Luis Orlando Lázaro Medrano

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

ESPECIALIDAD FORMATIVA

Operación en sistemas de comunicaciones de voz y datos

IFCM0110

Luis Orlando Lázaro Medrano

UF1347: Instalación y configuración de los nodos de interconexión de redes privadas con públicas

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en la plataforma denominada Portal del Alumno, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Luis Orlando Lázaro Medrano

* Bibliografía usada en este documento:
UF1347: Instalación y configuración de los nodos de interconexión de redes privadas con públicas, Autor: Pedro Mora Pérez, EDITORIAL ELEARNING S.L. Edición: 6.1
Capturas de pantalla y textos electrónicos de varias webs únicamente para ilustrar la actividad educativa

Luis Orlando Lázaro Medrano

Contenido

1. Procedimientos de gestión en el subsistema de conmutación telefónica 1

1.1. Procedimientos de prueba y verificación del subsistema de conmutación telefónica 1

Conmutación telefónica. Equipos de conmutación automática 1

Presentación de pruebas 1

Procedimientos de funciones para la identificación, prueba y verificación de incidencias – averías del subsistema de conmutación telefónica 2

1.2. Procedimientos y herramientas de diagnóstico y gestión de averías e incidencias 2

Operación y mantenimiento en centrales telefónicas 2

Tipos de mantenimiento 3

Tipología de averías 4

1.3. Procedimientos de diagnóstico y gestión de averías e incidencias 7

1.3.1. Función AlarmSurveillance: Conceptos y elementos relacionados 14

1.3.2. Análisis y diagnóstico de información de alarma 15

1.3.3. Documentación y seguimiento de incidencias: procedimientos y herramientas de troubleticketing 16

1.3.4. Casos prácticos y ejemplos 20

2. Interconexión de redes 22

2.1. Conceptos básicos sobre redes públicas 22

Definición de conceptos de red 22

Adaptación de las necesidades de empresa a un modelo jerárquico 22

2.2. Servicios de interconexión con la red pública 25

Principios de la interconexión entre redes 25

Servicios de interconexión con redes públicas 26

ATM 30

RDSI 31

Redes de área local (LAN): 32

2.2.1. Parámetros: alimentación eléctrica, sujeción mecánica, otros 33

2.2.2. Requerimientos de interconexión. Normativa de calidad 38

2.2.3. Interfaces en función de la tipología de red 39

2.2.4. Normativas de seguridad 39

2.3. Arquitectura de un dispositivo de interconexión de redes 40

2.3.1. Interfaces 41

2.3.2. Módulos 46

2.3.3. Cables 49

2.4. Conceptos de encaminamiento 54

2.4.1. Segmentación de redes 56

2.4.2 Algoritmos de encaminamiento 59

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Luis Orlando Lázaro Medrano

3. Dispositivos de interconexión de redes 62
3.1. Interfaces más habituales de interconexión de redes 62
3.1.1. Interconexión de área local (RAL-RAL) 62
3.1.2. Interconexión de área extensa (RAL-MAN o RAL-WAN) 64
3.2. Características de los servicios de interconexión de redes 68
3.3. Tecnologías empleadas 73
Introducción tecnología xDSL 73
Introducción tecnología ATM 75
Introducción a la tecnología de FRAME RELAY 76
Introducción a la tecnología MPLS 77
Introducción a la tecnología X.25 77
Introducción a la tecnología RDSI 78
3.4. Identificación de los servicios de conexión 79
3.4.1. Interrelación de los servicios 82
3.4.2. Implementación en los equipos de la red local 83
3.5. Los proveedores de servicios de comunicaciones 86
3.5.1. Servicios de interconexión 87
3.5.2. Perfiles de los servicios 87
4. Protocolos de interconexión de redes 89
4.1. Protocolos utilizados en la interconexión redes privadas y públicas 89
4.1.1. Clasificación según sus funciones 102
4.1.2. Servicios soportados 104
4.1.3. Pila de protocolos TCP/IP 108
4.2. Cifrado. Redes privadas virtuales 120
4.2.1 Descripción 121
4.2.2. Usos 124
4.2.3. Tipos 125
4.2.4. Implementaciones 128
4.2.5. Parámetros de configuración y gestión de interconexión de redes privadas virtuales 129
4.3. Mecanismos de seguridad 130
4.3.1. Enmascaramiento y redirección 131
4.3.2. Filtrado de paquetes 132
5. Procedimientos de instalac. y prueba de dispositivos de interconexión de redes 137
5.1. Normativas de seguridad física y eléctrica aplicables a los dispositivos de interconexión de redes 137
5.1.1. Lista de las principales normas 140
5.1.2. Características destacadas de cada una 141
5.2. Procedimientos de carga de configuración en dispositivos de interconexión de redes 146
5.2.1. Carga mediante ficheros 153
5.2.2. Modificación de parámetros 158

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Luis Orlando Lázaro Medrano
Luis Orlando Lázaro Medrano
Luis Orlando Lázaro Medrano
Luis Orlando Lázaro Medrano

5.2.3. Actualización de firmware 160
5.2.4. Conexiones locales y remotas para configuración..... 161
5.3. Procedimientos de verificación de los servicios de comunicación..... 161

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Luis Orlando Lázaro Medrano
Luis Orlando Lázaro Medrano
Luis Orlando Lázaro Medrano
Luis Orlando Lázaro Medrano

1. Procedimientos de gestión en el subsistema de conmutación telefónica

1.1. Procedimientos de prueba y verificación del subsistema de conmutación telefónica

Conmutación telefónica. Equipos de conmutación automática

Las centrales telefónicas o centrales de conmutación son las encargadas de proporcionar las funciones para poder realizar una llamada, de las cuales, las más importante es la de "conexión" o "conmutación" de los abonados llamante y llamado.

Abonados y enlaces

Al equipo de conmutación de una central telefónica se conectan: Abonados y Circuitos de unión con otras centrales telefónicas (enlaces). Por un enlace concreto y en un instante determinado, solamente puede cursarse una comunicación.

Los enlaces que pueden establecer comunicaciones en ambas direcciones se denominan enlaces bidireccionales.

Un enlace bidireccional puede establecer comunicaciones en direcciones contrarias, pero nunca simultáneamente.

Los enlaces que están especializados en cursar comunicaciones que se establecen en una determinada dirección, y sólo en esa, se denominan enlaces unidireccionales.

Tipos de llamadas

Los distintos tipos de llamadas que pueden existir son los siguientes:

- Si un abonado de la central llama a un abonado que también es de la central, el equipo ha de efectuar la conexión de ambos abonados. Esta llamada se denomina "**llamada local**".
- Si un abonado de la central, llama a un abonado que no es de la central, el equipo de conmutación ha de efectuar la conexión entre dichos abonados y uno cualquiera de los enlaces de salida libres que encaminan la llamada hacia la central donde se conecta el abonado llamado, ya sea directamente, ya sea a través de otras centrales intermedias. Esta llamada se denomina "llamada **saliente**".
- En el caso de la llamada de un abonado no perteneciente a la central, llama a un abonado de la central, el equipo de conmutación efectúa la conexión entre el enlace de llegada por el que se presenta la llamada en la central y el abonado llamado. A este proceso se le denomina "llamada **entrante**".
- Una llamada entre dos abonados, que no pertenecen a la central, pero que hace tránsito en la central. La llamada se presenta por un enlace de llegada y la misión del equipo de conmutación es efectuar la conexión entre dicho enlace de llegada y uno cualquiera de los enlaces de salida libres que encaminen la llamada hacia la central donde se conecta el abonado llamado. Esta llamada se denomina "**llamada de tránsito**"

Presentación de pruebas

En la presentación de pruebas, se determina que como mínimo, se debe de incluir una serie de pruebas y sus resultados, las cuales son:

- Capacidades y funcionalidades específicas.
- Estabilidad de los componentes y funciones, en un entorno operativo.
- Revisión del inventario de Hardware y Software.
- Pruebas necesarias para verificar el correcto funcionamiento del sistema.
- Pruebas unitarias de cada componente del sistema.
- Pruebas integrales de todos los componentes interno del sistema.
- Prueba de integración, cuyo objetivo es la adecuada integración externa del sistema con el resto de elementos de la infraestructura.
- Pruebas de restauración transaccional, donde su objetivo es verificar la capacidad de recuperación del sistema y restaurar su funcionamiento normal, después de eventos de errores, como por ejemplo caídas de luz.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

- ⇨ Pruebas de disponibilidad, cuyo objetivo es asegurar la plena disponibilidad de todos los servicios del sistema, a usar por los usuarios u otras partes del sistema.
- ⇨ Pruebas de seguridad, cuyo objetivo es asegurar que no existen caminos alternativos que eludan los mecanismos de seguridad implementados en el sistema, y que todos los abonados estén debidamente vinculados a los sistemas de seguridad implementados o bajo las políticas de seguridad establecidas.

Procedimientos de funciones para la identificación, prueba y verificación de incidencias – averías del subsistema de conmutación telefónica

Función de aseguramiento de circuito automático

Esta función, sirve para identificar troncales defectuosas. Cuando dicha función está activada, y se detecta un uso inusual del enlace troncal, la función notifica con una llamada de referencia al problema, por ejemplo realizando llamadas muy cortas o muy largas. Esta llamada de referencia, llega a través de un sistema que emplea el uso de una llamada inactiva. En el momento que la llamada se responde, existen varios estados que serán mostrados en pantalla:
a) Identifica la llamada como una llamada de Aseguramiento de Circuito Automático.
b) Muestra el código de acceso a grupo de troncales.
c) El número de miembro del grupo de troncales.
d) El motivo de la llamada (indica el tiempo de retención corto o largo).

Función de Verificación de Línea Ocupada

Esta función, tiene el objetivo de probar y verificar la condición de ocupados de troncales, teléfonos o grupos de búsqueda, mediante la realización de una llamada. Esta función, nos permite verificar si el troncal está ocupado debido a la intensidad de su uso, o bien existe un problema en los troncales, teléfonos o grupos de búsqueda.

Función de indicación de Sistema Ocupado

- ⇨ Con esta función, podemos visualizar el estado de teléfonos, troncales o zonas de localización como inactivas u ocupadas.
- ⇨ Este sistema se puede configurar mediante unos mecanismos que asocian dicha función a un mecanismo concreto, cuya misión es la de monitorear el sistema que se desee.

Función de llamadas de prueba de sistema

- ⇨ Esta función se utiliza para realizar llamadas de pruebas a troncales o teléfonos determinados.
- ⇨ Esta función es muy útil para encontrar líneas ruidosas u con otros problemas, ya que esta función funciona fuera del tráfico normal del sistema.
- ⇨ En contraposición con las ventajas de esta función, es que los usuarios externos del sistema, pueden hacer un uso abusivo de ella fácilmente.

Una de las recomendaciones para evitar violaciones de seguridad, es desactivar el código de acceso a esta función en cuanto no se necesite más para realizar las pruebas.

Función de Identificación de Troncal

Esta función, identifica una troncal defectuosa o ruidosa.

1.2. Procedimientos y herramientas de diagnóstico y gestión de averías e incidencias

Operación y mantenimiento en centrales telefónicas

En los procedimientos de operación y mantenimiento en centrales telefónicas, así como en la gestión de averías e incidencias, se deben definir cuáles son los procesos idóneos a llevar a cabo para el diagnóstico y gestión de las averías de los equipos, ya sea a nivel de software o a nivel de bloque de hardware.
Por otro lado, también se debe de diferenciar cuáles son las funciones principales y primordiales en los procedimientos operativos de las averías e incidencias, así como las funciones principales y primordiales en su gestión. Junto a los procesos diferenciadores que hemos mencionado, la definición de una estrategia de control de dichos procesos, resulta esencial, para la correcta actuación, gestión de las averías e incidencias de los equipos involucrados.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Los procedimientos y tratamientos de averías e incidencias, se realizan directamente en las funciones de operación, ya que son los procesos intervinientes en un subsistema de conmutación telefónica, que dan lugar a la creación de un nuevo abonado, el cambio de la categoría perteneciente a dicho abonado en la red telefónica, la definición de la ruta del servicio, etc.
Estos procesos, poseen sus propias funciones de operación, que como se ha indicado anteriormente, poseen sus propios procedimientos y tratamientos de averías e incidencias, los cuáles su principal ámbito de actuación son:

- ⇨ Administración de líneas de abonado.
- ⇨ Asignación de números telefónicos.
- ⇨ Estudio de líneas.
- ⇨ Trazo de llamadas.
- ⇨ Medida de tráfico.
- ⇨ Monitorio de tráfico.
- ⇨ Manejo de archivos.

En la operativa y en el proceso de mantenimiento de una central telefónica, existen 2 tipos de mantenimientos bien diferenciados, que se llevan a cabo, antes de que entren en funcionamiento los procedimientos y tratamientos de averías e incidencias, minimizando la acción o acciones de estos últimos, gracias a los tipos de mantenimiento llevados a cabo durante la operativa del servicio del subsistema de conmutación telefónica.

Tipos de mantenimiento

Mantenimiento preventivo

Se basa en el control de los dispositivos de la operación o bien se realiza el control a determinados bloques de software del subsistema de conmutación telefónica, con una determinada frecuencia, con ciertos dispositivos o bloques de software, y realizándose inspecciones en cada visita.

Mantenimiento correctivo

En esta fase, entraría de pleno los procedimientos y tratamientos de averías e incidencias, ya que aquí se determinan cuáles serían los idóneos, cada vez que se activa una alarma de operación.
Sus características son:

- ⇨ No poseen una determinada frecuencia.
- ⇨ Las rutinas de inspección se realizan cada vez que sucede un fallo del subsistema de conmutación telefónica.

Diagnóstico de averías en sistemas de telefonía básica

En el diagnóstico de averías en sistemas de telefonía, seguimos una serie de procesos, entre los cuáles destacamos:

a) Análisis del funcionamiento de equipos o sistemas.
   En este apartado, formarían parte por ejemplo, los bloques, flujos de información, señales, medidas, etc. En el análisis del funcionamiento de equipos o sistemas, partimos de las averías de forma general, a los problemas más específicos, situándonos en la perspectiva externa del conocimiento del usuario, como pueden ser los servicios utilizados, condiciones de funcionamiento, flujo de información, etc.

b) Análisis de disfunciones.
   En este apartado, se analiza cuestiones como por ejemplo:
   - ⇨ Los motivos que han provocado la avería.
   - ⇨ Bloques afectados.
   - ⇨ El resultado de los efectos que producirá en los equipos o sistemas.
   - ⇨ Síntomas que se producirán en los equipos o sistemas.
   - ⇨ Medidas y pruebas para determinar el equipo o elemento afectado.

   En el análisis de disfunciones, entendido este análisis como efectos producidos por un funcionamiento anómalo del equipo, como por ejemplo, entre un hilo de la extensión 3 y otro hilo de la extensión 4, donde existe resistencia en el repartidor.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

- ⇨ Indicar las causas para que se pudiese producir la avería (por ejemplo “Humedad en el repartidor que ha hecho que se sulfaten los contactos y se cree una resistencia entre los mismos”)
- ⇨ Bloques afectados (por ejemplo “Instalación y terminales”)
- ⇨ Qué efecto producirá en el equipo o sistema
  (Por ejemplo “habrá un trasvase de corriente entre la extensión seis y siete provocando que las variaciones de corriente de una aparezcan en la otra, existirá diafonía entre las ext 3 y 4”).
- ⇨ Síntomas que se presentará el equipo o sistema.
  Por ejemplo “Se escucharán las conversaciones de la extensión seis en la extensión siete y viceversa”).
- ⇨ Forma de delimitar el equipo o elemento afectado
  (Medidas y pruebas por ejemplo “desconectar la central y terminales de estas extensiones y verificar con ayuda del polímetro la resistencia entre hilos de las dos extensiones”).

c) Diagnóstico y reparación.
En este apartado, utilizamos la información de avería proveniente del usuario y los efectos derivados de la avería. Junto a esto, poner en marcha el plan de localización y reparación de averías.

- ⇨ Partir de los síntomas de un hipotético cliente
  (Por ejemplo “Se escuchan las conversaciones de la extensión 3 en la extensión 4 y viceversa”)
- ⇨ Realizar la/s hipótesis del bloque y/o elementos afectados
  (Por ejemplo “Instalación y terminales”)
- ⇨ Realizar un plan de intervención a forma de árbol de averías para delimitar el equipo o elemento afectado
  (Medidas, pruebas y toma de decisión en función de los datos obtenidos, por ejemplo “desconectar la central y terminales de estas extensiones y verificar con ayuda del polímetro la resistencia entre hilos de las dos extensiones, si la medida es infinita el problema está en la central o en el repartidor de su placa…”).
- ⇨ Una vez localizada la avería es necesario que el alumno se interrogue si esta podría haber sido producida por otro elemento, una incorrecta manipulación o actuaciones de terceros (obras, roturas de cañerías, goteras…) para evitar que se repita o delimitar responsabilidades.

Tipología de averías

Terminales

Su detección es bastante sencilla, siempre y cuando haya otro terminal de similares características, u otra extensión con un terminal similar. En el caso, de que no se disponga de un terminal similar de ninguna forma, solo queda descartar la instalación de la línea, como fuente del problema o avería y verificar la continuidad hasta el terminal, en los casos en los que el terminal fuera de tipología específica. Si el terminal es de tipología clásica, estas verificaciones, se harían con el equipo multiprueba.
En el hipotético caso de que existan 2 o más terminales, se probarían cada uno de ellos de forma independiente, y si las pruebas son correctas, se procedería igualmente a realizar las comprobaciones oportunas con el equipo multiprueba en cada uno de ellos, por si las características de cada terminal, hubieran cambiado por alguna razón.

Instalación

En este tipo de averías, y según la longitud de las instalaciones > 500 metros, se comprueba la continuidad y aislamiento de la misma, salvo en las instalaciones de >500 metros, resulta necesario comprobar la capacidad de la misma.

- Interrupción del bucle:
  Este tipo de averías, consiste en el corte de un hilo o incluso de los 2, que pueden darse por ejemplo en rosetas, conectores y/o repartidores.
- Resistencia del bucle:
  Este tipo de averías, se producen por una excesiva resistencia del bucle por falsos contactos, en las rosetas, conectores y/o repartidores, o bien por un excesivo estiramiento del cable debido a la utilización de cableado no adecuado.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España

- Pérdida de aislamiento
  Este tipo de averías se produce por ruido entre pares (diafonía) o entre los hilos del mismo par (descolgado), generalmente provocada por la humedad en los contactos de las rosetas – repartidor, o bien en el propio cable debido a la rotura de la funda protectora del cableado, quedando expuesto a la intemperie.
  Este tipo de averías, cuando es producida por la rotura de la funda protectora de aislamiento, los cables que están a la intemperie, cuando entran en contacto con la humedad, los contactos se sulfatan y el óxido producido actúa como resistencia.

Central y líneas de enlace

En términos generales, para solventar averías en la central, se recurre a un reseteo, sin carga de parámetros por defecto de la central, separando en cualquier caso, la central de la instalación, en el caso de que el reseteo en caliente, no fuese realmente efectivo.
En las líneas de enlace, para lograr el diagnóstico y detección de la avería, en primer lugar se separan de la central, y se comprueba en el PTR o PAU, mediante un terminal o dispositivo multiprueba.
Existen diversos tipos de averías de enlace, como son:

- Bucle abierto: Se detecta con un terminal normal.
- Resistencia de línea: Como efecto produce un bajo nivel de tensión y la corriente de llamada es insuficiente para ser detectado por la central. Se comprueba con el equipo multiprueba o poniendo en corto con el amperímetro (debe dar una corriente superior a 20 mA), para comprobar la corriente de llamada se comprueba con un teléfono con un condensador (no polarizado o dos electrolíticos en serie + con +) en paralelo para simular tres terminales.
- Falta de aislamiento: Debido generalmente a repartidores abiertos o empalmes cuya protección se ha roto; dan lugar a “cruces” y también en algunos casos a resistencia de línea.

Herramientas de diagnóstico

El polímetro

El polímetro, es un aparato de medida de continuidad multifuncional, con el que en un dispositivo, contienes varios equipos, como por ejemplo, un voltímetro, amperímetro y óhmetro. Este dispositivo, realiza medidas de diferentes magnitudes, por ello, tiene múltiples funciones o dicho de otro modo, múltiples dispositivos en uno solo.
Con este dispositivo, se puede realizar 3 tipos de medidas:

- Intensidades.
- Tensiones.
- Resistencias.

