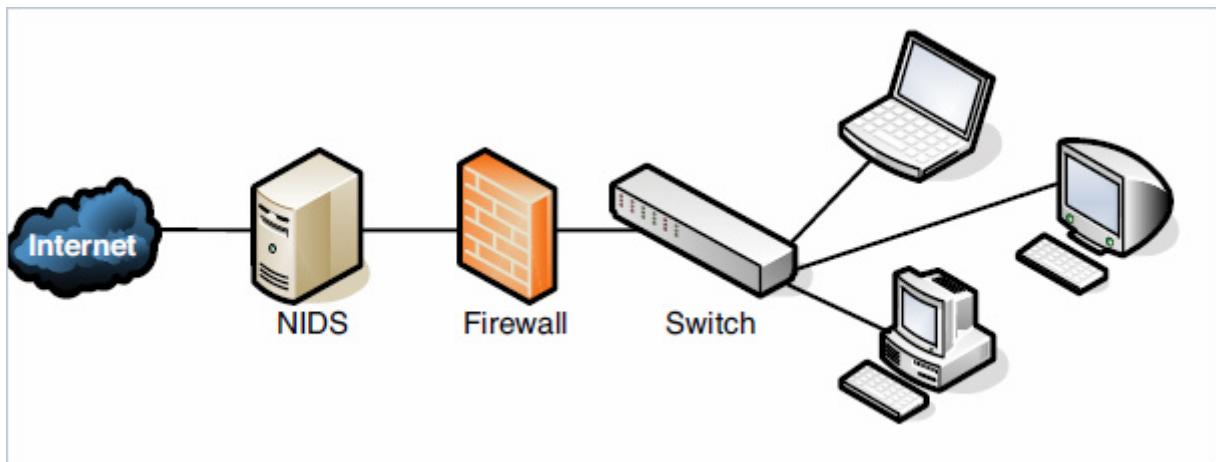
"Firewall hardware" | <http://www.ordenadores-y-portatiles.com/images/firewall-ip2.jpg>

Además de los equipos Firewall, muchos routers que pasan los datos entre redes contienen componentes de

servidor de seguridad y, también a la inversa, muchos *firewalls* pueden realizar funciones básicas de enrutamiento. También muchos sistemas operativos de computadoras personales incluyen Firewalls basados en *software* de protección contra las amenazas de Internet.

## IDS

Un IDS (*Intrusion Detection System*) o sistema de detección de intrusos puede ser un dispositivo de hardware o también una aplicación de software que monitorea las actividades de red o sistema, de actividades maliciosas o violaciones a la política de seguridad y produce informes que envía a computadora de administración. En una red se lo denomina también NIDS (*Network Intrusion Detection System*)



"IDS Diagrama" | [http://thuansoldier.net/?attachment\\_id=669](http://thuansoldier.net/?attachment_id=669)

No se espera que estos equipos detengan las intrusiones. Aunque algunos pueden hacer algo, la finalidad de estos equipos se centra principalmente en la prevención, identificando posibles incidencias, registrando la información sobre ellas, e informando los intentos de intrusión.

Además, las organizaciones utilizan IDS para otros fines, tales como la identificación de los problemas con las políticas de seguridad, la documentación de las amenazas existentes y la disuasión de las personas a violar las políticas de seguridad.

Su finalidad es detectar anomalías que impliquen riesgos, como pueden ser los intentos de ingresar a la red, los ataques de denegación de servicios, el escaneo de puertos o el análisis en tiempo real del tráfico de la red.

En la actualidad, los IDS se han convertido en un complemento necesario a la infraestructura de seguridad de casi todas las organizaciones y es necesario tenerlos en cuenta en la planificación de la red.



¿Te animás a medir cuánto aprendiste?

**1. Indique la opción correcta**

La segmentación de una red a través de un Switch crea dominios libres de colisión, a partir de un dominio de colisión grande.

- Verdadero
- Falso

**2. Indique la opción correcta**

Si el switch no conoce el segmento destino, transmite la trama a todos los segmentos, salvo el segmento origen.