Tanto de corriente alterna como continua.
El polímetro, aparte de los 3 tipos básicos de medidas, están dotados igualmente de otras capacidades de medición como pueden ser, la medida de continuidad (resistencia cero, y están dotados de un zumbador), medida de capacidades de condensadores y medida de semiconductores (diodos y transistores). El multímetro, polímetro, tester o multitester resulta una herramienta indispensable para todo electricista o apasionado de la electrónica.
Existen a la venta numerosos tipos de polímetros o multímetros.
Existen aparatos de medida digitales e incluso analógicos. Estos últimos indican los valores medidos con la ayuda de una aguja. A penas existen diferencias de precios entre los multímetros digitales y los analógicos por lo que recomendamos adquirir uno digital ya que no existirán errores de lectura. Para un multímetro apto para bricolaje y reparaciones en casa los valores máximos de medición son:

- Corriente contínua (CC): 0-300 voltios.
- Corriente alterna (CA): 0-300 voltios.
- Corriente contínua: 0-10 amperios.
- Resistencia: 0-2 mega ohmios.

Existen multímetros más avanzados en el mercado que incluyen más funciones como por ejemplo: medida de la capacidad de un condensador, medida de autoinducción, frecuencia, temperatura, etc.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Los multímetros se venden con dos cables con punta de pruebas, uno negro y el otro rojo. Los multímetros más altos de gama son más precisos que los baratos, aunque una diferencia de un mili voltio no será importante para realizar trabajos de bricolaje y reparaciones domésticas.

a) Regulación del multímetro y su empleo para realizar medidas
   - Generalmente se deberá conectar el cable rojo al borne VΩmA del multímetro y el cable negro al borne COM.
   - Para realizar la lectura de la intensidad de corriente debéis colocar el selector sobre la escala mayor pero en este caso en la posición DCA o A…
   - Para el caso de la medición de la corriente se emplea la misma posición tanto en corriente contínua como en corriente alterna.
   - Si deseáis medir corrientes elevadas (hasta 10A en nuestro ejemplo), es conveniente conectar el cable rojo al borne 10A MAX (en nuestro ejemplo).
   - Para medidas de hasta 200 mA según el tester de este ejemplo podremos tener el cable rojo en el borne VΩmA.
   - Debemos destacar también que para corrientes grandes del orden de los amperios, se suele establecer además de la corriente máxima, el tiempo máximo que puede estar aplicada dicha corriente al amperímetro.
   - Para este ejemplo aparece escrito en el polímetro 10A MAX, MAX 10 sec, each 15 min.
   - Se puede medir 10A manteniendo la lectura un máximo de 10 segundos y a intervalos de 15 minutos.

b) Medida de la resistencia
   - La medida de la resistencia puede ayudarnos a verificar el estado del cableado o de detectar la presencia de un cortocircuito.
   - Antes de realizar lecturas de la resistencia debemos cortar todo suministro eléctrico.
   - Posicionamos el selector sobre la posición Ω en la escala más grande, el tester estará situado en paralelo.
   - Reduciremos la escala para obtener un resultado más preciso.
   - Si obtenemos una lectura de 1 quiere decir que la resistencia es enorme o que el circuito está abierto.
   - Si obtenemos un valor de 0 indica que la resistencia es ínfima o que existe un cortocircuito.
   - La medida de la resistencia también resulta práctica para comprobar un fusible, aplicando lo anterior o también para comprobar las diferentes conexiones de un disyuntor.
   - Existen multímetros que tienen una posición en la que pintan cuando existe (cortocircuito) entre las puntas de prueba.

c) Mantenimiento del multímetro
   - De tiempo en tiempo será necesario abrirlo para sustituir un fusible quemado o para cambiar la pila de alimentación que suele ser de 9 voltios.
   - El polímetro, está compuesto de 2 cables con puntas metálicas, con unos mangos de plástico, como medida de protección ante posibles descargas eléctricas.
   - Una de las clavijas, de color negro, va conectado a un conector de color negro y con la palabra COM, y la otra clavija es roja, y se conecta al terminal con el que se va a realizar la medición, y se conectará según las instrucciones del terminal y al tipo de medición a realizar.

Generador de tono y localizador de tono

Los generadores de tono y los localizadores de tono son pequeños dispositivos manuales utilizados para identificar los pares de hilos.

Al utilizar el método de "zorro y sabueso", los hilos se pueden identificar y rastrear. Para identificar el cable, se coloca un generador de tono en uno de los extremos del par trenzado. En el otro extremo, cerca del cable, se coloca un amplificador para recibir y amplificar la señal audible. Mediante esta técnica se puede identificar el hilo de interés entre los diversos cables existentes.

El Receptor de Tonos/Detector de Traza Modelo TR02 es un instrumento de mano de reducidas dimensiones que, mediante la identificación de los tonos emitidos por un cable, permite seguir su recorrido

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

o traza sin cortar el recubrimiento aislante. Consta de un amplificador y un parlante con un robusto cono de mylar de gran resistencia a la humedad.
Se utiliza con los instrumentos Modelos CA7024, CA7026 o CA7028 funcionando en modo Transmisor de Tonos, conformando así un método muy rápido y eficiente para determinar el recorrido de un conductor o su localización. El equipo se enciende y activa como receptor oprimiendo un botón. Mediante un control se puede ajustar el volumen del parlante al nivel deseado. También posee un conector de audio para enchufar un auricular común que inhibe el funcionamiento del parlante. De esta forma el operador obtiene una señal clara y puede trabajar en una oficina sin molestar al personal de la misma.

- ⇨ Características
  - Determinar la traza de los cables.
  - Detectar roturas en los cables.
  - Encontrar cables ocultos en paredes, tuberías y paneles.

1.3. Procedimientos de diagnóstico y gestión de averías e incidencias

A continuación, se hace un repaso de algunos aspectos relacionados con la operativa que se sigue en el tratamiento de tickets o actividades en la identificación y descripción de las diferentes actividades en el tratamiento de las incidencias.
Como premisa de actuación en el proceso de identificación y descripción de las actividades, todos los técnicos asignados al área deberán entrar en el sistema, identificar las incidencias y describir las actividades del proceso, para su tratamiento completo, dentro de su ciclo de vida en el sistema de gestión de incidencias.

- ⇨ Periódicamente se hará un seguimiento para comprobar si se han realizado las modificaciones solicitadas y en caso de que no se hayan hecho se volverán a reclamar.
- ⇨ Cuanto antes se identifique y detecte una incidencia, menor será su impacto en la infraestructura subyacente y en definitiva para el conjunto de la red telemáticas que sustenta el negocio de la organización.
- ⇨ La crucial importancia, de monitorizar constantemente los recursos, para detectar de manera temprana al ser posible, potenciales incidencias, es para normalizar el servicio cuanto antes, para minimizar el impacto negativo que causaría si se mantuviera el evento o suceso en cuestión durante un mayor tiempo de prolongación.
- ⇨ De todas formas, en el caso de que no resulte posible reducir a nulo el impacto de la incidencia, habría que reducir su impacto al mínimo posible.
- ⇨ De todas formas, en el caso de que no resulte posible reducir a nulo el impacto de la incidencia, habría que reducir su impacto al mínimo posible.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

El paso siguiente es analizar toda la información disponible para identificar las causas y factores contribuyentes asociados al incidente.

- ⇨ Causa
  - Produjo el evento adverso.
  - Su ausencia prevendrá o reducirá este incidente en circunstancias parecidas en el futuro.
- ⇨ Factor contribuyente
  - No hubieran impedido el incidente pero contribuyen (tierra abonada).
  - Su ausencia mejora la seguridad del sistema.
- ⇨ Las herramientas más utilizadas para identificar las causas y los factores contribuyentes son:
  - Diagrama de Ishikawa.
  - Análisis Causa-Raíz: preguntas "por qué" en cascada.
  - Análisis de barreras, cambios, procesos.

Todas las incidencias del servicio deben ser registradas y cada incidencia debe registrarse de forma independiente.

La información a registrar generalmente incluye:

- ⇨ Identificador único.
- ⇨ Categorización.
- ⇨ Urgencia, impacto y prioridad.
- ⇨ Fecha y hora.
- ⇨ Persona/grupo que registra la incidencia
- ⇨ Canal de entrada.
- ⇨ Datos del usuario.
- ⇨ Síntomas.
- ⇨ Estado.
- ⇨ CIs (Configuration Items, elementos de configuración) asociados.
- ⇨ Persona/grupo asignado para la resolución.
- ⇨ Problema/Known error asociado.
- ⇨ Actividades realizadas para la resolución.
- ⇨ Fecha y hora de la resolución.
- ⇨ Categoría del cierre.
- ⇨ Fecha y hora de cierre.

A parte de la información general que acabamos de ver, también es muy importante llevar un registro diario, con los siguientes parámetros:

- ⇨ Nº de incidencias
- ⇨ Tipo / Clasificación
- ⇨ Segmento de cliente
- ⇨ Tareas en las que está.
- ⇨ Servicio afectado.
- ⇨ Carterización en Provisión.

Los datos a aportar son los siguientes:

- ⇨ Control de todos los pedidos en incidencia pendientes
  - Segmento de cliente.
  - Tipo de incidencia.
  - Servicio afectado.
- ⇨ Control de áreas que tienen que cerrar incidencias
  - Entradas y Salidas.
  - SLOs y SLAs.
  - Tiempo medio en pendientes.
  - Nº pedidos superan niveles de calidad en incidencia.
  - Tipo de incidencia.
- ⇨ Control de áreas que abren incidencias

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

- Entradas y Salidas.
- Pendientes.
- Nº medio mensual de incidencias abiertas desde área que realiza la tarea.
- Tareas en las que se han abierto las incidencias.

⇨ Control de rotaciones de incidencias

- Nº incidencias están mal abiertas (por tarea y tipo).

Se realizará un registro semanal que tendrá los siguientes componentes

- Nº medio de incidencias abiertas al día.
- Nº medio de incidencias cerradas al día.
- Nº medio de incidencias pendientes.
- Tiempo medio de incidencias abiertas pendientes.

Todo ello, atendiendo a la siguiente clasificación

- Por tipo de incidencia.
- Por tarea.
- Por segmento.
- Por servicio.
- Diferenciando carterizados en Provisión.

En esta clasificación, generalmente se establece el tipo de incidencia, con una clasificación multinivel, con varias dependencias entre niveles, todo está correlacionado. El número total de niveles, dependerá en gran medida de la diversidad en la tipificación de las incidencias, que necesitemos clasificar, según nuestros criterios para su correcta gestión y resolución.

Existe una multitud de ocasiones, donde al producirse una incidencia, no se establece adecuadamente su clasificación, en el momento de registrarla, por lo que si esto sucede, en el momento del cierre de la misma, es necesario su correcta clasificación. Generalmente, la prioridad de una incidencia, va a determinar su tratamiento y su gestión de cara a su resolución.

La prioridad de la incidencia depende de:

⇨ Rapidez: La urgencia que necesita la incidencia par ser resuelta en un tiempo óptimo.

⇨ Impacto: Por norma general, se determina por usuarios afectados, aunque lo realmente importante es la criticidad de los servicios afectados por la incidencia, siendo lo realmente importante, el impacto adverso que tiene la incidencia en la infraestructura subyacente de la organización, causando efectos muy negativos para su negocio en general.

El equipo de soporte, debe de conocer las reglas en las cuales ha de basarse la priorización de las incidencias.

Resulta muy conveniente, que la herramienta de soporte utilizada, sea capaz de basarse en reglas, para la priorización de las incidencias

También se deben tener en cuenta factores auxiliares tales como el tiempo de resolución esperado y los recursos necesarios: los incidentes “sencillos” se tramitarán cuanto antes.

Dependiendo de la prioridad, se asignarán los recursos necesarios para la resolución de la incidencia. La prioridad del incidente puede cambiar durante su ciclo de vida. Es conveniente establecer un protocolo para determinar, en primera instancia, la prioridad del incidente.

La priorización de una incidencia está relacionada con el impacto y la urgencia para los usuarios o clientes del servicio TI.

El impacto se determina según el efecto que tiene sobre la operación del negocio o sobre el funcionamiento del servicio, mientras que la urgencia es determinada por la velocidad que se requiere para su resolución.

Cuando se recibe una incidencia el personal de soporte de primer nivel, en base a los síntomas, diagnostica la incidencia y la resuelve si está capacitado para ello. Este diagnóstico inicial de las incidencias, dan lugar a múltiples tipos de incidencias, posibilitando al personal de soporte de nivel 1, poder gestionarlas por sí mismos, o con el departamento correspondiente.

Para ver, según el diagnóstico inicial, podemos encontrarnos con los siguientes tipos de incidencias:

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

a) Incidencias por Causas del Cliente

- ⇨ Retenida por cliente: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + Nombre y teléfono de contacto del cliente que retiene la instalación y la causa expresada de retención.
- ⇨ Demanda Aplazada: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + Indicar la persona y teléfono del contacto del cliente que retiene la instalación y la fecha programada en la que quiere realizar el trabajo.
  En el caso de que se tratara de un Proyecto Especial donde se estableciera un plan de implantación con el cliente semanal o mensual, el Jefe de Proyecto de provisión podrá indicar entonces en la incidencia la fecha de fin de proyecto. También se utilizar este tipo de incidencia para los cambios de router, indicando la fecha programada con el cliente.

b) Incidencias por Causas Comerciales

Tramitación Incompleta: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + [LITERAL] + Indicar los datos erróneos y la causa de por qué no son correctos. Los literales serán:

1. [INCIDENCIA TRAMITACIÓN]: si sospechamos que hay un error en la tramitación
2. [INCIDENCIA SISTEMA]: si sospechamos que hay un error en la tramitación debido al sistema.

c) Soporte a Comercial

(Siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + [LITERAL] + Indicar todos los datos posibles del problema y de la duda comercial que hay que aclarar con el gestor que atiende la cuenta del cliente, en función del literal conforme se específica abajo.

Los literales posibles son los siguientes:

1. [CONFIRMAR ANULACIÓN]: Nº del pedido con el que se ha duplicado. Nombre del cliente y teléfono de contacto y causa por la que no lo quiere.
2. [ACLARAR DOMICILIO]: Descripción de los datos de domicilio que faltan.
3. [CONSULTA COMERCIAL]: Descripción de la incidencia.
4. [FALTA COBERTURA]: Descripción de la conexión en la que no existe cobertura del proveedor de circuitos.

d) Incidencias por Causas de Provisión

1. Soporte a Coordinación: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + Indicar la información adicional que debe ser aclarada para poder finalizar el trabajo.
2. Incidencia Aplicación: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + Indicar el número de incidencia aportada desde la aplicación.
3. Avería de línea: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + Indicar el número de avería proporcionados por el grupo de Gestión de Circuitos de acceso y Cortes en Red.
4. Pendiente Soporte a Ingeniería: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto + (fecha en la que se abre la incidencia) + Indicar número del soporte proporcionado por Ingeniería de Servicios o por Soporte Técnico a la Gestión.
5. Pendiente de Circuito: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + Indicar el teléfono y nombre de la persona del cliente, datos donde se debe instalar la línea y los datos donde está la línea en ese momento.
6. Cortes coordinados: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + Indicar el tipo de cambio que falta por realizar.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

7. Pendiente de Stock: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + Indicar el material que falta para la instalación.
8. Elemento de RED: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + Descripción del problema localizado en Nodo de Red.
9. Incidencia en Multienlace: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + Descripción del problema localizado.
10. Faltan Datos para la configuración del equipo: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + Indicar los parámetros técnicos del cliente configurables, que no se tienen y son necesarios.
11. Pendiente de proyecto: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia)+ Indicar bajo que causa se encuentra el proyecto que se demanda.

Las herramientas de Gestión del Servicio deben usarse para automatizar escalas de tiempo (tiempos de escalado) y escalar la incidencia como requieran unas reglas predefinidas.
En realidad, esta definición de las herramientas de gestión del servicio, en relación con los tiempos de escalado, nos viene a decir que, dependiendo del tipo de incidencia y transcurrido un tiempo establecido para su resolución, debe de pasar de un grupo de soporte a otro más especializado para resolverla. No es en absoluto recomendable, el escalado de incidencias de manera automática, ya que puede generar tensiones entre los diferentes grupos de soporte, sin que un específico grupo, no haya trabajado nada con ella, y por lo tanto, llegarán incidencias sin documentar, incidencias resueltas en anteriores ocasiones etc.
Para un proceso de gestión de incidencias no muy maduro, el escalado de incidencias de manera automática, serviría muy bien en organizaciones que están empezando a prestar servicios, y que por supuesto aquellas incidencias, estén muy bien definidas, para que no haya ambigüedades ni lagunas en su documentación.
Para definir un proceso de asignación de incidencias con respecto a los tiempos de escalado, lo primero que hay que definir es:

- ⇨ Qué tipo de incidencias van a ser resueltas y por cada grupo de soporte.
- ⇨ Tener en cuenta la criticidad de la incidencia

Existen dos tipos de escalado

- ⇨ Funcional: El grupo de nivel 1, se ve incapacitado para resolver la incidencia, y la escala al grupo especializado de nivel 2 para su resolución.
- ⇨ Jerárquico: en caso de que se den ciertas circunstancias (incidencias graves o críticas, riesgo de incumplimiento del SLA o SLO, dependiendo de los tiempos estimados de resolución), éstas se deben notificar a los responsables del servicio correspondientes.

A tenor del escalado que se realice, la incidencia que está escalada, sigue perteneciendo al grupo de nivel 1.
El grupo de nivel 1, es quién debe de hacer el seguimiento de la incidencia, gestionarla adecuadamente, para que sus tiempos de resolución no excedan los parámetros de calidad marcados en los SLAs y SLOs.
Este grupo de nivel 1, es quién debe de cerrar la incidencia cuando esté resuelta, además de ser los responsables de la interlocución con los usuarios finales con respecto a la misma. Si la incidencia hace referencia a un fallo en el sistema, lo más probable es que se necesite investigar la causa del fallo. Las tareas más comunes dentro de esta actividad son las siguientes:

- ⇨ Establecer exactamente qué es lo que no funciona correctamente y para qué secuencia de acciones del usuario (casuística).
- ⇨ Establecer el impacto potencial de la incidencia.
- ⇨ Determinar si la incidencia está producida por la implantación de un cambio.
- ⇨ Buscar en la base de datos de conocimiento (base de datos de errores conocidos, registro de incidencias, etc.) posibles soluciones y/o workarounds.

Diagnóstico

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

- ⇨ En base al estado del circuito, corresponde con una primera valoración de la causa de la incidencia
- ⇨ Es muy importante realizar el diagnóstico rápidamente (10-15min) ya que es la prueba de que comenzamos a tratar la incidencia

Problemática

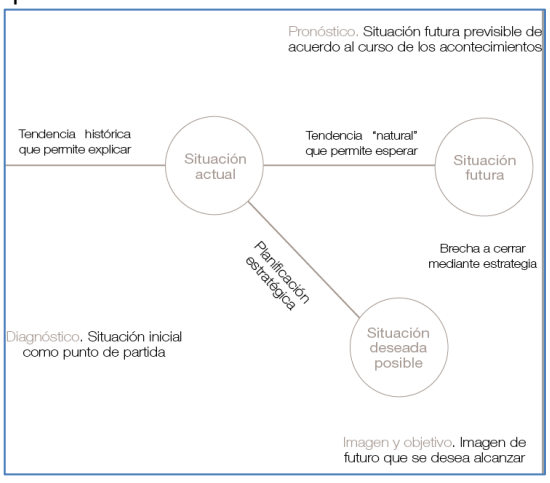
- ⇨ Peticiones de los clientes de dejar en observación los circuitos un largo período de tiempo – Localización de los clientes durante periodos festivos: fines de semana, vacaciones...
- ⇨ Solución: serie local (solo aperturas proactivas)
- ⇨ Estado observación por más de 12 horas: se cierra y se abre una nueva como proactiva para convertirla en local.
- ⇨ Provisión incompleta: se anula (si no es proactiva) y se reabre como proactiva para convertirla en local Solución: serie local (solo aperturas proactivas).
  - Incidencia proactiva pero NO se puede contactar con cliente en dos horas: local.
  - Si existe avería real, se cierra la incidencia local y se abre una nueva para tratarla.
  - Si no existe avería real, se cierra la incidencia local y se abre una nueva para cerrarla indicando la causa adecuada.
  - Abiertas por cliente y NO se contacta con él en dos horas
  - Se cierra dicha incidencia indicando 'mala operación de cliente'.
  - Abrimos una como 'proactiva por rutina' e indicamos el número de la incidencia anterior de la que procede.

La planificación de las intervenciones, son un conjunto de capacidades en relación a la comprensión de un plan trazado, con el firme objetivo de organizar, elaborar un plan, buscar estrategias y tomar decisiones al respecto.

Las acciones llevadas a cabo por la planificación, se articulan mediante una serie de procedimientos en los que la existencia de una mejor racionalidad y organización, en el conjunto de las actividades que hay que realizar, influyen directamente sobre el curso causal de estas actividades, con el fin de poder obtener unos resultados o una situación como deseable, mediante el uso eficiente de los medios y los recursos escasos o limitados.

La planificación, al ser un proceso que se desarrolla en un período de tiempo determinado y con la misión de definir la dirección del proceso de cambio de la actividad o conjunto de actividades, se va a ilustrar en un esquema, la planificación, desde su origen, pasando por la dirección del proceso de cambio, llegando a la situación deseada.

Como en todo servicio, estos se pueden desglosar en un número determinado de niveles operativos, los cuales no van a ser menos en la planificación de las intervenciones.



Niveles operativos en la planificación de las intervenciones

1. Las políticas son las bases en las que se fundamentan los procesos de desarrollo, en dirección a la culminación de los objetivos marcados.
2. El plan es el instrumento del proceso y del sistema de planificación que concreta y materializa la visión, los principios, los objetivos, las políticas, las estrategias y las metas de desarrollo deseado y posible.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

3. Los objetivos hacen referencia al fin o propósito de la situación futura deseable.
4. Las metas cuantifican los objetivos a través de indicadores e índices con los que se pretende evaluar su grado de cumplimiento.
5. Las estrategias se refieren a los caminos o direcciones sobre cómo lograr los objetivos, las políticas elegidas.
6. Los instrumentos son las diferentes herramientas que permiten evaluar y hacer el seguimiento del plan.
7. El programa materializa un conjunto de decisiones, cuyas directrices deben estar orientadas a solucionar los problemas, satisfacer las necesidades y conseguir los objetivos del plan.
8. El proyecto se percibe como un conjunto de acciones, orientadas a la solución de un problema o una necesidad, teniendo en cuenta los recursos disponibles debidamente programados en el tiempo y en el espacio. Los objetivos del proyecto concretan y materializan los objetivos del programa y a su vez los del plan de desarrollo.
9. Los recursos pueden ser de carácter humano, físico, económico, financiero...
10. La actividad es un conjunto de tareas u operaciones interrelacionadas entre sí, enfocadas a la obtención de objetivos parciales y localizados dentro del proyecto y del plan de desarrollo.

Estas capacidades en relación a la planificación de las intervenciones en una situación dada a un problema existente, podemos clasificarlas en 4 bloques distintos:

Análisis de la información existente

Aquí se trata de saber la información disponible de la que se tiene, la necesidad y la relevancia de dicha información disponible con respecto a la planificación de las intervenciones y si son importantes o meramente superfluas con respecto al fin que se persigue. Dentro del análisis de la información existente, podemos distinguir igualmente 2 partes bien diferenciadas:

- ⇨ Una reflexión sobre las posibilidades de la información disponible:
  Aquí, podemos extraer las distintas combinaciones posibles entre las informaciones que disponemos, como se pueden combinar entre ellas, las relaciones existentes entre ellas, además de poder deducir los tipos de operaciones que se pueden llevar a cabo en la planificación de las intervenciones, junto con su sentido o coherencia.
- ⇨ Reflexiones sobre los medios empleados, en relación a los fines. La relación de los datos disponibles con las preguntas formuladas al respecto.
  En este apartado, podemos preguntarnos sobre como los datos de los que disponemos, puede responder eficazmente al problema que se nos plantea. Como elegir los medios idóneos y necesarios con la información disponible, para dar respuesta al problema del que se adolece, para conseguir u obtener un fin en concreto, para responder a lo que el problema en si está pidiendo.

Organización de la información disponible

La información, debe de ser estructurada en esquemas y diagramas con datos e incógnitas, es decir con datos que se saben y otros datos que no se saben.

Exploración

Se trata de capacidades asociadas a examinar problemas equivalentes, modificar problemas y examinar problemas particulares.

Concebir y estructurar un plan de resolución

En este apartado, consiste en razonar con una parte del plan o con toda, a raíz de los datos de los que disponemos, realizar prospecciones sobre los resultados posibles a obtener, probar estrategias previamente elaboradas o heurísticas.

La situación y problemática actual de los servicios, en relación a la resolución de incidencias en redes telemáticas, requieren una planificación previa de las intervenciones a realizar en los diferentes servicios que se presten.

En algunos casos, esta planificación de las intervenciones, requieren desplazamientos de los técnicos para revisar y solucionar los problemas que se hayan presentado.

Uno de los inconvenientes en algunos casos que pueden presentarse en la planificación de las intervenciones y en el cierre de una incidencia, es determinar si la intervención, es o no facturable.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

En la siguiente página se presentan los conceptos que pueden ser facturables y los que no lo son.

FACTURABLE	NO FACTURABLE
· Problema localizado en equipamiento de cliente. · Problema en instalación interior de cliente. · Problema localizado en algún elemento de la línea del proveedor, originado por una mala operación del cliente.	· Problema localizado en cualquier elemento responsabilidad del proveedor.

1.3.1. Función AlarmSurveillance: Conceptos y elementos relacionados

Función de vigilancia de alarma

La función de la vigilancia de alarmas de manera genérica, se refiere a que un sistema de alarma es un elemento de seguridad pasiva. Esto significa que no evitan una situación anormal, pero sí son capaces de advertir de ella, cumpliendo así, una función disuasoria frente a posibles problemas.
Ejemplo:
Por ejemplo: La intrusión de personas. Inicio de fuego. El desbordamiento de un tanque. La presencia de agentes tóxicos. Cualquier situación que sea anormal para el usuario.
Son capaces además de reducir el tiempo de ejecución de las acciones a tomar en función del problema presentado, reduciendo así las pérdidas.

Función de gestión de incidencias

La función de gestión de incidencias, cubre cualquier tipo de incidencia que se pueda dar, desde fallos del sistema, consultas formuladas por los usuarios de las propias aplicaciones o sistemas a monitorear, o bien aquellas incidencias que sean abiertas por el propio personal técnico, además de aquellas, abiertas automáticamente por el propio sistema de monitorización de eventos.
Existen unos conceptos fundamentales, con respecto a la gestión de incidencias, que son:

- ⇨ Límites de tiempo: Aquí se deben de definir los límites de tiempo, para cada uno de los procesos, y que sirvan o se emplean como elementos integradores en los acuerdos de nivel operativo OLAs y contratos de soporte ULs.
- ⇨ Modelos de incidencia: Formas de procesar las incidencias, para poder ejecutarlas adecuadamente, según las políticas de gestión de incidencias de la organización. De forma que las incidencias estándar o más comunes, se gestionarán y resolverán en un tiempo record y se gestionarán también, en un tiempo record.
- ⇨ Incidencias graves: En este tipo de incidencias, se debe de establecer la prioridad de la misma, junto con un sistema de prioridades para incidencias, con un procedimiento de resolución más corto y una mayor urgencia en la gestión y resolución de la misma. También, es importante realizar una descripción exacta del problema.
- ⇨ Escalado funcional: Esto significa, el traslado de la incidencia, a un equipo de mayor experiencia para ayudar a la resolución de la incidencia.
- ⇨ Escalado jerárquico: Este tipo de escalado, significa involucrar más niveles de gestión de incidencias, para tareas de soporte en un escalado.

Conceptos y elementos relacionados. la integración de los sistemas de vigilancia de alarmas y de gestión de incidencias – atención al cliente
La función de vigilancia de alarmas y la función de gestión de incidencias, están estrechamente interrelacionadas entre sí, pudiéndose maximizar los beneficios de ambas funcionalidades en una sola integración de ambos servicios.
Los elementos de la vigilancia de alarmas, son susceptibles de traspaso de información a los elementos que gobiernan un sistema de gestión de incidencias, con el objetivo, de servir en tiempo y forma, la urgencia de las alarmas y su gestión asociada.
Esta solución de elementos relacionados de un sistema de vigilancia de alarmas y un sistema de gestión de incidencias, facilitará a los usuarios autorizados de operación y supervisión, la posibilidad de registrar incidencias de servicio directamente a partir de la información contenida en las alarmas recogidas por la consola.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Con los sistemas de vigilancia de alarmas y de gestión de incidencias – Atención al cliente, existen diversas debilidades, que son mejorables con la integración de ambos servicios. Las debilidades que podemos detectar con la independencia de estos servicios son:

- ⇨ La posibilidad de cometer errores involuntarios en la información que se suministra al sistema de gestión de incidencias – Atención al cliente.
- ⇨ La ineficiencia de un modelo basado dos sistemas separados y en copiar y pegar información entre ellos.
- ⇨ La información sobre la relación existente entre una alarma y su correspondiente incidencia reside solo en uno de los extremos, el sistema de gestión de incidencias – Atención al cliente, y ello obliga a los operadores a abandonar su entorno natural de trabajo para consultar la incidencia en el sistema de gestión de incidencias – Atención al cliente derivada de una alarma.

Ejemplo:

Tenemos un ejemplo claro, para poder ilustrar con más facilidad los beneficios de la integración de estos 2 servicios, en relación a la operativa diaria del usuario o equipo de soporte encargado de estas gestiones.
La solución propuesta a modo de ejemplo es la integración de Netcool – SAC (Sistema de gestión de incidencias – Atención al cliente). Con la solución de integración Netcool-SAC aportada, se pretende subsanar estos inconvenientes, haciendo el trabajo de los operadores más eficiente y animándoles a concentrar su esfuerzo en las responsabilidades específicas de su puesto. Así, la herramienta Netcool-SAC:

- ⇨ Evita la comisión de errores involuntarios en la información transferida entre los sistemas al realizarlo de forma automática
- ⇨ Rentabiliza el proceso de apertura de incidencias SAC puesto que el operador, sin tener que abandonar su entorno de trabajo, inicia el proceso directamente desde su consola de operación Netcool.
- ⇨ Registra el número de incidencia relacionada en un campo especial de la alarma (“Ticketing”) preparado para este fin, facilitando de esta forma, la identificación directa de las alarmas con incidencias abiertas en SAC y también el número de incidencia relacionada.

1.3.2. Análisis y diagnóstico de información de alarma

En el análisis y diagnóstico de la información proveniente de las diferentes alarmas del sistema de monitoreo, es muy importante saber poder interpretarla adecuadamente, para realiza un análisis y diagnóstico acertado, de la información que nos proporciona dicha alarma.
A continuación, se resumen algunos campos de las alamas de un sistema de monitoreo.
Estos son los campos donde vamos a recibir los distintos tipos de eventos alarmas, según nuestras preferencias. Se alimentan de los campos que les proporciona la base de datos, si hacemos doble clic en una alarma/evento accederemos a toda la información que la base de datos.

- ⇨ Identifier. Parámetro identificado para reduplicar mensajes
- ⇨ Serial. Identificador de alarma
- ⇨ Node. Nombre del EDC o Passport afectado
- ⇨ NodeAlias. Nombre del EDC remoto afectado
- ⇨ Manager. Origen del mensaje VPO o NMS.
- ⇨ Agent. Proporciona el Customer_id de NMS.
- ⇨ AlertGroup. Proporciona una característica de la alarma, circuito, caída de Enlace, Conectividad.
- ⇨ Severity. Severidad de alarma.
- ⇨ Summary. Descripción de la alarma.
- ⇨ StateChange. Se actualiza cada vez que se modifica un evento (de duplicaciones, usuario, gateway, probe).
- ⇨ FirstOcurrence. Se fija cuando se inserta una alarma por primera en el Object Server.
- ⇨ LastOcurrence. Se actualiza en las de duplicaciones utilizando la hora que viene en la alarma.
- ⇨ InternalLast. Se actualiza en las de duplicaciones utilizando la hora interna del Object Server que viene con la alarma.
- ⇨ Poll. Hora de muestreo.
- ⇨ Type. Nos dice si la alarma es un problema (1), una resolución (2) o un evento que tiene fijado un tiempo de expiración.
- ⇨ Class. Clase de evento. Según este parámetro tendrá disponible unas u otras herramientas.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

- ⇨ Grade. Se usa para identificar criticidad de alarmas.
- ⇨ Location. Localización.
- ⇨ OwnerUID. UID del usuario que tiene asignando el evento.
- ⇨ OwnerGID. GID del usuario que tiene asignado el evento.
- ⇨ Acknowedge. Se usará para intervenir cierto tipo de alarmas.
- ⇨ Flash. Nos dice si la alarma tiene que parpadear. No se usa.
- ⇨ SeverName. Object Server desde el que la alarma fue originada.
- ⇨ ServerSerial. Número de serie de la alarma originada.
- ⇨ Ticketing. Determinará el estado de un ticket. (Cuando haya integración con SAC).
- ⇨ Object. Objeto que presenta problema.
- ⇨ MsgId. Contendrá el identificador de mensaje original de una alarma de VPO.
- ⇨ NodeGroup. Nombre del Cliente al que pertenece la alarma.
- ⇨ TypeServ.
- ⇨ TypeIdent.
- ⇨ ValueServ. Valor del servicio afectado.
- ⇨ CodSin. Código del síntoma asociado a la incidencia.
- ⇨ Origen. Origen de la alarma.
- ⇨ TelefCoor. Teléfono del coordinador técnico.
- ⇨ Passport. Passport.
- ⇨ Interface.
- ⇨ Fruni. Fruni del circuito.
- ⇨ Field1. Parámetro comodín. Sin uso.
- ⇨ Field2. Parámetro que identifica si la alarma paso por Impact.
- ⇨ Field3. Parámetro comodín. Sin uso.
- ⇨ Field4. Grupo de soporte al que pertenece la alarma.

A continuación, se va a mostrar los colores según la gravedad del evento.

Color	Grado de criticidad	Significado
Rojo	Critical	La alarma recibida denota una situación crítica en el sistema
Naranja	Major	La alarma recibida denota una situación grave en el sistema
Amarillo	Minor	La alarma recibida indica que podría existir algún error en el sistema
Verde	Clear	La alarma recibida indica que el sistema funciona correctamente
Azul	Warning	La alarma recibida avisa sobre una situación que se debería de tener en cuenta
Morado	Indeterminate	La criticidad de la alarma aún no ha sido definida por el administrador

Esta información sobre el análisis y el diagnóstico de las diferentes informaciones que nos proporcionan las distintas alarmas que se ha descrito anteriormente, están en relación a la programación de los diferentes eventos que pueden suceder en el entorno donde trabaja el sistema de monitorización.
En base a diversos elementos, eventos u objetos, la información de la alarma que nos proporcionará un campo de alarma de terminado, será distinto, dependiendo de la elección que hagamos de los diferentes elementos, eventos u objetos a filtrar.
En el análisis y diagnóstico de la información proveniente de las diferentes alarmas del sistema de monitoreo, es muy importante saber poder interpretarla adecuadamente, para realiza un análisis y diagnóstico acertado, de la información que nos proporciona dicha alarma.

1.3.3. Documentación y seguimiento de incidencias: procedimientos y herramientas de troubleticketing

Los procesos de trouble ticketing

Para la documentación y seguimientos de incidencias, se ha tenido que crear un sistema de gestión de las mismas, cuyos principales componentes de dichos sistemas, son los propios departamentos internos de la compañía que presta estos servicios de trouble ticketing.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Esta colaboración interdepartamental, en definitiva se traduce en clientes internos de la compañía, y aquellos que han contratado el servicio, se les denomina clientes externos.
Llegados a este punto, tanto los clientes internos como los externos, son igual de importantes, en todo sistema de gestión de avería e incidencias del sistema.
En los procesos de supervisión y gestión de incidencias, se detectan normalmente una serie de anomalías que pueden ir desde problemas puntuales en el servicio o la red del sistema, hasta por motivos de mantenimiento, ha existido un problema que cubra un área geográfica determinada, incluyendo en la incidencia, un gran número de componentes del sistema y clientes involucrados.
Este tipo de incidencias, se les denomina incidencias masivas.
En algunos sistemas de gestión de incidencias, hacen distinción entre las incidencias por servicios o las incidencias de red.
Dicha gestión de incidencias, deben de agilizar la resolución de las mismas, y poner a disposición de atención al cliente el problema, y con más razón si se tratan de incidencias masivas.
Esto permitiría un tratamiento proactivo del problema.

Sistemas de trouble ticketing

La documentación y seguimiento de las incidencias tanto reactivas como proactivas, se llevan a cabo a través de los sistemas de trouble ticketing, como consecuencia de la labor del departamento de atención al cliente, a la supervisión de los sistemas y a la labor de mantenimiento. La documentación como el seguimiento de las diferentes incidencias, se llevan a cabo mediante un sistema conocido como boletines, que son generados por atención al cliente, por la labor de supervisión de los sistemas o a su mantenimiento.
Estos boletines, una vez generados, son llevados a cabo por las personas más adecuadas para su tratamiento, cuyos grupos para su resolución son:

- ⇨ Grupo de soporte centralizado que actúa en la incidencia de forma remota sobre las centrales.
- ⇨ Grupo móvil de soporte, que son personas que se desplazan físicamente hasta la central.
- ⇨ Grupo móvil cliente, son aquellos técnicos, que se desplazan al domicilio del cliente para atender la incidencia.

Tratamiento básico de las averías y reclamaciones
El tratamiento básico de averías y reclamaciones, se centra básicamente en 3 pilares básicos para todo sistema de averías y reclamaciones. En los sistemas de gestión de averías y reclamaciones, también existen otros sistemas más específicos en la gestión de averías, o sistemas específicamente diseñados a la resolución de las mismas.

Documentación de las incidencias

En este apartado de documentación, es donde se genera toda la documentación de partes de no conformidades, de inspección y de acción correctiva/preventiva o de comprobación, por el departamento correspondiente donde se genera.
Mientras aquella documentación relacionada con el sistema de calidad en la comprobación, serán archivados por este último. Será el encargado de la guardia y custodia de dicha documentación.
Por otro lado, todo aquellos partes o quejas / reclamaciones, informes de auditoría y altas de revisión o comprobación, perteneciente al proceso de comprobación de la reparación de la incidencia, será archivado por el área de calidad.
Esta fase de documentación en el proceso de gestión de incidencias, sirve como tales, para el mismo registro de incidencias, así como para establecer, aplicar y verificar todas aquellas acciones correctivas para tratar la incidencia.
Todo ello, debe de ser documentado mediante un procedimiento de documentación, de tales pasos.
Este procedimiento de documentación, no solo serviría como proceso para el tratamiento de las incidencias y recoger las reclamaciones a clientes y proveedores, sino que además, deberá recoger ciertos procesos del sistema de calidad, como por ejemplo, las sugerencias del personal propio, material en mal estado e incumplimiento de requisitos preestablecidos.
En el procedimiento debidamente documentado, deberá entenderse que se entiende por incidencia, los tipos que existen, las diferentes actuaciones y quienes son los responsables de las mismas.
La documentación de todas las distintas fases o procesos por los que se gestionan las incidencias, son de vital importancia.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

La aprobación por parte de la alta dirección, no es un mero capricho del responsable de calidad, sino que establece una forma más segura de poner en marcha todos los procedimientos y pautas a seguir, para el tratamiento y gestión de las incidencias.
Antes de la aceptación del documento de procedimientos por parte de la alta dirección, dicho documento de procedimientos, ha sufrido importantes debates acerca de su desarrollo e implementación, teniendo en cuenta las diferentes opiniones del personal y de todos los responsables implicados.
Una vez tenidos en cuenta las diferentes opiniones del personal y de todos los responsables, el documento de procedimientos, se aseguraba su implicación y ejecución, junto con un nivel de detalle.
Finalmente, para que la documentación de procedimientos tuviera la difusión que le correspondía, debido a la gran implicación que se recogía en él, debía de estar suficientemente expuesto a todos el personal y responsables de la organización para su posterior consulta y seguimiento.
Esta difusión de la documentación, deberá estar regida a su vez, por un procedimiento también documentado, sobre la distribución de documentación por toda la organización.
Para todas las incidencias, deberán ser registradas y documentadas con detalle y extensión adecuados a la magnitud y criticidad de la incidencia, por medio de cualquiera de los medios de comunicación puestos a disposición para el tratamiento y gestión de incidencias.