- Verdadero
- Falso

**3. Indique la opción correcta**

Aunque el switch elimina los dominios de colisión, todos los hosts conectados al switch siguen estando en el mismo dominio de broadcast.

- Verdadero
- Falso

**4. Indique la opción correcta**

Una LAN que utiliza una topología Ethernet commutada crea una red que se comporta como si tuviera múltiples nodos.

- Verdadero
- Falso

**5. Indique la opción correcta**

El método de conmutación se produce:

- A nivel de Capa 2.
- A nivel de Capa 3.

- Las respuestas anteriores son correctas.
- Las respuestas anteriores son incorrectas.

#### 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Switch

segmenta redes con N interfaces. Tiene capacidad de memorizar / priorizar tráfico. detecta los posibles intrusos que intentan obtener acceso no autorizado a través de la red o en un servidor.

IDS

protege una red de otras clasificadas como de menor nivel de seguridad.

Firewall

interconecta segmentos de distintas redes dividiendo dominios de colisión y de broadcast.

Router

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

La segmentación de una red a través de un Switch crea dominios libres de colisión, a partir de un dominio de colisión grande.

- Verdadero
- Falso

## 2. Indique la opción correcta

Si el switch no conoce el segmento destino, transmite la trama a todos los segmentos, salvo el segmento origen.

- Verdadero
- Falso

## 3. Indique la opción correcta

Aunque el switch elimina los dominios de colisión, todos los hosts conectados al switch siguen estando en el mismo dominio de broadcast.

- Verdadero
- Falso

## 4. Indique la opción correcta

Una LAN que utiliza una topología Ethernet commutada crea una red que se comporta como si tuviera múltiples nodos.

- Verdadero
- Falso

## 5. Indique la opción correcta

El método de conmutación se produce:

- A nivel de Capa 2.
- A nivel de Capa 3.
- Las respuestas anteriores son correctas.
- Las respuestas anteriores son incorrectas.

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Switch	segmenta redes con N interfaces. Tiene capacidad de memorizar / priorizar tráfico.
IDS	detecta los posibles intrusos que intentan obtener acceso no autorizado a través de la red o en un servidor.
Firewall	protege una red de otras clasificadas como de menor nivel de seguridad.
Router	interconecta segmentos de distintas redes dividiendo dominios de colisión y de broadcast.



## SP11 / H3: VLAN (Virtual LAN)

Un switch segmenta físicamente una LAN en dominios de colisión individuales. Sin embargo, cada segmento sigue formando parte de un dominio de broadcast.

La cantidad total de segmentos en un switch es igual a un dominio de broadcast.

Esto significa que todos los nodos de todos los segmentos pueden ver un broadcast desde un nodo de un segmento.

Una VLAN es una agrupación lógica de dispositivos de red o de usuarios que no se limita a un segmento de switch físico.

Los dispositivos o usuarios de una VLAN se pueden agrupar por funciones, departamentos, aplicaciones, etc., independientemente de la ubicación física de su segmento. Una VLAN crea un dominio de broadcast único que no se restringe a un segmento físico y se considera como una subred.

La configuración de la VLAN se realiza en el switch a través del software. Las VLAN de la actualidad han sido estandarizadas de acuerdo con la norma IEEE 802.1Q; sin embargo, las implementaciones varían de un proveedor a otro.

### Configuraciones de LAN compartidas - VLAN

Una LAN típica se configura según la infraestructura física que conecta. Los usuarios se agrupan según su ubicación en relación con el HUB al que están conectados y según cómo el cable se tiende al centro del cableado.

El router que interconecta cada hub compartido normalmente proporciona segmentación y puede actuar como firewall de broadcast.

Los segmentos creados por los switches no lo hacen. La segmentación tradicional de las LAN no agrupa a los usuarios según su asociación de grupo de trabajo o necesidad de ancho de banda. Por lo tanto, comparten el mismo segmento y ocupan el mismo ancho de banda, aunque los requisitos de ancho de banda varían enormemente por grupo de trabajo o departamento.