Relación de formatos de documentación

Podemos establecer una relación a modo de introducción y guía, sobre los posibles formatos de los diferentes documentos, citando por ejemplo:

- ⇨ Formato F01: para la apertura y formulación de incidencias.
- ⇨ Formato F02: para la presentación de quejas, sugerencias y reclamaciones.
- ⇨ Formato F03: para la obtención de resultados de los indicadores.
- ⇨ Formato F04: para la solución de las incidencias.
- ⇨ Formato F05: para el cierre de incidencias.

Seguimiento de incidencias

Una vez determinados todas las identificaciones y descripciones de las actividades necesarias para determinar el tipo de problema y generar la incidencia adecuada a sus peculiaridades intrínsecas.
Pues bien, una vez determinados estas actividades, podemos dar paso, a un importante hito en el seguimiento de incidencias, donde resulta del todo imprescindible su generación y adecuado seguimiento, con el objetivo de realizar un proceso de calidad del seguimiento de la incidencia, que desembocará en una óptima y satisfactoria resolución de la misma.
Hablamos de la generación de informes de seguimientos, donde esta herramienta del seguimiento de incidencias, es un potente y eficaz método para un óptimo y correcto proceso de seguimiento.

Se realizará un informe diario que deberá tener como parámetros los siguientes componentes:

- ⇨ Nº de incidencias.
- ⇨ Tipo / Clasificación.
- ⇨ Segmento de cliente.
- ⇨ Tareas en las que está.
- ⇨ Servicio afectado.
- ⇨ Carterización en Provisión.

Los datos a aportar son los siguientes:

- ⇨ Control de todos los pedidos en incidencia pendientes
  - ○ Segmento de cliente
  - ○ Tipo de incidencia
  - ○ Servicio afectado
- ⇨ Control de áreas que tienen que cerrar incidencias:
  - ○ Entradas y Salidas
  - ○ SLOs y SLAs,
  - ○ Tiempo medio en pendientes
  - ○ Nº pedidos superan niveles de calidad en incidencia

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

- Tipo de incidencia

⇨ Control de áreas que abren incidencias:
- Entradas y Salidas
- Pendientes
- Nº medio mensual de incidencias abiertas desde área que realiza la tarea
- Tareas en las que se han abierto las incidencias

⇨ Control de rotaciones de incidencias
- Nº incidencias están mal abiertas (por tarea y tipo)

Se realizará un informe semanal que tendrá los siguientes componentes
- Nº medio de incidencias abiertas al día
- Nº medio de incidencias cerradas al día
- Nº medio de incidencias pendientes
- Tiempo medio de incidencias abiertas pendientes

Todo ello, atendiendo a la siguiente clasificación:
- Por tipo de incidencia
- Por tarea
- Por segmento
- Por servicio
- Diferenciando carterizados en Provisión

Una vez generados los informes de seguimiento, una de las casusas muy importantes en el seguimiento de las incidencias, es la superación de los tiempos pactados para su resolución, debiéndose elaborar diferentes procedimientos para las distintas reclamaciones oportunas, a las áreas implicadas en las incidencias. Todas las incidencias tienen establecido unos tiempos objetivo (SLO) y medio (SLA) de resolución.
En caso de incumplimiento de estos tiempos pactados, el Grupo de Control Operativo de Servicios, procederá a reclamar al área correspondiente, siguiendo los siguientes niveles de escalado:

⇨ Nivel 1 (SLO): Cuando una incidencia cumple el SLO establecido sin resolverse, se comunicará al área responsable de su resolución.

⇨ Nivel 2 (SLA): Cuando una incidencia cumple el SLA establecido sin resolverse, se comunicará al área responsable de su resolución y al primer nivel jerárquico.

⇨ Nivel 3 (N x SLA): Cuando una incidencia cumple N x SLA establecido sin resolverse, se comunicará al área responsable de su resolución, al primer nivel jerárquico y al segundo nivel jerárquico

⇨ Nivel 4 (5 x SLA): Cuando una incidencia cumple 5 x SLA establecido sin resolverse, se comunicará al área responsable de su resolución, al primer nivel jerárquico, al segundo nivel jerárquico y al tercer nivel jerárquico

Herramientas para la gestión, seguimiento y reclamaciones de averías e incidencias

Algunos de los sistemas que existen, para la gestión de averías e incidencias, son el sistema:

⇨ AF (Sistema para el tratamiento de averías de telefonía básica).

⇨ SIRIO (Sistema para el tratamiento de reclamaciones y averías de organización o empresas).

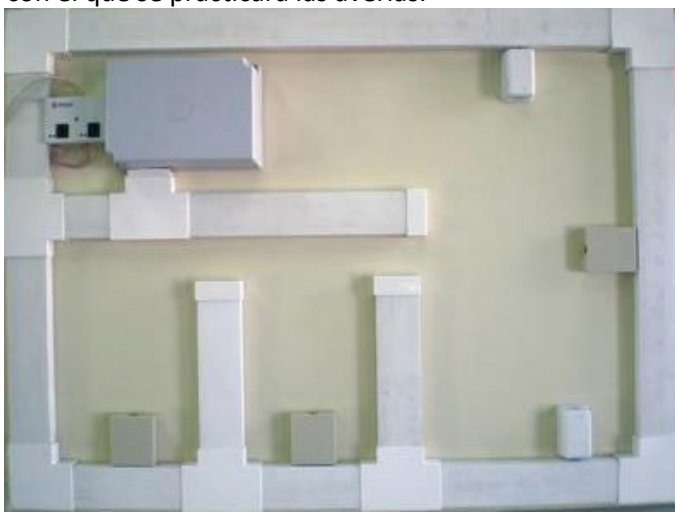
Estos sistemas, están destinados para la resolución de averías y reclamaciones por parte de los clientes externos.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

1.3.4. Casos prácticos y ejemplos

Par con circuito abierto

En este supuesto práctico, se va a especificar que un cable está en circuito abierto. Para realizarla, es necesario tener el tablero con el que se practicará las averías.



Un comprobador de prueba y tono, un conector 6p2c y un cable telefónico de 2 hilos (sobre unos 30 cm).

Inicio de la simulación de la avería

1. Abrimos una roseta cualquiera del tablero fabricado y soltamos un terminal a propósito.

2. Conectamos el generador del comprobador de prueba y tono, a la salida del PTR.

3. Colocamos el generador en posición de CONTINUITY.

4. Fabricamos un conector 6p2c especial, el cual ayudará a medir la continuidad, lo cual cortocircuitamos los pines centrales del conector y crimpamos.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

5. Colocamos el cable fabricado cortocircuitado a propósito, en la roseta donde queramos hacer la medición.

6. Cogemos el generador y observamos que no se enciende la luz verde, por lo que hay falta de continuidad.

7. Para localizar la falta de continuidad, colocamos el generado en la posición TONE.

8. Con el receptor, vamos recorriendo todo el cable, hasta llegar al punto donde el cable se corta.

9. En este caso, en la roseta encontramos el fallo. Si la avería estuviera en el cable, lo arreglaríamos empalmándolo con un conector UY o similar.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

2. Interconexión de redes

2.1. Conceptos básicos sobre redes públicas

Conceptos generales de interconexión

Definición de conceptos de red

Las redes de datos han cambiado nuestra forma de ver nuestras empresas y empleados. Ya no es necesario mantener una ubicación común para todos los empleados si se quiere acceder a la información que estos necesitan para desarrollar su trabajo.

Debido a esto, hay muchas organizaciones que han cambiado sus estrategias comerciales para utilizar estas redes de la forma en que llevan a cabo su actividad empresarial.

Hoy día es frecuente que una empresa organice el internetworking corporativo de tal forma que permita optimizar sus recursos.

Los criterios a utilizar para definir la red, en función del agrupamiento de los usuarios, destacamos:

- ⇨ La oficina principal es aquella donde todos están conectados a una LAN y donde está ubicada la mayoría de la información corporativa.
- ⇨ Una oficina principal podría contar con cientos o miles de usuarios que dependen de la red para desarrollar su trabajo.
- ⇨ La oficina principal podría consistir en un edificio con muchas redes de área local (LAN), o bien en un campus de edificaciones de ese estilo.

Dado que todos los usuarios necesitan acceder a recursos e información centralizados, es habitual encontrarse con una LAN backbone de alta velocidad, así como un centro de datos general con computadoras mainframe y servidores de aplicaciones.

Las demás conexiones consisten en una diversidad de ubicaciones de acceso remoto que necesitan conectarse a los recursos de las oficinas principales y/o entre ellas, incluidas las siguientes:

- ⇨ Sucursales. Se trata de ubicaciones remotas donde trabajan grupos más reducidos de individuos. Estos usuarios se conectan entre sí por medio de una LAN. Para acceder a la oficina principal, los usuarios utilizan servicios de redes de área amplia (WAN).
  Aunque parte de la información podría estar almacenada en la sucursal, lo más probable es que los usuarios tengan que acceder a la mayoría de los datos desde la oficina principal.
  La frecuencia con la que se accede a la red de la oficina principal determina si las conexiones WAN deben ser permanentes, o bien mediante acceso telefónico.
- ⇨ Teletrabajadores. Se trata de empleados que trabajan desde sus domicilios.
- ⇨ Usuarios móviles. Se trata de individuos que trabajan desde distintas ubicaciones y dependen de distintos servicios para poder conectarse a la red. Cuando están en las oficinas principales o sucursales, estos usuarios se conectan a la LAN.
  Cuando se encuentran fuera de la oficina, normalmente dependen de servicios de acceso telefónico para conectarse a la red corporativa.
  Para conocer los tipos de equipo y servicios que es necesario implementar en una red y cuándo deben utilizarse, es importante tener en cuenta las necesidades comerciales y de los usuarios.
  Esto permite subdividir la red en un modelo jerárquico que se expande desde el equipo de usuario final hasta el núcleo (backbone) de la red.
  Para subdividir un internetworking de redes en componentes más pequeños, Cisco utiliza un modelo jerárquico de tres niveles (capas), como se describe en el siguiente apartado.

Adaptación de las necesidades de empresa a un modelo jerárquico

Con el fin de simplificar el diseño, implementación y administración de las redes, Cisco utiliza un modelo jerárquico para describir la red.

Aunque la práctica de este método suele estar asociado con el proceso de diseña de una red, es importante comprender el modelo para poder determinar el equipo y características que van a necesitar en la red.

Tradicionalmente, las redes de campus han colocado la logística y servicios básicos a nivel de red en el centro de la red, compartiendo el ancho de banda a nivel de usuario.

Las demandas del usuario y las aplicaciones de red han obligado a los profesionales de las redes a utilizar patrones de tráfico en la red como criterio para construir un internetworking.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Las redes no pueden ser divididas en subredes basándose únicamente en el número de usuarios.
La aparición de servidores capaces de ejecutar aplicaciones globales tiene también una incidencia directa en la carga de la red. Un tráfico elevado en la red global supone tener que emplear técnicas de enrutamiento y conmutación más eficaces.Los patrones de tráfico son hoy día los que dictan el tipo de servicios necesarios para los usuarios finales de la red.
Para construir correctamente un internetworking de redes que pueda dar una respuesta eficaz a las necesidades de un usuario, se utiliza un modelo jerárquico de tres capas para organizar el flujo de tráfico. El modelo consta de tres capas:

- ⇨ Acceso
- ⇨ Distribución.
- ⇨ Núcleo principal.

Cada una de estas capas tiene una función en el suministro de servicios de red, como se describe en los siguientes apartados.

Capa de acceso

La capa de acceso de la red es el punto en el que cada usuario se conecta a la red. Ésta es la razón por la cual la capa de acceso se denomina a veces capa de puesto de trabajo.

- Los usuarios, así como los recursos a los que estos necesitan acceder con más frecuencia, están disponibles a nivel local.
- El tráfico hacia y desde recursos locales está confinado entre los recursos, switches y usuarios finales.
- En la capa de acceso podemos encontrar múltiples grupos de usuarios con sus correspondientes recursos.

En estos casos, el tráfico de usuarios que demandan estos servicios se desvía a la siguiente capa del modelo: la capa de distribución.

Capa de distribución

La capa de distribución de la red (denominada a veces de grupo de trabajo) marca el punto medio entre la capa de acceso y los servicios principales de la red.
La función primordial de esta capa es realizar funciones tales como enrutamiento, filtrado y acceso a WAN.
En un entorno de campus, la capa de distribución abarca una gran diversidad de funciones, entre las que figuran las siguientes:

- Servir como punto de acumulación para acceder a los dispositivos de capa.
- Enrutar el tráfico para proporcionar acceso a los departamentos o grupos de trabajo.
- Segmentar la red en múltiples dominios de difusión / multidifusión.
- Traducir los diálogos entre diferentes tipos de medios, como Token Ring y Ethernet.
- Proporcionar servicios de seguridad y filtrado.

La capa de distribución determina la forma más rápida para que la petición de un usuario (como un acceso al servidor de archivos) pueda ser remitida al servidor. Una vez que la capa de distribución ha elegido la ruta, envía la petición a la capa del núcleo principal.
La capa principal podrá entonces traspasar rápidamente la petición al servicio apropiado.

Capa del núcleo principal

La capa del núcleo principal (también llamada capa backbone), se encarga de desviar el tráfico lo más rápidamente posible hacia los servicios apropiados.
Normalmente, el tráfico transportado se dirige o proviene de servicios comunes a todos los usuarios. Estos servicios se conocen como servicios globales o corporativos.
Algunos de tales servicios pueden ser e-mail, el acceso a Internet o la videoconferencia. Cuando un usuario necesita acceder a un servicio corporativo, la petición se procesa al nivel de la capa de distribución.
El dispositivo de la capa de distribución envía la petición del usuario al núcleo. Este se limita a proporcionar un transporte rápido hasta el servicio corporativo solicitado.
El dispositivo de la capa de distribución se encarga de proporcionar un acceso controlado al núcleo.
Para construir una red de forma eficaz, es necesario entender en primer lugar cómo se utiliza el internetworking de redes, las necesidades corporativas y las demandas de los usuarios.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Estas necesidades pueden ser adaptadas a un modelo que pueda usarse para construir el internetworking de redes. Una de las mejores formas de comprender cómo construir un internetworking de redes pasa por asimilar la forma en que el tráfico circula a través de la red.
Esto se consigue por medio de un marco de trabajo de red conceptual, el más popular de los cuales es el modelo de referencia OSI.

Red pública de datos

Una red pública de datos, consiste en una red conmutada de comunicación de datos, muy similar a la red pública telefónica, pero con la particularidad de que esta sirve para transferir datos.
En la red pública, todos los datos que circulan por dichas redes son registrados y las condiciones en las que se presentan, son mucha más estrictas que en las privadas, por ello, esta serie de redes públicas son de mayor escasez.
Estas redes cubren distancias muy grandes y se les denomina redes WAN, ya que las distancias que pueden cubrir pueden ir desde los 100 km hasta los 1000 km, dando servicio a áreas regionales, a un país o incluso a un continente completo. Estas redes públicas de datos, combinan los conceptos de redes con valor agregado y redes de conmutación de paquetes.
Con el fin de entender un poco más, como se articulan las redes públicas de datos, vamos a ver una pequeña introducción a los conceptos que estas redes públicas combinan, que son los de valor agregado y de redes de conmutación de paquetes.

Conmutación de paquetes

La conmutación de circuitos es un sistema muy ineficiente ya que mantiene las líneas mucho tiempo ocupadas aun cuando no hay información circulando por ellas.
En conmutación de paquetes, los datos se transmiten en paquetes cortos. Para transmitir grupos de datos más grandes, el emisor trocea estos grupos en paquetes más pequeños y les añade una serie de bits de control. En cada nodo, el paquete se recibe, se almacena durante un cierto tiempo y se transmite hacia el emisor o hacia un nodo intermedio.
Las ventajas de la conmutación de paquetes frente a la de circuitos son:

- La eficiencia de la línea es mayor: ya que cada enlace se comparte entre varios paquetes que estarán en cola para ser enviados en cuanto sea posible. En conmutación de circuitos, la línea se utiliza exclusivamente para una conexión, aunque no haya datos a enviar.
- Se permiten conexiones entre estaciones de velocidades diferentes: esto es posible ya que los paquetes se irán guardando en cada nodo conforme lleguen (en una cola) y se irán enviando a su destino.
- No se bloquean llamadas: ya que todas las conexiones se aceptan, aunque si hay muchas, se producen retardos en la transmisión.
- Se pueden usar prioridades: un nodo puede seleccionar de su cola de paquetes en espera de ser transmitidos, aquellos más prioritarios según ciertos criterios de prioridad.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Red con valor agregado

Este concepto, hace mención a una red determinada, agrega valor a los servicios proporcionados, ya que este valor agregado a la red, proporciona nuevos servicios de comunicaciones a los ya existentes.
Podemos citar algunos ejemplos de valor agregado para las redes públicas de datos, como pueden ser:

- El control de los errores.
- La confiabilidad de conexión.
- Direccionamiento dinámico.
- Protección contra posibles fallos en las comunicaciones.
- Las conversiones oportunas para los formatos de datos.

En definitiva una VAN, como puede ser una organización u operador de telecomunicaciones, que alquile líneas de telecomunicaciones, y posteriormente tiene en su portfolio, una serie de redes que proporcionan valor agregado a esas líneas que han alquilado.
Estas redes con valor agregado, pueden llevar nombres distintos según la organización u el operador de telecomunicaciones en cuestión, pero lo verdaderamente importante, con independencia de los nombres que le sean asignados, es tener claro que estas redes, proporcionan servicios adicionales, como los que hemos tenido ocasión de citar más arriba.
Una red pública de datos, consiste en una red conmutada de comunicación de datos, muy similar a la red pública telefónica, pero con la particularidad de que esta sirve para transferir datos.
En la red pública, todos los datos que circulan por dichas redes son registrados y las condiciones en las que se presentan, son mucha más estrictas que en las privadas, por ello, esta serie de redes públicas son de mayor escasez.
Estas redes cubren distancias muy grandes y se les denomina redes WAN, ya que las distancias que pueden cubrir pueden ir desde los 100 km hasta los 1000 km, dando servicio a áreas regionales, a un país o incluso a un continente completo.
Estas redes públicas de datos, combinan los conceptos de redes con valor agregado y redes de conmutación de paquetes. Con el fin de entender un poco más, como se articulan las redes públicas de datos, vamos a ver una pequeña introducción a los conceptos que estas redes públicas combinan, que son los de valor agregado y de redes de conmutación de paquetes.

2.2. Servicios de interconexión con la red pública

Principios de la interconexión entre redes

Requisitos

- Proporcionar un enlace entre redes.
- Proporcionar encaminamientos y entrega de datos entre procesos de diferentes redes.
- Mantener un mecanismo de contabilidad y estado de redes y encaminamientos.
- Proporcionar estos servicios sin tener que cambiar la arquitectura de la red.

Para esto, los sistemas se tienen que acomodar a las diferencias entre las redes con:

- Diferentes esquemas de direccionamiento.
- Diferente tamaño máximo de bloque.
- Diferentes mecanismos de acceso a la red.
- Diferentes valores de expiración de los temporizadores.
- Recuperación de errores.
- Informes de estado.
- Técnicas de encaminamiento
- Control de acceso al usuario.
- Conexión, sin conexión

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Enfoques sobre la arquitectura

El modo de funcionamiento (en datagramas o en circuitos virtuales) determina la arquitectura de la red.

- Modo de funcionamiento con conexión
  Cuando se emplea este tipo de funcionamiento (generalmente en circuitos virtuales) cada sistema intermedio conecta dos subredes.
  Para pasar información desde un emisor hasta un receptor, ambos sistemas establecen un circuito lógico a través de una serie de sistemas intermedios.
  Estos sistemas intermedios son los mismos y únicos para cada conexión de los dos equipos conectados.
  Para los usuarios emisor y receptor, parece que la conexión es punto a punto. Para hacer esto posible, la capa de red del emisor, receptor y sistemas intermedios deben de proporcionar funciones similares.
- Modo de funcionamiento sin conexión
  En funcionamiento sin conexión (generalmente en datagramas) el emisor envía un bloque a la red y cada sistema intermedio repite el bloque para encaminarlo al sistema final. De esta forma, es posible que el mismo bloque llegue al destino varias veces y por distintos caminos.
  En cada unidad de encaminamiento se decide el mejor camino a seguir por cada bloque, independientemente de que pertenezca al mismo emisor y al mismo destino. Para esto, es necesario que todos los sistemas emisor, receptor e intermedios tenga un protocolo similar de red (IP).
- Enfoque utilizando puentes
  Mediante los puentes, es la capa MAC (debajo de la de red) la encargada de la retransmisión de los bloques. Para esto, los sistemas inicial y final deben compartir la capa de red y transporte. Además, todas las redes deben usar el mismo protocolo en la capa de enlace.

Servicios de interconexión con redes públicas

Redes de área amplia (WAN)

En las redes de área amplia, llamadas WAN en sus siglas inglesas, son redes destinadas a cubrir áreas geográficas muy extensas, que van desde 100 km hasta incluso los 1000 km, pudiendo cubrir un país entero o incluso todo un continente.
Las redes WAN, pueden ser desarrolladas e utilizadas por organizaciones, o proveedores de telecomunicaciones ICPs o ISPs (proveedor de servicios de internet). Esta red por lo general, funciona punto a punto, pudiendo emplearse en campos de radios y satelitales, empleándose sus ventajas para estos sistemas de comunicaciones.
La permisividad para interconectar redes a través de distintos medios como son la fibra óptica y el cableado de cobre, alcanzando velocidades que van desde 1 mbps hasta 1gbps, dependiendo de la tecnología empleada, son una muestra para establecer comunicaciones privadas, por todo el mundo, con una fiabilidad y una versatilidad para realizar modificaciones en software y hardware impresionante.

Ventajas de la red wan

–Utilizan software especial para la coexistencia de equipos pequeños y computadoras gigantescas.
–No tienen ningún límite de espacio, para su implementación y radio de acción.
–Ofrece una amplia gama de medios a usar para la transmisión de datos, como pueden ser enlaces satelitales, fibra óptica, cableado de cobre, etc.

Desventajas de la red wan

–Es necesario, emplear equipos con una gran capacidad de memoria y de procesamiento, ya que de estos equipos, depende la velocidad de acceso a la información.
–La red WAN, no destaca por medidas de seguridad importantes que ofrece a los usuarios de ella, ya que el software de carácter malicioso, es uno de los grandes males para la red WAN.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Tipos de wan

Existen 3 tipos de redes WAN, dentro del funcionamiento interno de la misma, basadas en la clasificación de red conmutada.
La permisividad para interconectar redes a través de distintos medios como son la fibra óptica y el cableado de cobre, alcanzando velocidades que van desde 1 mbps hasta 1gbps, dependiendo de la tecnología empleada, son una muestra para establecer comunicaciones privadas, por todo el mundo, con una fiabilidad y una versatilidad para realizar modificaciones en software y hardware impresionante.

Por circuitos

Para establecer una comunicación, este tipo de red WAN exige que se realice una llamada y justo cuando la conexión se efectúa cada usuario dispone de un enlace directo.

Por mensaje

Sus conmutadores suelen ser computadoras que cumplen la tarea de aceptar el tráfico de cada terminal que se encuentre conectado a ellas. Dichos equipos evalúan la dirección que se encuentra en la cabecera de los mensajes y pueden almacenarla para utilizarla más adelante. Cabe mencionar que también es posible borrar, redirigir y responder los mensajes en forma automática.

Por paquetes

Se fracciona cada mensaje enviado por los usuarios y se transforman en un número de pequeñas partes denominadas paquetes, que se vuelven a unir una vez llegan al equipo de destino, para reconstruir los datos iniciales.

Conmutación de circuitos

En conmutación de circuitos, los nodos intermedios no tratan los datos de ninguna forma, sólo se encargan de encaminarlos a su destino. En redes de comunicación conmutadas, los datos que entren en la red proveniente de alguna de las estaciones, son conmutados de nodo en nodo hasta que lleguen a su destino. Hay nodos sólo conectados a otros nodos y su única misión es conmutar los datos internamente a la red. También hay nodos conectados a estaciones y a otros nodos, por lo que deben de añadir a su función como nodo, la aceptación y emisión de datos de las estaciones que se conectan. Los enlaces entre nodos están multiplexados en el tiempo o por división de frecuencias.
Generalmente hay más de un camino entre dos estaciones, para así poder desviar los datos por el camino menos colapsado.
Para redes de área amplia, generalmente se utilizan otras técnicas de conmutación: conmutación de circuitos y conmutación de paquetes.

Redes de conmutación de circuitos

Para cada conexión entre dos estaciones, los nodos intermedios dedican un canal lógico a dicha conexión. Para establecer el contacto y el paso de la información de estación a estación a través de los nodos intermedios, se requieren estos pasos:
1.Establecimiento del circuito: el emisor solicita a un cierto nodo el establecimiento de conexión hacia una estación receptora. Este nodo es el encargado de dedicar uno de sus canales lógicos a la estación emisora (suele existir de antemano). Este nodo es el encargado de encontrar los nodos intermedios para llegar a la estación receptora, y para ello tiene en cuenta ciertos criterios de encaminamiento, coste, etc.
2.Transferencia de datos: una vez establecido el circuito exclusivo para esta transmisión (cada nodo reserva un canal para esta transmisión), la estación se transmite desde el emisor hasta el receptor conmutando sin demoras de nodo en nodo (ya que estos nodos tienen reservado un canal lógico para ella).
3.Desconexión del circuito: una vez terminada la transferencia, el emisor o el receptor indican a su nodo más cercano la finalización de la conexión, donde este le comunica al nodo más próximo la liberalización del canal, y así sucesivamente, hasta que todos los nodos, completan el proceso de desconexión total del circuito.
Debido a que cada nodo conmutador debe saber organizar el tráfico y las conmutaciones, éstos deben tener la suficiente “inteligencia” como para realizar su labor eficientemente. La conmutación de circuitos suele ser bastante ineficiente ya que los canales están reservados aunque no circulen datos a través de ellos.
Para tráfico de voz, en que suelen circular datos (voz) continuamente, puede ser un método bastante eficaz ya que el único retardo es el establecimiento de la conexión, y luego no hay retardos de nodo en nodo (al

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

estar ya establecido el canal y no tener que procesar ningún nodo ninguna información). La red pública de telefonía utiliza conmutación de circuitos.
Su arquitectura es la siguiente:
–Abonados: son las estaciones de la red.
–Bucle local: es la conexión del abonado a la red. Esta conexión, como es de corta distancia, se suele hacer con un par trenzado.
–Centrales: son aquellos nodos a los que se conectan los abonados (centrales finales) o nodos intermedios entre nodo y nodo (centrales intermedias).
–Líneas principales: son las líneas que conectan nodo a nodo. Suelen usar multiplexación por división en frecuencias o por división en el tiempo.
La conmutación de circuitos, a pesar de sus deficiencias es el sistema más utilizado para conectar sistemas informáticos entre sí a largas distancias debido a la profusión e interconexión que existe (debido al auge del teléfono) y a que una vez establecido el circuito, la red se comporta como si fuera una conexión directa entre las dos estaciones, ahorrando bastante lógica de control.

Conceptos sobre conmutación

Cada nodo de conmutación de circuitos consta básicamente de un conmutador digital, circuito que tiene una serie de conexiones al exterior (cada una es un canal) y una lógica de puertas interna que conecta unos canales con otros cuando se requieren estas conexiones. Por lo que dos canales conectados por el conmutador es como si estuvieran unidos sin interrupción.
El conmutador posee la lógica de control suficiente para conectar y desconectar canales conforme sea necesario.
Estos conmutadores deben permitir conexión full-duplex (típica en telefonía).
–El conmutador digital se compone de:
·Interfaz de red: incluye las funciones y hardware para conectar los dispositivos digitales (y analógicos) a la red.
·Unidad de control: establece, gestiona y corta las conexiones conforme se le requieran al sistema.
Hay dos tipos básicos de redes respecto a su capacidad o no de bloquear las comunicaciones entre dos estaciones:
–Bloqueantes: aquellas que impiden una conexión cuando no es posible dedicar canales para ella (por ejemplo en telefonía ya que no suele haber muchos teléfonos funcionando a la vez al ser las conexiones relativamente cortas).
–No bloqueantes: aquellas que siempre disponen de algún canal para cada conexión (esto debe ser así para conexiones entre sistemas informáticos en los que la conexión típica es de larga duración).

Conmutación de paquetes

En conmutación de paquetes, los datos se transmiten en paquetes cortos.
Para transmitir grupos de datos más grandes, el emisor trocea estos grupos en paquetes más pequeños y les adiciona una serie de bits de control.
En cada nodo, el paquete se recibe, se almacena durante un cierto tiempo y se transmite hacia el emisor o hacia un nodo intermedio.
Las ventajas de la conmutación de paquetes frente a la de circuitos son:
a)La eficiencia de la línea es mayor: ya que cada enlace se comparte entre varios paquetes que estarán en cola para ser enviados en cuanto sea posible. En conmutación de circuitos, la línea se utiliza exclusivamente para una conexión, aunque no haya datos a enviar.
b)Se permiten conexiones entre estaciones de velocidades diferentes: esto es posible ya que los paquetes se irán guardando en cada nodo conforme lleguen (en una cola) y se irán enviando a su destino.
c)No se bloquean llamadas: ya que todas las conexiones se aceptan, aunque si hay muchas, se producen retardos en la transmisión.
d)Se pueden usar prioridades: un nodo puede seleccionar de su cola de paquetes en espera de ser transmitidos, aquellos más prioritarios según ciertos criterios de prioridad.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Técnica de conmutación

Cuando un emisor necesita enviar un grupo de datos mayor que el tamaño fijado para un paquete, éste los trocea en paquetes y los envía uno a uno al receptor.
Hay dos técnicas básicas para el envío de estos paquetes:
–Técnica de datagramas: cada paquete se trata de forma independiente, es decir, el emisor enumera cada paquete, le añade información de control (por ejemplo número de paquete, nombre, dirección de destino, etc.) y lo envía hacia su destino.
Puede ocurrir que por haber tomado caminos diferentes, un paquete con número por ejemplo 6 llegue a su destino antes que el número 5. También puede ocurrir que se pierda el paquete número 4.
Todo esto no lo sabe ni puede controlar el emisor, por lo que tiene que ser el receptor el encargado de ordenar los paquetes y saber los que se han perdido (para su posible reclamación al emisor), y para esto, debe tener el software necesario.
–Técnica de circuitos virtuales: antes de enviar los paquetes de datos, el emisor envía un paquete de control que es de Petición de Llamada, este paquete se encarga de establecer un camino lógico de nodo en nodo por donde irán uno a uno todos los paquetes de datos. De esta forma se establece un camino virtual para todo el grupo de paquetes.
Este camino virtual será numerado o nombrado inicialmente en el emisor y será el paquete inicial de Petición de Llamada el encargado de ir informando a cada uno de los nodos por los que pase de que más adelante irán llegando los paquetes de datos con ese nombre o número.
De esta forma, el encaminamiento sólo se hace una vez (para la Petición de Llamada).
El sistema es similar a la conmutación de circuitos, pero se permite a cada nodo mantener multitud de circuitos virtuales a la vez.
Las ventajas de los circuitos virtuales frente a los datagramas son:
a)El encaminamiento en cada nodo sólo se hace una vez para todo el grupo de paquetes. Por lo que los paquetes llegan antes a su destino.
b)Todos los paquetes llegan en el mismo orden del de partida ya que siguen el mismo camino.
c)En cada nodo se realiza detección de errores, por lo que si un paquete llega erróneo a un nodo, éste lo solicita otra vez al nodo anterior antes de seguir transmitiendo los siguientes.
Desventajas de los circuitos virtuales frente a los datagramas:
a)En datagramas no hay que establecer llamada (para pocos paquetes, es más rápida la técnica de datagramas).
b)Los datagramas son más flexibles, es decir que si hay congestión en la red una vez que ya ha partido algún paquete, los siguientes pueden tomar caminos diferentes (en circuitos virtuales, esto no es posible).
c)El envío mediante datagramas es más seguro ya que si un nodo falla, sólo un paquetes se perderá (en circuitos virtuales se perderán todos).

Tamaño del paquete

–Un aumento del tamaño de los paquetes implica que es más probable que lleguen erróneos.
–Pero una disminución de su tamaño implica que hay que añadir más información de control, por lo que la eficiencia disminuye.
–Hay que buscar un compromiso entre ambos.

Comparación de las técnicas de conmutación de circuitos y conmutación de paquetes

Hay 3 tipos de retardo:
1.Retardo de propagación: tiempo despreciable de propagación de la señal de un nodo a otro nodo.
2.Tiempo de transmisión: tiempo que tarda el emisor en emitir los datos.
3.Retardo de nodo: tiempo que emplea el nodo desde que recibe los datos hasta que los emite (gestión de colas, etc.).
Las prestaciones de conmutación de circuitos y conmutación de paquetes:
–En conmutación de circuitos hay un retardo inicial hasta establecer la conexión (en cada nodo se produce un retardo). Tras el establecimiento de la conexión, existe el retardo del tiempo de transmisión y el retardo de propagación. Pero toda la información va a la vez en un bloque sin más retardos adicionales.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

–En conmutación de paquetes mediante circuitos virtuales, existe el mismo retardo inicial que en conmutación de circuitos. Pero además, en cada nodo, cada paquete sufre un retardo hasta que le llega su turno de envío de entre la cola de paquetes a emitir por el nodo. A todo esto, habría que sumar el retardo retransmisión y el retardo de propagación.
–En datagramas, se ahorra el tiempo de establecimiento de conexión, pero no los demás retardos que hay en circuitos virtuales. Pero existe el retardo de encaminamiento en cada nodo y para cada paquete.
Por tanto, para grupos grandes de datos, los circuitos virtuales son más eficaces que los datagramas, aunque para grupos pequeños sean menos eficaces que los datagramas.
Funcionamiento externo e interno
Hay dos niveles en donde se pueden utilizar técnicas de datagramas y de circuitos virtuales.
En un nivel interno (entre estación y nodo), se llaman operación de datagrama interno y operación de circuito virtual interno.
Pero cuan do se sale de este ámbito controlable por la estación emisora, la propia red decide la utilización de servicios de datagrama externo o servicio de circuito virtual externo para sus comunicaciones (ocultos al usuario o emisor).
Para los servicios externos hay una serie de consideraciones a seguir:
–Si se utilizan operaciones de datagrama interno y servicios de datagrama externo, al haber errores, no hay pérdidas de tiempo en establecer nuevas conexiones ni se necesitan muchos espacios de almacenamiento.
–Si se utilizan operaciones de circuitos virtuales internos y servicios de circuitos virtuales externos, se mejoran las prestaciones para transmisiones de grandes grupos de información y de acceso a terminales remotos.

ATM

Introducción al ATM

ATM (Asynchronous Transfer Mode), es una tecnología de conmutación de alta velocidad, que utiliza el método de la multiplexación por división en el tiempo asíncrona.
La unidad de información en ATM es la celda, que se caracteriza, por tener una longitud fija de 53 octetos. Esto permite que la conmutación de dichas celdas se realice por hardware, con lo que se consiguen velocidades de transmisión de hasta 622 Mbps.
Cada una de las celdas, está formada por una cabecera de 5 octetos, seguida por otros 48 octetos que contienen la información.
Dicha cabecera, contiene la información que permite identificar una comunicación, así como el tipo de información que transporta y la prioridad de descarte.
El Modo de Transferencia Asíncrono (ATM) es la tecnología para el despliegue de servicios troncales más extendida en la actualidad.
–Es utilizada tanto en el núcleo como en el acceso a sistemas de telecomunicación de alta velocidad.
–Permite ofrecer un contrato de servicio.
–Orientado a la conexión.
–Calidad del servicio (QoS) entre extremos garantizada.
–Escalable en velocidad y distancia.
–Utilizada tanto en WANs como en LANs de altas prestaciones.

Características del servicios ATM

a)Es una técnica de transferencia orientada a paquetes, en la que el flujo de información se organiza en bloques de tamaño fijo y pequeño (celdas).
b)No se garantiza la entrega al destino de todas las células generadas por una fuente de información.
c)Se garantiza la secuencia de entrega de las células transmitidas por el mismo circuito virtual.
d)No existe protección contra errores ni control de flujo en la transferencia entre enlaces.
e)Estos se realizan extremo a extremo entre los terminales de manera transparente a la red.
f)La cabecera de las celdas tiene una funcionalidad reducida:
·Identifica las células pertenecientes a la misma comunicación (circuito virtual).
·Las celdas se transfieren usando la técnica de multiplexación asíncrona por división en el tiempo.
·Orientado a la conexión: cada llamada se constituye en un canal virtual en el multiplex ATM.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

·La información de señalización va por un canal virtual diferente.

Conexiones ATM

–En cada conexión física ATM, pueden coexistir varios canales, estableciéndose un camino estable entre los dos extremos de la conexión (VC), y entregándose la información ordenadamente.
–Para distinguir a qué canal pertenece cada celda, se utiliza un mecanismo de direccionamiento que se identifica por un VPI y un VCI.
–El rango de VCI/VPI para conexiones de DTE, va desde 0.32 al 0.767.
–Estas direcciones tienen sentido local, y pueden variar en ambos extremos del circuito virtual.
–En el equipo de cliente, debe estar configurado coherentemente con el puerto al que accede, esto es, debe tener el mismo identificativo VCI/VPI.
–Las conexiones virtuales extremo a extremo, son PVC punto a punto, que se construyen por concatenación de VCC.

RDSI

La Red Digital de Servicios Integrados o RDSI, es la evolución de las redes telefónicas actuales.
Originalmente, todo el sistema telefónico estaba compuesto por elementos analógicos, y la voz era transportada por las líneas telefónicas modulada como una forma de onda analógica.
Posteriormente aparecieron las centrales digitales, que utilizan computadores y otros sistemas digitales.
Estas son menos propensas a fallos que las centrales analógicas y permiten además controlar más líneas de usuarios y realizar las conexiones mucho más rápidamente.
En estas centrales la voz se almacena y transmite como información digital, y es procesada por programas informáticos.
A la vez que se desarrollan las centrales digitales, también se produce un cambio en la comunicación entre centrales, que también pasa a ser digital, lo que permite mejorar en gran medida la calidad de las comunicaciones.
De esta forma, en la actualidad una comunicación por una línea telefónica convencional se realiza de forma analógica entre el equipo de un abonado y la central, pero de forma digital hasta llegar a la central donde está conectado el abonado destino.
La RDSI supone el último avance:
–La comunicación digital entre el abonado y su central telefónica.
–Esto supone una comunicación digital de extremo a extremo que conlleva un gran número de ventajas.
–Así, las recomendaciones de la serie I de la CCITT2 definen la RDSI como una red desarrollada a partir de la red telefónica que proporciona una conexión digital de extremo a extremo que soporta una gran variedad de servicios.
Ventajas que aporta la RDSI.
La RDSI ofrece gran número de ventajas, entre las que se pueden destacar las siguientes:
–Velocidad: Actualmente el límite de velocidad en las comunicaciones a través de una línea telefónicas empleando señales analógicas entre central y usuario mediante el uso de módems está alrededor a los 56Kbps.
–En la práctica las velocidades se limitan a unos 45Kbps debido a la calidad de la línea. Además, todavía no se datado un estándar definitivo para comunicaciones a 56Kbps (actualmente se está desarrollando el V.90).
La RDSI ofrece múltiples canales digitales que pueden operar simultáneamente a través de la misma conexión telefónica entre central y usuario; la tecnología digital está en la central del proveedor y en los equipos del usuario, que se comunican ahora con señales digitales.

Este esquema permite una transferencia de datos a velocidad mucho mayor.
Así, con un servicio de acceso básico, y empleando un protocolo de agregación de canales, se puede alcanzar una velocidad de datos sin comprimir de unos 128 Kbps.
Además, el tiempo necesario para es establecer una comunicación en RDSI es cerca de la mitad del tiempo empleado con una línea con señal analógica.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

–Conexión de múltiples dispositivos: Con líneas analógicas resulta necesario disponer de una línea por cada dispositivo del usuario, si estos se quieren emplear simultáneamente. Resulta muy caro enviar datos (archivos o vídeo) mientras se mantiene una conversación hablada.
Por otra parte, se requieren diferentes interfaces para emplear diferentes dispositivos al no existir estándares al respecto.
Con la RDSI es posible combinar diferentes fuentes de datos digitales y hacer que la información llegue al destino correcto.
Como la línea es digital, es fácil controlar el ruido y las interferencias producidos al combinar las señales.
Además, las normas de la RDSI especifican un conjunto de servicios proporcionados a través de interfaces normalizados.
–Señalización: La forma de realizar un llamada a través de una línea analógica es enviando una señal de tensión que hace sonar la "campana" en el teléfono de destino.
·Esta señal se envía por el mismo canal que las señales analógicas de sonido.
·Establecer la llamada de esta manera requiere bastante tiempo.
·Por ejemplo, entre 30 y 60 segundos con la norma V.34 para módems.
En una conexión RDSI, la llamada se establece enviando un paquete de datos especial a través de un canal independiente de los canales para datos.
Este método de llamada se engloba dentro de una serie de opciones de control de la RDSI conocidas como señalización, y permite establecer la llamada en un par de segundos.
Además informa al destinatario del tipo de conexión (voz o datos) y desde que número se ha llamado, y puede ser gestionado fácilmente por equipos inteligentes como un ordenador.
–Servicios: La RDSI no se limita a ofrecer comunicaciones de voz. Ofrece otros muchos servicios, como transmisión de datos informáticos (servicios portadores), télex, facsímil, videoconferencia, conexión a Internet y opciones como llamada en espera, identidad del origen, etc.
Los servicios portadores permiten enviar datos mediante conmutación de circuitos (con un procedimiento de llamada se establece un camino fijo y exclusivo para transmitir lo datos en la red, al estilo de las redes telefónicas clásicas) o mediante conmutación de paquetes (la información a enviar se divide en paquetes de tamaño máximo que son enviados individualmente por la red).