### Agrupación en topologías virtuales

Las LAN se dividen cada vez con mayor frecuencia en grupos de trabajo, conectados mediante backbones comunes para formar topologías VLAN.

Las VLAN segmentan lógicamente la infraestructura física de las LAN en diferentes subredes (o dominios de broadcast para Ethernet).

Las tramas de broadcast se comutan sólo entre puertos dentro de la misma VLAN.

Las primeras implementaciones de VLAN ofrecían una función de asignación de puertos que establecía un dominio de broadcast entre un grupo de dispositivos por defecto.

Los requisitos actuales de la red exigen la funcionalidad de VLAN que cubre toda la red. Este enfoque de las VLAN permite agrupar usuarios separados por grandes distancias físicas en topologías virtuales que abarcan toda la red. Las configuraciones VLAN agrupan a los usuarios por asociación lógica, en lugar de por ubicación.

física.

La mayoría de las redes actuales ofrecen una segmentación lógica muy limitada. Los usuarios se agrupan normalmente según las conexiones al hub compartido y los puertos de router entre los hub. Esta topología brinda segmentación sólo entre hub, que normalmente se ubican en pisos separados, y no entre usuarios conectados al mismo hub. Esto impone restricciones físicas en la red y limita la manera en que los usuarios se pueden agrupar.

## Diferencias entre LAN conmutadas y VLAN

En una LAN que utiliza dispositivos de conmutación, la tecnología VLAN es una manera económica y eficiente de agrupar usuarios en grupos de trabajo virtuales, más allá de su ubicación física en la red.

Algunas de las diferencias principales son las siguientes:

- La comunicación entre las VLAN se implementa por enrutamiento de Capa 3.
- Las VLAN proporcionan un método para controlar los broadcast de red.
- El administrador de la red asigna usuarios a una VLAN.
- Las VLAN pueden aumentar la seguridad de la red, definiendo cuáles son los nodos de red que se pueden comunicar entre sí.

Mediante la tecnología VLAN, se pueden agrupar los puertos de switch y sus usuarios conectados en grupos de trabajo lógicamente definidos, como los siguientes:

Se pueden asociar puertos y usuarios en grupos de trabajo con un solo switch o varios switches conectados. Al agrupar los puertos y usuarios a través de múltiples switches, las VLAN pueden abarcar infraestructuras contenidas en un solo edificio, edificios conectados entre sí o, aun, redes de área amplia (WAN).

## Los routers y las VLAN

Los routers proporcionan *firewalls*, administración de broadcast y distribución de rutas. Los routers brindan rutas de conexión entre VLAN diferentes.

Obviamente también conectan otras partes que están lógicamente segmentadas desde el punto de vista más tradicional de subredes o accesos a la WAN. La comunicación de Capa 3 es una parte integral de cualquier arquitectura de conmutación de alto rendimiento.

Se pueden integrar routers en la arquitectura de conmutación, utilizando conexiones de backbone de alta velocidad. Normalmente éstas son conexiones *Fast Ethernet* o ATM, y brindan ventajas:

- Aumentan el rendimiento entre switches y routers.
- Consolidan la cantidad total de puertos de router físicos requeridos para la comunicación entre VLAN.

La arquitectura VLAN no sólo proporciona segmentación lógica, sino que puede mejorar considerablemente la eficiencia de la red.

## Las VLAN y el broadcast

El tráfico de broadcast se produce en todas las redes. La frecuencia de broadcast depende de las aplicaciones,

los tipos de servidores, la cantidad de segmentación lógica y la manera en que se usan estos recursos de red.

Aunque las aplicaciones se han perfeccionado durante los últimos años para reducir la cantidad de broadcast, se están desarrollando nuevas aplicaciones multimediales que producen gran cantidad de broadcast y multicast.

Es necesario tomar medidas para evitar los problemas relacionados con los broadcast. Una de las más efectivas es segmentar de manera adecuada la red, con firewalls de protección que, dentro de lo posible, eviten que los problemas de un segmento dañen otras partes de la red.