Redes de área local (LAN):
Una red de área local es un conjunto de equipos (ordenadores, impresoras, faxes e incluso centralitas telefónicas y otros dispositivos electrónicos) unidos un medio de transmisión, generalmente cable UTP, de manera que todos esos equipos puedan intercambiar información.
Las principales características por las que se clasifica un tipo de redes de datos como redes LAN son:
1.La distancia máxima entre los equipos a conectar está en el rango de las centenas de metros.
2.La capacidad de transmisión es muy grande, generalmente mucho mayor que la de las redes de área extensa, siendo las velocidades habituales entre 10 y 100 Mbps, alcanzando actualmente las más rápidas hasta 1 Gbps.
3.Los componentes que las forman (equipos hardware y software) son de propiedad particular así como los edificios y locales donde están ubicados dichos componentes; todo lo contrario ocurre con muchas de las redes de área extensa.
4.Los errores introducidos en la transmisión de los datos son menores que en las redes de área extensa. Son típicas tasas de error de 1 bit por cada 108, mientras que en las redes de área extensa son habituales errores de 1 bit por cada 105.
Todas estas definiciones actualmente están un poco desfasadas.
Las LAN actuales pueden conectar a equipos separados por grandes extensiones.
Además la capacidad de transmisión de las WAN ha aumentado considerablemente, y su tasa de errores se ha reducido.
Por todo lo comentado sería más conveniente diferenciar entre redes LAN y WAN como sigue:
–La red local es de propiedad del cliente, mientras la red de área amplia es gestionada por un operador de red que ofrece sus servicios públicos de conectividad y transporte de información.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

–Las redes de área local facilitan la comunicación de un gran número de equipos y aplicaciones a las organizaciones en un entorno reducido, mientras que las redes de área extensa interconectan a estas LAN permitiendo el intercambio de información entre sitios que están distantes geográficamente.
–Una red de área local es un conjunto de equipos (ordenadores, impresoras, faxes e incluso centralitas telefónicas y otros dispositivos electrónicos) unidos un medio de transmisión, generalmente cable UTP, de manera que todos esos equipos puedan intercambiar información.

2.2.1. Parámetros: alimentación eléctrica, sujeción mecánica, otros

Fuentes de alimentación eléctrica

Proceso de transformación de la corriente eléctrica, dentro de la fuente de alimentación

1.Transformación
Se reduce la tensión de entrada a la fuente (220V o 115V) que son los que corresponden a la red eléctrica domiciliaria. En esta parte del proceso de la transformación, se realiza con un transformador. La tensión de la salida de este proceso generará valores de 5 a 12 Volts.
2.Rectificación
La corriente de la red eléctrica domiciliaria es alterna, esto quiere decir, que sufre variaciones en su línea de tiempo, con variaciones, nos referimos a variaciones de tensiones, por tanto, su amplitud no siempre es la misma.
Las tensiones de alimentación son de nivel de continua, similar al de las baterías o pilas. Se utiliza un convertidor de alterna a continua, este dispositivo se llama rectificador.
3.Filtrado.
La corriente continua obtenida por el proceso de rectificación debe ser mejorada para lograr una continua libre de fluctuaciones de amplitud. Mediante circuitos especiales, llamados filtros, se logra esto.
4.Estabilización.
La tensión de la salida de la fuente puede cambiar, si se modifica la entrada. Si baja la tensión de entrada (brownout), o sea por ejemplo de 220 V descienda a 190 V, las salidas se mantengan dentro de los 5,3.3 ó 12 VDC.
–Las tensiones de la fuente sirven para:
·12 V.- Motores y para transformar a otros niveles de tensión.
·5 V.- Procesos de datos, algunos motores de ventilación y alimentación en general (USB).
·3.3 V.- Procesamiento de datos y transformar.

Tipos de Fuentes

Podemos encontrar dos tipos de fuentes:
–1. AT (Advanced Technology).
–2. ATX (AT eXtended).
Las fuentes de alimentación AT, fueron usadas hasta que apareció el Pentium MMX, es en ese momento cuando ya se empezarían a utilizar fuentes de alimentación ATX.
Las características de las fuentes AT, son que sus conectores a la motherboard varían de los utilizados en las fuentes ATX, y por otra parte, quizás bastante más peligroso, es que la fuente se activa a través de un interruptor conectado directamente a los 220 V.
Además un problema que existía sobre la dos conectores que alimentaban a la motherboard, con lo cual podía dar lugar a confusiones y a cortocircuitos, la solución a ello es basarse en un truco muy sencillo, hay que dejar en el centro los cables negros que los dos conectores tienen, así no hay forma posible de equivocarse.
Las fuentes ATX no disponen de un interruptor que enciende/apaga la fuente, si no que se trata de un pulsador conectado a la MOTHERBOARD, y esta se encarga de encender la fuente, esto conduce a que se puedan realizar conexiones o desconexiones mediante software.
Otras de las características es que siempre están activa aunque la PC se encuentre apagada, mantiene un nivel pequeño de alimentación para mantenerla en espera.
La tensión aparece con la designación VSB (Volts Stand By), esto la PC se encienda a una hora determinada, o encenderlo pulsando una tecla del teclado, moviendo el ratón.
–Tipos de conectores de la fuente

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Molex es un fabricante de componentes electrónicos y conectores. Comúnmente se denomina como Molex a determinados conectores internos. Se utilizan en periféricos que necesiten más consumo de corriente que el que puede facilitar el cable de datos tales como:
·Discos duros (IDE, SCSI y los SATAs).
·Unidades ópticas (CD,DVD y Blu-Ray).
·Placas de video (Geforce Serie 5 y 6, Placas PCI y AGP).
·Sistemas de refrigeración (aire o líquido).
·Circuitos para modding (del inglés "modify": modificar), es la técnica de modificar la estética o funcionalmente partes de las computadoras, ya sea la torre, ratón, teclado o monitor, y en especial los componentes de los videojuegos, como pueden ser las consolas.
Puede referirse tanto a las modificaciones al hardware como al software de las mismas, aunque este último también puede llamarse "chipping". En este caso para el uso de este tipo de conectores en los circuitos de modding tenemos a: Diodos luminosos, tubos de luz, etc.
Se encuentran en la fuente conectores del tipo molex: un conector macho y un conector hembra.
Los conectores hembra se utilizan para bifurcar las salidas y dividirlas en dos pero la mayoría de las veces están integradas a los PCB (Printed Circuit Board –circuito impreso) de los mismos periféricos.
–Selección de una Fuente de Alimentación
Las computadoras actuales cada vez consumen más potencia (aunque también son más eficientes en cuanto a consumo, es decir que un equipo actual es más rápido que otro de hace unos años, sin embargo tiene un consumo en "Watt" similar) por lo que es necesario usar una fuente de alimentación que pueda suministras suficiente energía, a fin de evitar posibles problemas (ejemplos: bloqueos, reinicios o bien posibles daños al equipo en especial en la propia fuente).
Es importante conocer el consumo de cada uno de los componentes, como es necesario que también hay dispositivos que no accionan simultáneamente por lo que da ciertos márgenes con relación al consumo máximo. Las fuentes actuales tienen PCF activo, pero en las más antiguas encontramos PFC Pasivo.
–Consideraciones para seleccionar una fuente
No debe valorar solamente por los watts que se indican en la venta del producto, sino por otras características como son:
·La relación Watt/Amper que pueda entregar en todas sus líneas: +3,3V; +5V; +12V; -5V (usados en las antiguas tarjetas ISA[1]-12V y +5Vsb.
·A mayor potencia, supone una gran cantidad de corriente.
·El tipo de PFC que posea, ya que las que lo llevan activo suelen tener una relación Watts/Amperios superior a las que son del tipo pasivo a igualdad de Watts.
·El certificado para norma ATX[1]siendo el último a la fecha la versión 2.20 del año 2.005.
·Certificaciones para uso de simultaneidad de los siguientes componentes:
·Para el uso de Procesadores Dual[2]de 65W/Quad[3]Core de 120 W (Procesadores de dos o cuatro núcleos).
·Sistemas " Scalable Link Interface"(SLI) de nVidia para usar dos gráficas simultáneas. (Actualmente algunas placas base de gama alta admiten QuadSLI usando tarjetas gráficas con doble GPU[4]como es el caso de la nVidia GTX295 (consume unos 290W).
Hay que tener en cuenta que montar un SLI con:
–Dos GTX295 que tienen un consumo total de unos 580w (cada una consume unos 290W).
–Sistemas Crossfire (CF) de Ati para usar dos gráficas simultáneas.
Hay que tener en cuenta que montar un CF con:
–Dos Ati HD4870 x2 que tienen un consumo total de unos 572 W (cada una consume unos 286 W).
–Sistema de "protección" contra sobrecargas y/o sobretensiones dentro de un margen pero ante situaciones puntuales es lo más efectivo para esto es un Sistema Ininterrumpible de Energía "SIE" (en inglés: Uninterruptible Power Supply "UPS"), aunque internamente, mediante electrónica, se logre buenos resultados pero hasta ciertos niveles energéticos.
–El tipo y cantidad de conectores que se dispongan.
–La longitud de los cables de los conectores, puedan ser de corta longitud para algunos gabinetes, lo que será necesario la utilización de prolongadores de cables. Es necesario recordar que no deben nunca estar tensos o molesten para cualquier tipo de manipulación interna del equipo.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

–La refrigeración, si es o no silenciosa implica un valor agregado, como además que la misma siga funcionando al apagar sigue la PC para sacar el calor residual.
–La garantía, normalmente estos productos tienen 2 años de garantía, sin embargo algunos fabricantes especifican períodos de garantía mayores.
–El peso (Kilogramos) de la fuente, las fuentes genéricas no suelen pesar poco con respecto a las de buena calidad que se encuentra entre 1,75 y 2,75 kilogramos aproximadamente.
–Tiempo medio entre fallos (MTBF), es el tiempo de vida estimado del producto antes de fallar, normalmente viene expresado en miles de horas (entre 100.000 y 150.000 horas) y con una carga determinada o una temperatura concreta; en principio a menor carga y/o temperatura de funcionamiento mayor tiempo de vida (Horas MTBF) estimado.
Extras útiles como pueden ser:
–Cables recubiertos por una malla (se supone que ocupan menos y son más "manejables").
–Sistema de conexión modular (esto es relativo; permite añadir conexiones a la fuente según las necesidades).
–Tener un interruptor que corte la energía (lamentablemente, no todas tienen este interruptor).
–Extras decorativos (Modding): Efecto UV (Ultravioleta); Carcasas traslúcidas; Ventiladores con Leds (Luces). Esto último es más bien relativo ya que no mejora el rendimiento del equipo.

Alimentación eléctrica a través de ethernet (POE)

La alimentación a través de Ethernet (PoE) es un mecanismo para suministrar alimentación eléctrica a los dispositivos de red por medio del mismo cable usado para el tráfico de red.
POE permite a los dispositivos que requieren alimentación, denominados dispositivos alimentados (PD), como teléfonos IP, puntos de acceso de redes de área local inalámbricas (LAN) y cámaras de red, recibir al mismo tiempo alimentación eléctrica y datos a través de la misma infraestructura existente.
No es necesaria ninguna mejora de la infraestructura.
Esta característica puede simplificar la instalación y el mantenimiento de una red usando el switch como fuente de alimentación central para otros dispositivos de la red. El reto durante la instalación es calcular el consumo total de energía necesaria de modo que sea menor que las capacidades de alimentación del switch.
–Existen dos estándares para PoE en la actualidad:
·802.3af permite un máximo de 15,4 W por canal, mientras que PoE 802.at duplica la potencia disponible a 25 W.
·La potencia total de las necesidades de consumo de todo el equipo que se conectará a un switch específico en una red debe calcularse necesariamente para garantizar la disponibilidad de alimentación suficiente por switch.
·Los requerimientos de potencia total deben ser menores que las capacidades de alimentación de un switch PoE (potencia PoE total por switch y por puerto).

Estructuras abiertas: bastidores, rack, bracket

–Brackets o rack de pared: Se denominan así a las estructuras abiertas que se montan sobre la pared, este tipo de bastidor puede tener las siguientes características, es importante destacar que el ancho del bastidor está estandarizado a 19" o 48.26 cm.
Pueden ofrecerle brackets de pared con las siguientes características:

Bracket de pared de 19"				
Altura	4 RU	6 RU	8 RU	10 RU
Profundidad en mm	203	330	457	610

·Fabricados 100% de acero laminado en frío.
·Rieles de montaje perforados con forma cuadrada o redonda con rosca conforme a normas EIA patrón 12-24, paso estándar de agujeros de paso 5/8"- 5/8" - 1/2".

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

·Todas las piezas que lo requieran se someten a procesos de desengrasado, fosfatado y cincado electrolítico asegurando el cumplimiento de las normas A.S.T.M. de impacto, flexibilidad y adherencia así como de resistencia al medio ambiente.
·Terminación en pintura electrostática (Electro Posición Catódica) en polvo Poliéster Epódica de máxima adherencia alta resistencia mecánica y química. Ofrece una resistencia cinco veces mayor al óxido y ralladuras que los sistemas tradicionales de pintura.
Desventajas
a)Los equipos activos (switches, routers, etc.) así como los cables quedan expuestos completamente al polvo y humedad, por lo que es conveniente prever un régimen de mantenimiento más frecuente.
b)Está expuesto a acciones vandálicas, las conexiones en los equipos o en los paneles de empalme (patch panel) pueden ser modificadas por cualquier persona.
Ventajas
a)Menor coste.
b)No requiere ventiladores.
c)Más fácil de administrar y mantener, al contar con mayor acceso a todos los puntos de conexión.
–Rack de piso: Se denominan así a las estructuras abiertas que son ancladas al piso, por eso es posible contar con bastidores de mayor tamaño, en este caso no es necesario considerar la profundidad a diferencia de los bastidores (brackets o racks de pared).
El Rack de piso es una solución económica de alta capacidad para colocar los equipos de red y sus cables, es posible incluir también el cableado de la telefonía.

Se cuenta con los siguientes tipos de bastidores de piso (Rack de piso)
Rack de Piso de 19” x 45 RU
Rack de Piso de 19” x 38 RU
Rack de Piso de 19” x 24 RU
Especificaciones técnicas del rack de piso:
·Normalizados en 19”.
·Totalmente desarmables y de fácil acceso.
·Entrada de cables por base.
·Base tipo pedestal con agujeros para anclaje al piso.
·Fabricados 100% en acero laminado en frío.
·Agujeros laterales para conectar rack’s en serie.
·Rieles de montaje perforados con forma redonda con rosca conforme a normas EIA patrón 12-24, paso estándar de agujeros de paso 5/8”- 5/8” - 1/2”, por sus dos caras.
·Ensamblados con pernos y tuercas de acero inoxidable mejorando notablemente la apariencia.
·Carga máxima de soporte 500 Kg (depende del modelo elegido).
·Tornillos para montaje de equipos incluidos.
·Todas las piezas que lo requieran se someten a procesos de desengrasado, fosfatado y cincado electrolítico asegurando el cumplimiento de las normas A.S.T.M. de impacto, flexibilidad y adherencia así como de resistencia al medio ambiente.
·Terminación en pintura electrostática (Electro Posición Catódica) en polvo Poliéster Epódica de máxima adherencia alta resistencia mecánica y química. Ofrece una resistencia cinco veces mayor al óxido y ralladuras que los sistemas tradicionales de pintura.
·Acabado en color Negro RAL 9005.
·Disponibles en gama liviana (económico) o pesada (premier).
·Se deben fijar al piso mediante 4 bujes de expansión.

Estructuras cerradas: cabinet

Una estructura cerrada tiene mayores ventajas que una abierta, ya que ofrece seguridad, protección contra el medio ambiente, permite dirigir mejor la ventilación y circulación del aire enfriado. También es posible elegir entre modelos de pared o de piso, dependiendo de las facilidades de espacio, peso y densidad de concentración que requiere la red de datos.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

–Gabinetes de pared: Los gabinetes de pared cuentan con un marco posterior con bisagra y chapa con llave que permite abrir el armazón principal por la parte posterior facilitando la labor de anclaje, luego de realizado el trabajo se coloca la llave para una mayor seguridad, adicionalmente cuenta con una puerta frontal con llave y cristal de seguridad que permite ver el interior del gabinete.
Entre sus principales características tenemos:
·Normalizados en 19".
·Fabricados en una sola pieza garantizando un excelente desempeño en capacidad y fortaleza.
·Desarmables y de fácil acceso.
·Puerta frontal ventilada, provista con cristal de seguridad y chapa más llave.
·Entrada de cables por base y/o techo.
·Fabricados 100% en acero laminado en frío.
·Paneles laterales ventilados en la parte superior e inferior, chapa en bajo relieve.
·Rieles de montaje perforados con forma cuadrada para tuercas enjauladas o roscada conforme a normas EIA patrón 12-24, paso estándar de agujeros de 5/8"- 5/8" - 1/2". Tornillos para montaje de equipos incluidos.
·Ajustadores de posición de columnas de montaje con 4 guías laterales corredizas de agujeros fijos.
·Todas las piezas que lo requieran se someten a procesos de desengrasado, fosfatado y cincado electrolítico asegurando el cumplimiento de las normas A.S.T.M. de impacto, flexibilidad y adherencia así como de resistencia al medio ambiente.
·Terminación en pintura electrostática (Electro Posición Catódica) en polvo Poliéster Epódica de máxima adherencia alta resistencia mecánica y química, Ofrece una resistencia cinco veces mayor al óxido y ralladuras que los sistemas tradicionales de pintura.
–Gabinetes de piso: Los gabinetes de piso son estructuras metálicas muy funcionales para alojar los dispositivos de red, vienen en diferentes tamaños y profundidades así como en grosor de la lámina metálica, por lo cual es posible encontrar el gabinete adecuado para cada necesidad.
·El gabinete de piso cuenta con un bastidor (rack) interno que realiza la función mecánica de soportar los dispositivos que se coloquen. El peso acumulado de un gabinete de piso con todo su equipamiento puede ser de cientos de kilos.
Características:
·Normalizado en 19" de ancho por 45RU (Área efectiva de alto).
·Entrada de cables por base y techo con perforación pre cortada, para hacer uso de esta en caso de que se necesite, con protector de jebe para proteger los cables de los filos. Fabricado 100% en acero laminado en frío ASTM A366.
·Estructura de tipo multipliegue con perforaciones laterales, frontal y posterior en techo y base para su correcta ventilación. Los gabinetes están habilitados por medio de un sistema para la sujeción en fila para que sean unidos unos con otros.
·Barra de tierra Vertical x 45 RU de 30 x 5 mm con 50 terminales de doble ojo Marca Panduit de diferentes calibres en la parte trasera del Gabinete tanto al lado derecho como en izquierdo.
·Incluye cuatro Rieles de montaje multi perforados para sujeción de diversos elementos.
·Acondicionado con mallas de protección incorporadas para la colocación de extractores de aire en la plancha.
·8 ajustadores de posición de columnas de montaje laterales, cada uno provisto para el ordenamiento de 80 cables de manera vertical tanto en el interior como en el exterior los cuales pueden ser cambiados de posición dependiendo del volumen de cables a ordenar o del peso de los equipos a soportar los cuales están sujetados con 8 pernos y tuercas enjauladas, así mismo pueden colocarse más ajustadores de posición según se requiera.
·20 anillos organizadoras de cables en los extremos.
·Perforaciones estándar según Norma EIA de perforación cuadrada y serigrafiados con medidas RU, paso estándar de agujeros de 5/8" - 5/8" - 1/2" NORMA ANSI-EIA-310-D.
·Barras de energía de 10 enchufes cada uno de tipo 2P+T de tierra aislada certificados, con punto a tierra en carcasa Metálica y recubrimiento anti flama y autoextingible.
·Carga máxima de soporte 900 Kg (CERTIFICADO).

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

·Todas las piezas se someten a procesos de desengrasado, fosfatado químico por conversión asegurando el cumplimiento de las normas A.S.T.M. de impacto, flexibilidad y adherencia así como de resistencia al medio ambiente.
·Terminación en pintura electrostática (Electro Posición Catódica) en polvo Poliéster de máxima adherencia, alta resistencia mecánica y química, de tipo auto extinguible según norma ASTM E-136 y Clase A para propagación de llama y desarrollo de humos ASTM-E84. Ofrece una resistencia cinco veces mayor al óxido y ralladuras que los sistemas tradicionales de pintura.
·40 Tornillos + Tuercas enjauladas + arandela plástica para montaje de equipos (cage nut and screw).

2.2.2. Requerimientos de interconexión. Normativa de calidad

La normativa de calidad con respecto a los requerimientos de interconexión, la explotación de las redes, la prestación de servicios por medios de comunicaciones electrónicas, junto con los recursos asociados que pudieran ser procedentes a la regulación de la ley 9/2014 de 9 de Mayo general de Telecomunicaciones, y de conformidad con el artículo 149.1.21 de la Constitución española, son de claro objetivo para la aplicación de la citada ley y las que pudieran darse lugar tras las modificaciones oportunas que se sucedan.
Antes de adentrarnos en la propia materia, es imprescindible realizar las indicaciones oportunas como una hoja de ruta, del camino que ha seguido esta ley desde sus inicios, y los reales decretos que la han modificado, además de las directrices por parte de la Unión Europea que se dictaron en su momento, que con ellas, dieron lugar a la citada ley, como mecanismo de transposición de las diferentes directrices europeas en materia de telecomunicaciones.
Desde la aprobación de la ley 32/2003 de 3 de Noviembre, general de Telecomunicaciones, que tuvo su origen dentro del marco regulador europeo de las comunicaciones electrónicas del año 2002, tuvo múltiples modificaciones (la última mediante el real decreto 13/2012) con el firme compromiso de garantizar la creación y viabilidad de nuevos operadores, la protección de los derechos de los usuarios y todos aquellos aspectos que tengan relación con el dominio público o servicio, junto con la defensa de la competencia y calidad en las interconexiones de redes.
La presente Ley regula, asimismo, otras cuestiones como la instalación de equipos y sistemas, la interceptación legal de las telecomunicaciones, la conservación de datos, o la evaluación de conformidad de equipos y aparatos, temas que a nivel comunitario son objeto de normativa específica. Por otro lado, en la citada ley, podemos encontrar en el título IV, en lo relativo a la evaluación de la instalación de aparatos y sistemas, se regulan aspectos como normalización técnica, la conformidad de los aparatos y sistemas, junto con las condiciones y requerimientos que deben de cumplir las instalaciones.
Con respecto a las normativas técnicas, el artículo 11 de la citada ley, cita expresamente el uso de normas o recomendaciones internacionales como son la Unión Internacional de Telecomunicaciones (ITU), la Conferencia Europea de Administraciones de Correos y Telecomunicaciones (CEPT), la Comisión Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (CEI), serán de aplicación, en ausencia de normativa reguladora nacional, cuyas bases sean sentadas por la Comisión Europea para fomentar el suministro y servicios de comunicaciones electrónicas, en los ámbitos de acceso e interconexión, garantizándose las pertinentes normas o especificaciones técnicas.
Dichas normas o especificaciones de conformidad con la normativa Europea, serán modificadas mediante real decreto, para determinar las formas de elaboración y adopción de las pertinentes normas. A continuación, presento una relación de los diferentes organismos de normalización para la interconexión de redes.

–Unión Internacional de Telecomunicaciones (UIT), fundada en 1865, es la más universal.
Es el principal organismo encargado de la emisión de normas de las telecomunicaciones. Es muy compleja y extensa y desde 1992 consta de tres subsectores: ITU-I Unión Internacional de Telecomunicaciones - sector telecomunicaciones.
–ITU-R Unión Internacional de Telecomunicaciones - sector comunicaciones de radio.
–ITU-D Unión Internacional de Telecomunicaciones - sector desarrollo.
–La Organización Internacional de Normalización (ISO) integrada por usuarios y fabricantes.
Ha definido un modelo de referencia que establece unas normas para interconectar diferentes equipos y posibilitar su comunicación.
–El Institución de Ingenieros Eléctrico y Electrónicos (IEEE) colabora en el desarrollo de estándares.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Últimamente centrados en los estándares que desarrollan el nivel 1 y 2 del modelo OSI (802.3, 802.4, 802.5).
–El Instituto Americano de Estándares Nacionales (ANSI) que coordina la estandarización del sector privado. Colabora con el ISO.

La ley general de telecomunicaciones

Desde la aprobación de la ley 32/2003 de 3 de Noviembre, general de Telecomunicaciones, que tuvo su origen dentro del marco regulador europeo de las comunicaciones electrónicas del año 2002, tuvo múltiples modificaciones (la última mediante el real decreto 13/2012) con el firme compromiso de garantizar la creación y viabilidad de nuevos operadores, la protección de los derechos de los usuarios y todos aquellos aspectos que tengan relación con el dominio público o servicio, junto con la defensa de la competencia y calidad en las interconexiones de redes.
La presente Ley regula, asimismo, otras cuestiones como la instalación de equipos y sistemas, la interceptación legal de las telecomunicaciones, la conservación de datos, o la evaluación de conformidad de equipos y aparatos, temas que a nivel comunitario son objeto de normativa específica.
En la citada ley, podemos encontrar en el título IV, en lo relativo a la evaluación de la instalación de aparatos y sistemas, se regulan aspectos como normalización técnica, la conformidad de los aparatos y sistemas, junto con las condiciones y requerimientos que deben de cumplir las instalaciones.
Con respecto a las normativas técnicas, el artículo 11 de la citada ley, cita expresamente el uso de normas o recomendaciones internacionales como son la Unión Internacional de Telecomunicaciones (ITU), la Conferencia Europea de Administraciones de Correos y Telecomunicaciones (CEPT), la Comisión Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (CEI), serán de aplicación, en ausencia de normativa reguladora nacional, cuyas bases sean sentadas por la Comisión Europea para fomentar el suministro y servicios de comunicaciones electrónicas, en los ámbitos de acceso e interconexión, garantizándose las pertinentes normas o especificaciones técnicas.

2.2.3. Interfaces en función de la tipología de red

En la interconexión de redes, las interfaces más habituales son:
–Ethernet 10BASET
–FastEthernet 100BASETX
–FastEthernet 100BASEFX
–Ethernet 1000-BASE-LX
–Ethernet 1000-BASE-SX
–Ethernet 1000-BASE-ZX
–Ethernet 1000-BASE-T
–Interfaz WAN Serial (Interfaz DSL WAN, Interfaz T1, E1 WAN, Interfaz V.92 modem WAN)
–Interfaz ISDN - BRI WAN
Los veremos con mas detenimiento en el capítulo 3

2.2.4. Normativas de seguridad

En la normativa de seguridad en los servicios de interconexión, existen diversas leyes o normativas legales relevantes, que hay que tener muy en cuenta, a la hora de la implantación y aplicación de los servicios de interconexión.
Podemos citar:
–Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (LOPD)
Esta ley, las medidas que adopta, son la protección y seguridad de todos los datos de carácter personal, con medidas idóneas, técnicas y organizativas, que garanticen la debida seguridad y eviten la alteración, pérdida, tratamiento o acceso no autorizado a la información de carácter personal.
Con esta norma, se trata de garantizar la seguridad en los ficheros, los centros encargados de su tratamiento, edificios, sistemas, equipos y programas que intervengan de alguna forma en el tratamiento de la información de carácter personal. Las Medidas de Seguridad vienen reguladas en el título VIII del Reglamento de desarrollo de la LOPD -Real Decreto 1720/2007, de 21 de diciembre (artículos 79 a 114).
Este Reglamento de desarrollo de la LOPD clasifica las Medidas de Seguridad atendiendo a dos criterios:
·Según los niveles de seguridad: Medidas de Seguridad de nivel básico, medio y alto.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

·Según la aplicación de las Medidas de Seguridad a ficheros y tratamientos automatizados o no automatizados.
–Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
En este Real Decreto, es donde se desarrolla el contenido de la LOPD, y las medidas de seguridad vienen reguladas en el título VIII del Reglamento de desarrollo de la LOPD -Real Decreto 1720/2007, de 21 de diciembre (artículos 79 a 114).
Este Reglamento de desarrollo de la LOPD clasifica las Medidas de Seguridad atendiendo a dos criterios: Según los niveles de seguridad: Medidas de Seguridad de nivel básico, medio y alto. Según la aplicación de las Medidas de Seguridad a ficheros y tratamientos automatizados o no automatizados.
–Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
–Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
El Real Decreto 3/2010 y el 4/2010 del 8 de Enero, regulan toda la política de seguridad que ha de tenerse en cuenta, en la utilización de los medios electrónicos, junto con los criterios y recomendaciones de seguridad y normalización de la información, además de los formatos y aplicaciones que han de tenerse en cuenta en los servicios de interconexión por parte de las administraciones públicas. Estas son en concreto normativas de seguridad en los servicios de interconexión por parte de las Administraciones Públicas.

Legislación europea

En materia de seguridad en los servicios de interconexión, se reseña 2 normativas legales relevantes al respecto:
–Directiva 2009/136/CE/ del Parlamento Europeo y del Consejo, de 25 de noviembre.
–Directiva 2009/140/CE del Parlamento Europeo y del Consejo, de 25 de noviembre.
En relación a la directiva 2009/136/CE, que modifica la anterior directiva 2002/22/CE, regula los servicios universales y los derechos de los usuarios, en relación con las redes y con los servicios de comunicaciones electrónicas.
En materia de protección de datos personales, tenemos la directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad, en las comunicaciones electrónicas.
Cabe destacar la directiva 2009/140/CE que modifica la directiva 2002/21/CE, en relación a la regulación mediante un marco común regulatorio, en materia de redes y servicios de comunicaciones electrónicas.
La directiva 2002/19/CE, es la norma europea relativa al acceso a las redes de comunicaciones electrónicas y recursos vinculantes a dichos accesos, y a la interconexión de todas las redes, sean públicas o privadas.
Por último, cabe destacar la directiva 2002/20/CE, relativa a la autorización de redes y servicios de comunicaciones electrónicas.

2.3. Arquitectura de un dispositivo de interconexión de redes

Componentes hardware

Dependiendo de la arquitectura del router, el procesador, el sistema de memorias y los controladores de interfaz, cada modelo de equipo posee unas características diferentes. Vamos a centrarnos en la arquitectura de los routers de gama baja denominados Shared Memory que aunque individualmente tienen sus propias características, juntos tienen dos cosas en común:
–Una arquitectura con una única CPU, memoria principal e interfaces.
–Sistema de buffers para almacenar los paquetes.
Dependiendo de las prestaciones que deba ofrecer el router, la estructura interna es más o menos compleja y especializada, pero para los modelos de gama baja, podemos pensar en una estructura muy parecida a un PC solo que sin ningún tipo de periférico: CPU, memoria, buses e interfaces de red.
Para el almacenamiento de datos es habitual utilizar la memoria RAM, la memoria ROM, la memoria Flash (EEPROM) y la NVRAM, sin contar con las conexiones a los interfaces.
Dependiendo de las prestaciones que deba ofrecer el router, la estructura interna es más o menos compleja y especializada, pero para los modelos de gama baja, podemos pensar en una estructura muy parecida a un PC solo que sin ningún tipo de periférico: CPU, memoria, buses e interfaces de red.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Para el almacenamiento de datos es habitual utilizar la memoria RAM, la memoria ROM, la memoria Flash (EEPROM) y la NVRAM, sin contar con las conexiones a los interfaces.

CPU

–Es el cerebro de este tipo de arquitecturas.

–Ejecuta la IOS (bien desde la flash para modelos run-from flash, bien desde la RAM para modelos run-from RAM) y conmuta paquetes.

–El tipo de procesador se puede visualizar con el comando “show ver”. Por ejemplo, los 1600 y los 2500 usan un Motorola 68000.

MEMORIA

Existen diversas clases de memoria en un router, y cada una de ellas tiene un propósito de terminado. Así podemos distinguir entre la memoria DRAM, Flash, NVRAM y ROM.

–MEMORIA DRAM (Dynamic Random Access Memory):

Distinguimos entre

·Memoria principal del procesador que se encarga de ejecutar la IOS, de almacenar la configuración del router en cada momento (running configuration), de ejecutar todos los procesos que intervienen en cada una de las funciones del router, etc.

·Memoria compartida de I/O que se utiliza para el almacenamiento temporal de paquetes en buffers del sistema durante el process switching, y buffers del interfaz durante el fast switching.

–MEMORIA FLASH

·La memoria Flash almacena una o más imágenes, normalmente comprimida, de la IOS que se ejecutará sobre la RAM.

·El contenido de la memoria Flash no se pierde cuando el router se apaga o resetea.

–MEMORIA NVRAM (Non Volátil Random Access Memory)

·La memoria NVRAM se encarga de almacenar el fichero de configuración del router (startup-config).

·Esta configuración se almacena en la RAM al arrancar el router (running config).

·También se utiliza para el almacenamiento del registro de configuración.

–MEMORIA ROM

·La memoria ROM es una memoria EPROM (Erasable Programmable Read-Only Memory) que almacena una versión reducida de la IOS (Rxboot) y un intérprete de comandos básico para casos de catástrofe (ROM monitor).

–BUSES

·Son utilizados por la CPU para tener acceso a los diferentes componentes del sistema y transferir las instrucciones y los datos desde direcciones de memoria especificadas.

·El bus de la CPU se utiliza para las operaciones de alta velocidad, con el acceso directo del procesador. Éstos incluyen el acceso al RAM dinámico (DRAM), a la BootROM, NVRAM, flash de PCMCIA, y a las WIC´s.

·Los buses de entrada-salida (I/O) permiten controlar individualmente otros dispositivos. Éstos incluyen el puerto de consola, el controlador de Ethernet y el interfaz WAN ambos fijos en placa.

–TARJETAS DE INTERFAZ (WICs Y VICs)

·Son interfaces responsables de la transferencia de datos dentro y fuera de los routers de la serie 160x, 3600, etc., también llamadas modulares.

·Las WICs se comunican con la CPU a través del bus de la CPU para la transferencia de los paquetes.

·Las WICs no soportan su retirada y su inserción en caliente.

–FUENTE DE ALIMENTACIÓN

·Proporciona energía a los diferentes componentes del router.

·Algunas plataformas poseen 2 fuentes de alimentación para soluciones de backup.

2.3.1. Interfaces

En un dispositivo de interconexión de redes, las interfaces son el instrumento indispensable que hace posible la capacidad de conexión del dispositivo. Los dispositivos, poseen slots libres para introducir nuevas tarjetas de interfaz (WIC o HWIC) y de slots adicionales para módulos de red.

Estos slosts libres, podrán completarse con el siguiente hardware de tarjetas WIC y HWIC, según necesidad:

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Código	Descripción
Cifrado hardware	
Módulo de cifrado HW EPII PLUS	
AIM-VPN/EPII -PLUS	DES/3DES/AES VPN Encryption/Compression Module
Tarjetas de interface (WIC)	
WIC 1 puerto Serie	
WIC-1T	1-Port Serial WAN Interface Card
A elegir	CAB-V35-MT/FC o CAB-232-MT/FC
WIC 2 puertos Serie	
WIC-2T	2-Port Serial WAN Interface Card
A elegir	CAB-SS-V35-MT/FC o CAB-SS-232-MT/FC
WIC 1 puerto RDSI – V3	
WIC-1B-S/T-V3	1-Port ISDN WAN Interface Card (dial and leased line)
CAB-S/T-RJ45	Orange Color Cable for ISDN BRI S/T, RJ-45, 6 feet
WIC 1 puerto ADSL	
WIC-1ADSL1	1-port ADSL WAN Interface Card
EtherSwitch de 4 puertos 10/100	
HWIC-4ESW	4-port Cisco EtherSwitch 10BASE-T/100BASE-TX autosensing HWIC
EtherSwitch de 4 puertos 10/100 con soporte POE	
HWIC-4ESW-POE (*)	4-port Cisco EtherSwitch 10BASE-T/100BASE-TX autosensing HWIC with Power Over Ethernet
EtherSwitch de 9 puertos 10/100	
HWIC-D-9ESW	9-port Cisco EtherSwitch 10BASE-T/100BASE-TX autosensing HWIC
EtherSwitch de 9 puertos 10/100 con soporte POE	
HWIC-D-9ESW-POE(*)	9-port Cisco EtherSwitch 10BASE-T/100BASE-TX autosensing HWIC with Power Over Ethernet
WIC 1 puerto Gigabit Ethernet	
HWIC-1GE-SFP	1-Port WAN Gigabit Ethernet
A elegir	GLC-SX-MM= GE SFP, LC connector SX transceiver o GLC-LH-SM= GE SFP,LC connector LX/LH transceiver
VWIC de 1 puerto MFT-E1	
VWIC-1MFT-E1	1-Port RJ-48 Multiflex E1
A elegir (SFPs)	CAB-E1-PRI o CAB-E1-BNC
VWIC de 2 puerto MFT-E1	
VWIC-2MFT-E1	2-Port RJ-48 Multiflex E1
A elegir	CAB-E1-PRI o CAB-E1-BNC

Tipos de interfaces

Todos los routers Cisco tienen un puerto de consola, con interfaz RJ45, que sirve para acceder al intérprete de comandos de la IOS. Es la manera básica de acceder a configurar el router.

A partir de los modelos 17xx, además tienen un puerto auxiliar, que es similar al de consola. El resto de interfaces son para conexiones de red, ya sean LAN o WAN. Dependiendo del modelo de router podemos encontrar routers con interfaces fijos y routers a los que se les pueden añadir tarjetas.

Podemos distinguir entre tarjetas WIC (Wan Interface Card) y VIC (Voice Interface Card).

–Las tarjetas WIC se utilizan para conexiones de datos de redes WAN. Dentro de las tarjetas WIC podemos encontrar interfaces Serial, HSSI (High Speed Serial Interface) RDSI básico, RDSI primario, E1, ATM, etc.

Tras realizar una completa descripción del hardware de tarjetas de interfaz disponible para los distintos slots libres en los dispositivos de interconexión de red, vamos a ver a continuación, las tarjetas WIC más comunes.

–Las tarjetas VCI se utilizan para enlaces o conexiones de voz y podemos encontrar interfaces E&M, FXS, FXO, Primarios, etc.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

También hay routers que incluyen interfaces fijos y algunos módulos para añadir tarjetas. A parte de las tarjetas, existen Network Modules (NM) que pueden englobar varios slots para tarjetas WIC o VIC, interfaces LAN, interfaces WAN y sus combinaciones (1intLAN + 2intWAN, 2intLAN + 2intWAN, etc.).