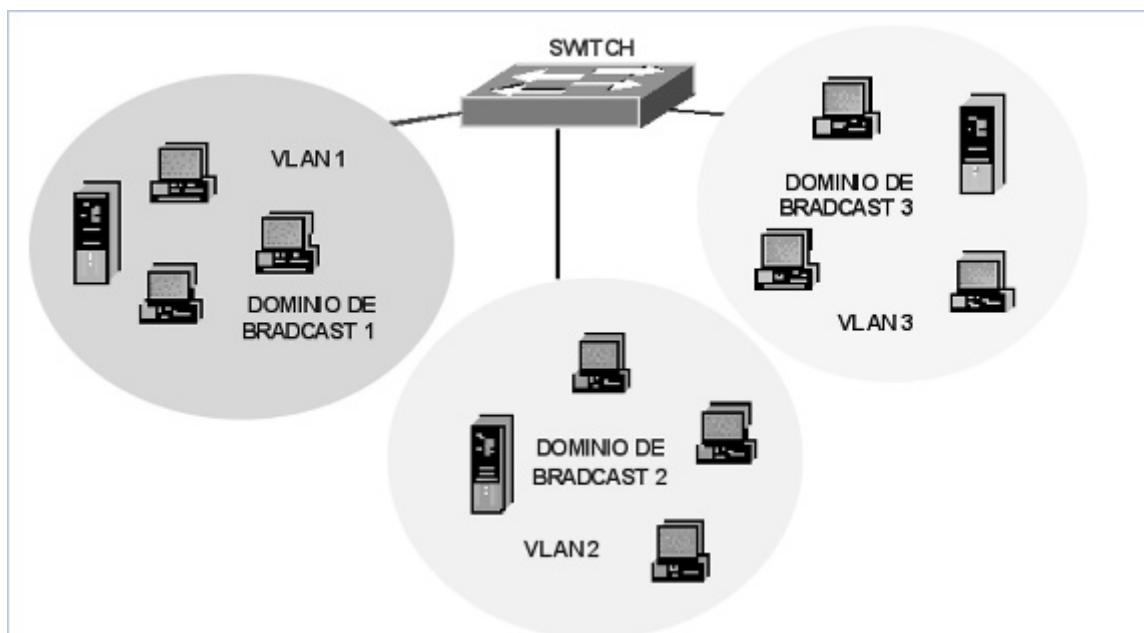
Así, aunque un segmento puede presentar condiciones de broadcast excesivas, el resto de la red se encuentra protegido. A esta división de los dominios de broadcast, la realizan normalmente los router. La segmentación con firewalls brinda confiabilidad y reduce al mínimo la sobrecarga de tráfico de broadcast, permitiendo un mayor rendimiento del tráfico de aplicaciones.

Cuando no se colocan routers para la conexión de switches, los broadcasts se envían a cada puerto del switches. Esto, normalmente, se denomina red plana, donde hay un solo dominio de broadcast para toda la red. La ventaja de una red plana es que proporciona baja latencia y alto rendimiento y es fácil de administrar. La desventaja es que aumenta la vulnerabilidad al tráfico de broadcast en todos los switches, puertos, enlaces de backbone y usuarios.

Las VLAN son un mecanismo efectivo para extender los firewalls desde los routers a la estructura de los switches y proteger la red contra problemas de broadcast potencialmente peligrosos. Además, las VLAN conservan todas las ventajas de rendimiento de la commutación.

El tráfico de broadcast dentro de una VLAN no se transmite fuera de la VLAN. Por el contrario, los puertos adyacentes no reciben ningún tráfico de broadcast generado desde otras VLAN.

Este tipo de configuración reduce sustancialmente el tráfico total de broadcast, libera el ancho de banda para el tráfico real de usuarios, y reduce la vulnerabilidad general de la red a las tormentas de broadcast.



Las VLAN establecen dominios de broadcast.



¿Estás listo para un desafío?

**1. Indique la opción correcta**

Una VLAN es una agrupación lógica de dispositivos de red o de usuarios que no se limita a un segmento de switch físico.

- Verdadero
- Falso

**2. Indique la opción correcta**

Las VLAN segmentan lógicamente la infraestructura física de las LAN.

- Verdadero
- Falso

**3. Indique la opción correcta**

Las VLAN no proporcionan un método para controlar los broadcast de red.

- Verdadero
- Falso

**4. Indique la opción correcta**

Las VLAN pueden aumentar la seguridad de la red.

- Verdadero
- Falso

**5. Indique la opción correcta**

Indicar cuál es el estándar propuesto por la IEEE para la configuración de Vlan.

- IEEE 802.3
- IEEE 802.11
- IEEE 802.1Q
- IEEE 802.5

**6. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Switch	brinda rutas de conexión entre VLANs diferentes.
VLAN	agrupa lógicamente los dispositivos y no se limita a un segmento físico de un switch.
Topologías virtuales	permite agrupar usuarios separados por grandes distancias físicas que abarcan toda la red.
Router	segmenta físicamente una LAN en dominios de colisión individuales.

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

Una VLAN es una agrupación lógica de dispositivos de red o de usuarios que no se limita a un segmento de switch físico.

- Verdadero
- Falso

## 2. Indique la opción correcta

Las VLAN segmentan lógicamente la infraestructura física de las LAN.

- Verdadero
- Falso

## 3. Indique la opción correcta

Las VLAN no proporcionan un método para controlar los broadcast de red.

- Verdadero
- Falso

## 4. Indique la opción correcta

Las VLAN pueden aumentar la seguridad de la red.

- Verdadero
- Falso

## 5. Indique la opción correcta

Indicar cuál es el estándar propuesto por la IEEE para la configuración de Vlan.

- IEEE 802.3
- IEEE 802.11
- IEEE 802.1Q
- IEEE 802.5

## 6. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Switch	segmenta físicamente una LAN en dominios de colisión individuales.
VLAN	agrupa lógicamente los dispositivos y no se limita a un segmento físico de un switch.
Topologías virtuales	permite agrupar usuarios separados por grandes distancias físicas que abarcan toda la red.
Router	brinda rutas de conexión entre VLANs diferentes.

## SP11 / Ejercicio resuelto

Partiendo de la situación de la empresa donde trabajamos (cuyo último crecimiento fue la adquisición de la sucursal planteada en la SP7) en la sucursal nos quedaron dos redes que totalizan 23 computadoras conectadas por medio de Hubs de 10 Mbps. donde la red se desempeña en forma más lenta. Además le consultan a Ud. si será necesario realizar alguna otra inversión para mejorar el desempeño de la red, ya que actualmente la sucursal totaliza 300 computadoras.

¿Qué dispositivos deberán instalarse para que la red funcione correctamente?

### Solución:

Una red implementada con Hubs constituye un único dominio de colisión, por lo cual, al incrementarse el número de estaciones o el tráfico, se aumenta el número de colisiones. Para evitar esto, la solución es:

Cambiar los Hubs por Switches de 100 Mbps (*Fast Ethernet*), verificar que las máquinas tengan NICs de 100 Mbps y en su defecto agregarlas, retirar los Hubs y en lo posible reemplazar las máquinas más viejas o reasignarlas para los lugares menos críticos de la empresa. Con el reemplazo de hubs por switches reducimos sustancialmente los dominios de colisión.

Como la empresa ya se dividió en subredes según lo visto en la SP8, ya existe instalado un Router que concentra las subredes con todos los beneficios que ello implica en cuanto a la reducción del tráfico de broadcasts

Para finalizar, presentamos a la empresa la propuesta de adquisición de un equipamiento para que desempeñe la función de Firewall y aconsejamos, ya que la empresa sostiene un alto intercambio de tráfico con Internet, la implementación de un complemento para incrementar la seguridad en la red: un sistema de detección de intrusos o IDS.

## SP11 / Ejercicio por resolver

Presente al Profesor por escrito la descripción de la situación de la red en la empresa donde Ud. trabaja. Exprese si se preve algún crecimiento en cuanto a cantidad de hosts o de tráfico para los próximos dos años. Analice si será necesario realizar alguna inversión para mejorar el desempeño de la red. ¿Qué dispositivos deberán instalarse para que la red funcione correctamente?

Tenga en cuenta lo aprendido en todas las SP anteriores y proponga la solución que, a su juicio, sea la mejor.

¿Cuál será la solución que propondrá?

Debate esto con el profesor y con los otros alumnos compañeros del curso

Sin dudas, después de haber incorporado todos los conocimientos vistos en este TID, Ud. está en condiciones de realizar la presentación de una buena propuesta de mejora de esta situación concreta.

La exposición al profesor y el debate que pueda originarse con sus compañeros de curso, hará que Ud. reciba una retroalimentación e integre sus conocimientos de forma sólida y además los pueda volcar a su vida profesional en forma inmediata con la seguridad de tener un respaldo fundamentado en la teoría y aplicado a la práctica.



¡Vamos a comprobar cuánto aprendiste!

**1. Indique la opción correcta**

La NIC (Network Interface Card) es la tarjeta que conecta cada dispositivo con los medios de red, tiene la dirección física o MAC y actúa en la Capa de Enlace de Datos del Modelo OSI.

- Verdadero
- Falso

**2. Indique la opción correcta**

El área donde se producen colisiones, se llama "Dominio de Colisión"

- Verdadero
- Falso

**3. Indique la opción correcta**

Los puentes o bridges filtran el tráfico, construyendo tablas con las direcciones MAC de todas las redes conectadas a él.

- Verdadero
- Falso

**4. Indique la opción correcta**

La NIC tiene la siguiente función:

- Brindar un punto de conexión para los medios de networking.
- Formar paquetes de datos y enviarlos a través de los medios y transformarlos en información que las estaciones puedan comprender.
- Implementar el acceso ordenado a los medios de red compartidos.
- Todas las anteriores.

**5. Indique la opción correcta**

El repetidor tiene la siguiente desventaja:

- No puede filtrar tráfico de red.

- Los bits que llegan a un puerto salen a todos los puertos (excepto por el puerto donde entraron).
- Los datos son transferidos a todos los segmentos de LAN (independientemente de si es necesario que deban llegar allí o no).
- Todas las anteriores.

**6. Indique la opción correcta**

Los Switches y Bridges tienen la siguiente característica:

- Actúan en la Capa de Enlace del Modelo OSI.
- Filtran datos según la dirección MAC de destino.
- Pasan tramas entre segmentos redes que operan bajo protocolos diferentes.
- Todas las anteriores.

**7. Indique la opción correcta**

Los Switches y Bridges tienen la siguiente ventaja:

- Operan en la Capa de Enlace de Datos (capa 2 del Modelo OSI).
- Eliminan el tráfico innecesario.
- Minimizan las colisiones, dividiendo las redes en segmentos y filtrando el tráfico en base a la dirección MAC.
- Todas las anteriores.

**8. Ordene relaciones**

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Switch	agrupa lógicamente dispositivos de red o de usuarios y no se limita a un segmento de switch físico.
Router	resuelve el problema del excesivo tráfico de broadcast, ya que no envían tramas a menos que se les indique.
VLAN	puede aprender la dirección de cada dispositivo de la red leyendo la dirección origen de cada trama transmitida y anotando el puerto donde la trama se introdujo en el switch.

# Respuestas de la Autoevaluación

## 1. Indique la opción correcta

La NIC (Network Interface Card) es la tarjeta que conecta cada dispositivo con los medios de red, tiene la dirección física o MAC y actúa en la Capa de Enlace de Datos del Modelo OSI.

- Verdadero
- Falso

## 2. Indique la opción correcta

El área donde se producen colisiones, se llama "Dominio de Colisión"

- Verdadero
- Falso

## 3. Indique la opción correcta

Los puentes o bridges filtran el tráfico, construyendo tablas con las direcciones MAC de todas las redes conectadas a él.

- Verdadero
- Falso

## 4. Indique la opción correcta

La NIC tiene la siguiente función:

- Brindar un punto de conexión para los medios de networking.
- Formar paquetes de datos y enviarlos a través de los medios y transformarlos en información que las estaciones puedan comprender.
- Implementar el acceso ordenado a los medios de red compartidos.
- Todas las anteriores.

## 5. Indique la opción correcta

El repetidor tiene la siguiente desventaja:

- No puede filtrar tráfico de red.
- Los bits que llegan a un puerto salen a todos los puertos (excepto por el puerto donde entraron).
- Los datos son transferidos a todos los segmentos de LAN (independientemente de si es necesario que deban llegar allí o no).
- Todas las anteriores.

## 6. Indique la opción correcta

Los Switches y Bridges tienen la siguiente característica:

- Actúan en la Capa de Enlace del Modelo OSI.
- Filtran datos según la dirección MAC de destino.
- Pasan tramas entre segmentos redes que operan bajo protocolos diferentes.
- Todas las anteriores.

## 7. Indique la opción correcta

Los Switches y Bridges tienen la siguiente ventaja:

- Operan en la Capa de Enlace de Datos (capa 2 del Modelo OSI).
- Eliminan el tráfico innecesario.
- Minimizan las colisiones, dividiendo las redes en segmentos y filtrando el tráfico en base a la dirección MAC.
- X Todas las anteriores.

#### 8. Ordene relaciones

Relacione los conceptos de la columna izquierda con sus características correspondientes en la columna derecha:

Switch	puede aprender la dirección de cada dispositivo de la red leyendo la dirección origen de cada trama transmitida y anotando el puerto donde la trama se introdujo en el switch.
Router	resuelve el problema del excesivo tráfico de broadcast, ya que no envían tramas a menos que se les indique.
VLAN	agrupa lógicamente dispositivos de red o de usuarios y no se limita a un segmento de switch físico.

## Cierre

Estimado lector, hemos llegado al final de este Texto Interactivo Digital. Espero que le haya sido de utilidad, no sólo para incorporar conocimientos teóricos sino también prácticos.

Quisiera agradecer especialmente a los profesores Norberto Cura y Ricardo Piña, quienes redactaron las versiones anteriores de este libro y cuyos contenidos esenciales se mantienen, pero que ineludiblemente debieron ser actualizados para ponerlos en manos de usted, alumno del tercer milenio, con todo lo que ello implica.

Si bien las redes como tales han existido desde tiempos muy lejanos (como por ejemplo los caminos), actualmente las redes de computadoras potencian la capacidad de las organizaciones para la correcta toma de decisiones. Hoy más que nunca, la información es un elemento decisivo para el éxito o el fracaso de las empresas.

Hemos visto en este TID los conceptos principales que nos permitirán administrar con eficiencia las redes de telecomunicaciones para lograr obtener, procesar y presentar información a los distintos niveles de una empresa. Hemos estudiado en detalle cómo es el proceso de la digitalización de todas las señales, las tecnologías de las redes y de las comunicaciones y los conceptos fundamentales para entender cómo son y cómo funcionan las distintas redes de datos que se emplean para la interconexión de computadoras y otros dispositivos; los servicios que se pueden utilizar a través de las redes y las técnicas que se utilizan para transmitir y acceder a la información. Comprender y usar correctamente estas herramientas le permitirán, sin duda, obtener una ventaja competitiva en su desarrollo profesional.

Hoy en día, asistimos a una etapa muy importante en la transformación de las redes. El hombre cada vez más necesita estar comunicado y, por ello, dichas redes crecen a un ritmo cada vez mayor. Esta tendencia se acentuará cada vez más, pues el avance en las áreas de informática, electrónica y telecomunicaciones hará que las redes sean más rápidas, eficientes, económicas y seguras.

Los nuevos enfoques de comunicaciones y redes, donde están involucrados tanto proveedores de hardware como de software y dispositivos de comunicación, producen sistemas cada vez más sencillos de utilizar. Los estándares hacen más fácil la interconectividad de distintos dispositivos. Diariamente los costos se reducen en forma asombrosa, y día a día disponemos de mayores velocidades de transmisión.

Somos testigos diariamente de transformaciones que facilitan el entendimiento de personas que viven en distintos países y hablan diferentes idiomas, y esto se realiza con pocas dificultades.

Todas estas mejoras tecnológicas predicen que las redes producirán hasta profundos cambios sociales en la manera en que nos relacionamos en lo laboral, en la educación, en la forma de hacer negocios, etc. Sin duda, estamos viviendo esos cambios y debemos estar preparados para convivir con esas reglas de juego.

También sabemos, que una vez que la tecnología se introduce en nuestra vida, no se vuelve atrás; por ello debemos estar preparados para que desde nuestra capacidad, de nuestra ética y nuestra hombría de bien utilicemos esta tecnología en pos de una sociedad cada día más justa y solidaria.

Esta obra, sin dudas, prepara a los que la consultan para enfrentar con éxito los retos que pronto les plantearán los nuevos desafíos tecnológicos. La misma es, en sí misma, una puerta que abre el camino de las redes. Si bien la misma fue redactada para ser utilizada como texto de estudio de la asignatura Redes y Comunicación, espero también que pueda ser utilizada como texto de consulta para administrar con eficiencia tanto las redes actuales como futuras.

Once situaciones profesionales han servido de guía para la comprensión acabada del funcionamiento de las

redes y nos han llevado a completar la idea del funcionamiento de los distintos tipos de redes; desde la relación matemática que nos permite medirlas y cuantificarlas, hasta el diseño completo de una red de gran envergadura.

Espero, ciertamente, que el presente TID les haya ayudado a prepararse para su desempeño profesional y que, a través de él, hayan encontrado las respuestas para administrar con eficiencia el maravilloso mundo de las redes. De aquí en más serán ustedes los que decidan seguir transitando este camino a través de la propia investigación. Le adelanto que este camino no tendrá fin, y quien conozca la forma de recorrerlo tarde o temprano ocupará un lugar muy valorado dentro de esta sociedad cada vez más comunicada.

*El autor*

# Bibliografía

- BLACK, Ulises. "Redes de computadoras. Protocolos normas e interfaces". Edit. Macrobit.
- CURA, Norberto J. "Comunicaciones de datos y redes de información" - TOMOS I y II. Edit. Universitas.
- DUCK, M; BISHOP, P; REED, R. "Data communicatios for engineers".
- HALSALL, Fred. "Comunicación de datos, redes de computadores y sistemas abiertos". Edit. Addison-Wesley Iberoamericana.
- MC. QUERRY, Steve. "Internetworking device cisco". Edit. Ciscopress.
- NOLL, Pierce. "Señales. La ciencia de las telecomunicaciones". Edit. Reverté.
- SPURGEON, E. Charles. "Ethernet - the definitive guide". Edit. O'Reilly
- STALLING, William. "Comunicaciones y redes de computadoras". Edit. Prentice Hall.
- STREMBLER, G. "Introducción a los sistemas de comunicación". Edit. Addison-Wesley Iberoamericana.
- Manuales de equipos e instalación de dispositivos de red".
- "Manual de fibra óptica de Siemens"
- "Revistas especializadas".

## Bibliografia Ampliatoria

BEHROUZ A. Forouzan, Transmisión de datos y redes de comunicaciones. Editorial Mc Graw Hill - 4ta Edición. ISBN: 9788448156176.

COMER, Douglas, Redes globales de información con internet y TCP/IP, principios básicos, protocolos y arquitectura". Editorial Prentice Hall Hispanoamericana. 1996.

GARAYZÀBAL, Diego, Redes y comunicaciones. Texto Multimedial. Editorial IES Siglo 21. 2003 .

HEYWOOD, Andrew, Redes Microsoft con TCP /IP. Ed. Prentice Hall 1999.

STALLING William. Comunicaciones y redes de computadoras. Editorial Prentice Hall. 7 edición - ISBN 978-84-205-4110-5.

TANENBAUM, Adrew, Redes de Computadoras. Editorial Prentice Hall Hispanoamerica. 1999.