Tarjetas wic

Módulo	Descripción
WIC-1T	One-port serial, async and sync (T1/E1)
WIC-2T	Two-port serial, async and sync (T1/E1)
WIC-2A/S	Two-port low-speed serial (up to 128 kbps), async and sync
WIC-1B-S/T	One-port ISDN BRI S/T
WIC-1B-U	One-port ISDN BRI U interface with integrated NT1
WIC-1DSU-56K4	One-port integrated 56/64-kbps, four-wire DSU/CSU
WIC-1DSU-T1	One-port integrated T1/fractional T1 DSU/CSU
WIC-1ADSL	One-port ADSL interface
WIC-1ENET	One-port 10BASE-T Ethernet interface
WIC-1SHDSL	One-port G.shdsl interface
WIC-1AM	One-port V.90 analog modem WIC
WIC-2AM	Two-port V.90 analog modem WIC

Tarjetas VIC

Módulo	Descripción
VIC-2E/M	Two-port E& voice/fax interface card for voice/fax network module
VIC-2FXO	Two-port voice/fax interface card for voice/fax network module
VIC-2FXS	Two-port voice/fax interface card for voice/fax network module
VIC-2FXO-M1	Two-port FXO voice/fax interface card for North America
VIC-2FXO-M2	Two-port FXO voice/fax interface card for Europe
VIC-2FXO-M3	Two-port FXO voice/fax interface card for Australia
VIC-2DID	Two-port analog DID4 voice interface card
VIC-2FXO-EU	Two-port FXO voice/fax interface card for Europe
VIC-2BRI-NT/TE	Two-port network-side ISDN BRI VIC
VWIC-1MFT-T1	One-port FJ-48 multiflex trunk - T1
VWIC-2MFT-T1	Two-port RJ-48 multiflex trunk - T1
VWIC-2MFT-T1-DI	Two-port RJ-48 multiflex trunk - T1 with drop and insert
VWIC-1MFT-E1	One-port RJ-48 multiflex trunk - E1
VWIC-2MFT-E1	Two-port RJ-48 multiflex trunk - E1
VWIC_2MFT-E1-DI	Two-port RJ-48 multiflex trunk - E1 with drop and insert
VWIC-1MFT-G.703	One-port RJ-48 multiflex trunk - E1 G.703
VWIC-2MFT-G.703	Two-port RJ-48 multiflex trunk - E1 G.703

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

LEDs asociados a las tarjetas WIC/VIC

Este conjunto de LEDs proporcionan información sobre el estado y actividad de los puertos WIC y VIC y se detallan a continuación:

LED	Color	Tarjetas soportadas	Significado del LED
SLOT 0 OK	Verde		On → Cuando se inserta correctamente en el slot 0 una tarjeta WIC/VIC
0	verde	ISDN	On → Cuando está conectado el 1º canal B de la RDSI
		Serial and CSU/DSU	Parpadea cuando los datos están siendo transmitidos o recibidos desde el puerto o al sloto
		2-port serial	
		VIC-2E&M	
		VIC-2FXO	
		VIC-2FXS	
		VIC-2BRI-ST-NT/TE	
		VIC-2DID	
		WIC-1ADSL	
		WIC-1ENET	
LED	Color	Tarjetas soportadas	Significado del LED
1	-	Serial and CSU/DSU	Off.
	verde	ISDN	On→Cuando está conectado el 2º canal B de la RDSI
		2-port serial	Parpadea cuando los datos están siendo transmitidos o recibidos desde el puerto 1 al sloto
		VIC-2E&M	
		VIC-2FXO	
		VIC-2FXS	
		VIC-2BRI-NT/TE	
		VIC-2DID	
SLOT 1 OK	verde		On → Cuando se inserta correctamente en el slot 1 una tarjeta WIC/VIC
0	verde	ISDN	On→ Cuando está conectado el 1º canal B de la RDSI.
		Serial and CSU/DSU	Parpadea cuando los datos están siendo transmitidos o recibidos desde el Puerto 0 al slot 1.
		2-port serial	
		VIC-2E&M	
		VIC-2FXO	
		VIC-2FXS	
		VIC-2BRI-NT/TE	
		VIC-2DID	
		WIC-1ADSL	
		WIC-1ENET	

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

LED	Color	Tarjetas soportadas	Significado del LED
1	-	Serial and CSU/DSU	Off.
	verde	ISDN	On→ Cuando está conectado el 2º canal de la RDSI.
		2-port serial	Parpadea cuando los datos están siendo transmitidos o recibidos desde el Puerto 1 al slot1
		VIC-2E&M	
		VIC-2FXO	
		VIC-2FXS	
		VIC-2BRI-NT/TE	
		VIC-2DID	
SLOT 2 OK	verde		On→Cuando se instala correctamente una tarjeta VIC
0	verde	VIC-2E&M	Parpadea cuando los datos están siendo transmitidos o recibidos desde el Puerto 0 al slot2.
		VIC-2FXO	
		VIC-2FXS	
		VIC-2BRI-NT/TE	
		VIC-2DID	
1	verde	VIC-2E&M	Parpadea cuando los datos están siendo transmitidos o recibidos desde el puerto 1 al slot2.
		VIC-2FXO	
		VIC-2FXS	
		VIC-2BRI-NT/TE	
		VIC-2DID	
SLOT 3 OK	verde		On→Cuando se inserta correctamente una tarjeta VIC.

LED	Color	Tarjetas soportadas	Significado del LED
0	Green	VIC-2E&M	Parpadea cuando los datos están siendo transmitidos o recibidos desde el Puerto 0 al slot3.
		VIC-2FXO	
		VIC-2FXS	
		VIC-2BRI-NT/TE	
		VIC-2DID	
1	verde	VIC-2E&M	Parpadea cuando los datos están siendo transmitidos o recibidos desde el Puerto 1 al slot3.
		VIC-2FXO	
		VIC-2FXS	
		VIC-2BRI-NT/TE	
		VIC-2DID	

–WIC-2T

Estas tarjetas, soportan 8 mb de memoria por cada puerto. Incluye 2 puertos seriales. Esta tarjeta, son para las series 2600 y 1700 de los routers de Cisco Systems.

–WIC-1T

Posee un puerto serial y usa conectores de 60 pins 5 en 1. Por otro lado, usa el mismo cableado que los Cisco Systems 2500 y 7000 series.

–HWIC-4ESW

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Estas tarjetas tienen la capacidad de soportar VLAN y POE, además de poseer 4 puertos ethernet. Son válidas para los routers Cisco Systems, 1841, 2801, 2811, 2821, 2851, 3825, 3845, 1941, 2901, 2911, 2921, 2951, 3925, 3945.

–NM-4E

Módulo de expansión de 4 puertos ethernet normalizados IEEE 802.3.

Funciona con el router 2811, 2621, 2620.

–NM-8A/S

Trae cuatro puertos serial usan conectores de 60 pin “5 in 1” usa el mismo cable que el 2500 y el 7000 series, También viene con ocho puertos.

2.3.2. Módulos

En este apartado, se va a describir los diferentes módulos que se pueden incorporar a los slots libres dentro del dispositivo de interconexión de redes. Los módulos que se van a detallar, incluyen todos los cables necesarios para su correcta instalación y puesta en marcha.

Módulos de Red

Código	Descripción
Módulos de red	
Módulo 4 puertos Asíncronos/Síncronos	
NM-4A/S	4-Port Async/Sync Serial Network Module
A elegir	CAB-V35-MT/FC o CAB-232-MT/FC
Módulo 8 puertos Asíncronos/Síncronos	
NM-8A/S	8-Port Async/Sync Serial Network Module
A elegir	CAB-V35-MT/FC o CAB-232-MT/FC
Módulo 4 puertos RDSI	
NM-4B-S/T	4-Port ISDN-BRI Network Module
Módulo 8 puertos RDSI	
NM-8B-S/T	8-Port ISDN-BRI Network Module
Módulo 4 puertos E1 ATM-AIM	
AIM-ATM	Módulo AIM para soporte de interfaces E1 ATM
Módulo 1 puerto E3 ATM	
NM-1A-E3	1-Port E3 ATM Network Module
Código	Descripción
Módulo 1 puerto E1/T1/ISDN-PRI	
NM-1CE1T1-PRI	1-Port Channelized E1/T1/ISDN-PRI Network Module
A elegir	CAB-E1-PRI o CAB-E1-BNC
Módulo 2 puerto E1/T1/ISDN-PRI	
NM-2CE1T1-PRI	2-Port Channelized E1/T1/ISDN-PRI Network Module
A elegir	CAB-E1-PRI o CAB-E1-BNC

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Módulos de Voz

Código	Descripción
Módulos de voz	
Módulo HDV2	
NM-HDV2	IP Communications High-Density Digital Voice Network Module
Módulo HDV2 1 puerto T1/E1	
NM-HDV2-1T1/E1	IP Communications High-Density Digital Voice NM with 1 T1/E1
Módulo HDV2 2 puertos T1/E1	
NM-HDV2-2T1/E1	IP Communications High-Density Digital Voice NM with 2 T1/E1

Algunos de los módulos de voz anteriores disponen de slots para tarjetas de voz, slots que se podrán completar con el siguiente hardware.

Código	Descripción
Tarjetas de voz (VIC)	
VIC2 con 2 puertos BRI NT	
VIC2-2BRI-NT/TE	Two-port Voice Interface Card - BRI (NT and TE)
VIC2 con 2 puertos FXO	
VIC2-2FXO	Two-port Voice Interface Card – FXO
VIC2 con 2 puertos FXS	
VIC2-2FXS	Two-port Voice Interface Card – FXS
VIC2 con 2 puertos E/M	
VIC2-2E/M	Two-port Voice Interface Card – E/M
VWIC2 con 1 puerto E1/T1	
VWIC2-1MFT-T1/E1	1-Port 2nd Gen Multiflex Trunk Voice/WAN Int. Card - T1/E1
A elegir (SFPs)	CAB-E1-PRI o CAB-E1-BNC
VWIC2 con 2 puerto E1/T1	
VWIC2-2MFT-T1/E1	2-Port 2nd Gen Multiflex Trunk Voice/WAN Int. Card - T1/E1
A elegir (SFPs)	CAB-E1-PRI o CAB-E1-BNC

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

PVDM (Packet Voice Data Module)

Las tarjetas HDV2 disponen de 4 slots para añadir tarjetas de 2ª generación con DSP's para comunicaciones de voz.

Código	Descripción
PVDM2	
PVDM2-8	
PVDM2-8	8-Channel Packet Voice/Fax DSP Module
Código	Descripción
PVDM2-16	
PVDM2-16	16-Channel Packet Voice/Fax DSP Module
PVDM2-32	
PVDM2-32	32-Channel Packet Voice/Fax DSP Module
PVDM2-48	
PVDM2-48	48-Channel Packet Voice/Fax DSP Module
PVDM2-64	
PVDM2-64	64-Channel Packet Voice/Fax DSP Module

Dependiendo de la complejidad del códec que se utilice se necesitará un número u otro de DSP's ya que la combinación de módulos PVDM es muy variada.

Module Name	Max channels High complex	Max channels Medium complex	Max channels Flexi complex
PVDM2-8	4	4	4-8
PVDM2-16	6	8	6-16
PVDM2-32	12	16	12-32
PVDM2-48	18	24	18-48
PVDM2-64	24	32	24-64

Tarjetas de puertos WAN

Puertos ethernet dedicados a recibir conexiones de fibra con la MAN o directamente con los routers fronterizos, donde será necesario aplicar configuraciones avanzadas de QoS.
Cisco 76xx. SPA 2 puertos GE
–7600-SIP-400. Cisco 7600 Series SPA Interface Processor-400.
–SPA-2X1GE. Cisco 2-port Gigabit Ethernet Shared Port Adapter.
Pudiendo utilizar cualquiera de los siguientes SFP's:
–SFP's SPA 2 puertos GE
·Cisco 76xx. Conversor de Interface GE Multimodo SPA-2GE
›SFP-GE-S. 1000BASE-SX SFP (DOM).
·Cisco 76xx. Conversor de Interface GE Monomodo corta distancia SPA-2GE
›SFP-GE-L. 1000BASE-LX/LH SFP (DOM).
·Cisco 76xx. Conversor de Interface GE Monomodo larga distancia SPA-2GE
›SFP-GE-Z. 1000BASE-ZX Gigabit Ethernet SFP (DOM).

Tarjetas de puertos LAN

Puertos ethernet dedicados a recibir conexiones de cliente, adicionales a los que pueda llevar la tarjeta supervisora.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Código	Descripción
Tarjetas de puertos LAN	
Cisco 76xx. Tarjeta 48 puertos 10/100/1000 RJ-45	
WS-X6148A-GE-TX	Catalyst 6500 48-port 10/100/1000 w/Jumbo Frame, RJ-45
Cisco 76xx. Tarjeta 24 puertos Gigabit SFP	
WS-X6724-SFP	Catalyst 6500 24-port GigE Mod: fabric-enablec (Req. SFPs)

Tarjetas de servicio

Tarjetas dedicadas a realizar determinadas funcionalidades (IPSec, etc.) en hardware en el equipo.

Código	Descripción
Tarjetas de servicio	
Cisco 76xx. Tarjeta de cifrado	
SPA-IPSEC-SSC400-1	Cisco 6500/7600 IPSec VPN Bundle1: 1 IPSec VPN SPA + SSC-400

2.3.3. Cables

En una arquitectura de un dispositivo de interconexión de redes, los medios de transmisión guiados por cables, el ancho de banda o velocidad de transmisión dependen de la distancia y de si el enlace es punto a punto o multipunto. En el cableado, podemos distinguir varios tipos de medios de transmisión guiados, como son:

Par trenzado

–Es el medio guiado más barato y más usado.
–Consiste en un par de cables, embutidos para su aislamiento, para cada enlace de comunicación.
–Debido a que puede haber acoples entre pares, estos se trenza con pasos diferentes.
–La utilización del trenzado tiende a disminuir la interferencia electromagnética.
–Este tipo de medio es el más utilizado debido a su bajo coste (se utiliza mucho en telefonía) pero su inconveniente principal es su poca velocidad de transmisión y su corta distancia de alcance.
–Con estos cables, se pueden transmitir señales analógicas o digitales.
–Es un medio muy susceptible a ruido y a interferencias.
–Para evitar estos problemas se suele trenzar el cable con distintos pasos de torsión y se suele recubrir con una malla externa para evitar las interferencias externas.
Pares trenzados apantallados y sin apantallar
–Los pares sin apantallar son los más baratos aunque los menos resistentes a interferencias (aunque se usan con éxito en telefonía y en redes de área local).
–A velocidades de transmisión bajas, los pares apantallados son menos susceptibles a interferencias, aunque son más caros y más difíciles de instalar.

Cable coaxial

–Consiste en un cable conductor interno (cilíndrico) separado de otro cable conductor externo por anillos aislantes o por un aislante macizo.
–Todo esto se recubre por otra capa aislante que es la funda del cable.
–Este cable, aunque es más caro que el par trenzado, se puede utilizar a más larga distancia, con velocidades de transmisión superiores, menos interferencias y permite conectar más estaciones.
–Se suele utilizar para televisión, telefonía a larga distancia, redes de área local, conexión de periféricos a corta distancia, etc.
–Se utiliza para transmitir señales analógicas o digitales.
–Sus inconvenientes principales son:
–Atenuación, ruido térmico, ruido de intermodulación.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

–Para señales analógicas, se necesita un amplificador cada pocos kilómetros y para señales digitales un repetidor cada kilómetro.

Fibra óptica

–Se trata de un medio muy flexible y muy fino que conduce energía de naturaleza óptica.
–Su forma es cilíndrica con tres secciones radiales: núcleo, revestimiento y cubierta.
–El núcleo está formado por una o varias fibras muy finas de cristal o plástico.
–Cada fibra está rodeada por su propio revestimiento que es un cristal o plástico con diferentes propiedades ópticas distintas a las del núcleo.
–Alrededor de este conglomerado está la cubierta (constituida de material plástico o similar) que se encarga de aislar el contenido de aplastamientos, abrasiones, humedad, etc.
–Es un medio muy apropiado para largas distancias e incluso últimamente para LAN's.
Sus beneficios frente a cables coaxiales y pares trenzados son:
–Permite mayor ancho de banda.
–Menor tamaño y peso.
–Menor atenuación.
–Aislamiento electromagnético.
–Mayor separación entre repetidores.
Su rango de frecuencias es todo el espectro visible y parte del infrarrojo.
El método de transmisión es:
a)Los rayos de luz inciden con una gama de ángulos diferentes posibles en el núcleo del cable, entonces sólo una gama de ángulos conseguirán reflejarse en la capa que recubre el núcleo.
b)Son precisamente esos rayos que inciden en un cierto rango de ángulos los que irán rebotando a lo largo del cable hasta llegar a su destino.
c)A este tipo de propagación se le llama multimodal.
d)Si se reduce el radio del núcleo, el rango de ángulos disminuye hasta que sólo sea posible la transmisión de un rayo, el rayo axial, y a este método de transmisión se le llama monomodal.
Los inconvenientes del modo multimodal es que debido a que dependiendo al ángulo de incidencia de los rayos, estos tomarán caminos diferentes y tardarán más o menos tiempo en llegar al destino, con lo que se puede producir una distorsión (rayos que salen antes pueden llegar después), con lo que se limita la velocidad de transmisión posible.
Hay un tercer modo de transmisión que es un paso intermedio entre los anteriormente comentados y que consiste en cambiar el índice de refracción del núcleo.
A este modo se le llama multimodo de índice gradual.
Los emisores de luz utilizados son:
–LED (de bajo coste, con utilización en un amplio rango de temperaturas y con larga vida media) y ILD (más caro, pero más eficaz y permite una mayor velocidad de transmisión).

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Cables para dispositivo de interconexión de redes

A continuación, voy a presentar los diferentes cableados que se hacen necesarios, cuando hablamos de equipos para la interconexión de redes, con especiales capacidades para su cometido.

Código	Descripción
Cables Serie	
V.35 DTE	
CAB-V35MT	V.35 Cable, DTE, Male, 10 Feet
V.35 DCE	
CAB-V35FC	V.35 Cable, DCE, Female, 10 Feet
V.24 (RS-232) DTE	
CAB-232MT	RS-232 Cable, DTE, Male, 10 Feet
V.24 (RS-232) DCE	
CAB-232FC	RS-232 Cable, DCE, Female, 10 Feet
SS V.35 DTE	
CAB-SS-V35MT	V.35 Cable, DTE, Male to Smart Serial, 10 Feet
SS V.35 DCE	
CAB-SS-V35FC	V.35 Cable, DCE, Female to Smart Serial, 10 Feet
SS V.24 (RS-232) DTE	
CAB-SS-232MT	RS-232 Cable, DTE, Male to Smart Serial, 10 Feet
SS V.24 (RS-232) DCE	
CAB-SS-232FC	RS-232 Cable, DCE, Female to Smart Serial, 10 Feet
OCTAL-V.35 DTE	
CAB-OCT-V35-MT	8 Lead Octal Cable and 8 Male V35 DTE Connectors
OCTAL-V.35 DCE	
CAB-OCT-V35-FC	8 Lead Octal Cable and 8 Female V35 DCE Connectors
OCTAL-V.24 (RS-232) DTE	
CAB-OCT-232-MT	8 Lead Octal Cable and 8 Male RS232/V.24 DTE Connectors
OCTAL-V.24 (RS-232) DCE	
CAB-OCT-232-FC	8 Lead Octal Cable and 8 Female RS232/V.24 DCE Connectors
E1 PRI	
CAB-E1-PRI	E1-ISDN PRI Cable, 10 feet
E1 BNC	
CAB-E1-BNC	E1 Cable BNC 75 ohm/Unbal 5 m
Conversor de 120 a 75 ohmios	
CAB-ADPT-75-120	75-120-Ohm Adapter Cable on E1 Multichannel Port Adapters
HSSI	
CAB-HSI1	HSSI Cable, Male to Male Connector
HSSI Null MODEM	
CAB-HNUL	Cabasy,Null Modem, DTE, HSSI

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

CABLE V.35 DTE Y V.35 DCE

Este cable, se utiliza para interconectar 2 enrutadores mediante un v.35 que posteriormente las interfaces serán configuradas como DTE y DCE.
Este tipo de cable se basa en la norma V.11, originalmente desarrollada por el CCITT (la actual ITU).
Es una norma de transmisión síncrona de datos, que especifica:
–Tipo de conector.
–Los pin outs.
–Diferentes niveles de tensión y corriente.
Las señales utilizadas por este tipo de cables son una combinación de las especificaciones V.11 y V.28, utilizando señales balanceados para proporcionar el transporte de datos necesarios (mediante niveles de tensión diferencial) y alta velocidad (clock).

Características

–Utiliza clocks de transmisión y recepción de manera independiente.
–La velocidad está entre 56kbps hasta 2 mbps, pudiendo alcanzar los 10mbps, dependiendo del cableado y equipamiento utilizado. Los valores normales utilizados son 64kbps, 128 kbps, 256 kbps.
–Normalmente se utiliza para el transporte de protocolos de la capa 2 o de nivel 2, es decir, de la capa de enlace de datos, como por ejemplo HDLC, X.25, SNA, PPP, etc.
–El conector tradicional es un MRAC-34, pudiéndose utilizar un DB-15 o uno propietario como por ejemplo de Cisco Systems.

Definición de DTE – DCE

En una comunicación extremo a extremo, hay involucrado 4 dispositivos, un DTE y un DCE en un extremo, y en el otro extremo otro DTE y DCE.
El equipo DTE, genera los datos a transmitir y los envía al DCE, que es el encargado de convertirlos a un formato apropiado al medio y los introduce en la red.
Cuando el receptor recibe los datos, ocurre el proceso inverso al descrito aquí.
–DTE: Equipo terminal de datos, siendo este un dispositivo como origen o destino, que genera los datos binarios digitales.
–DCE: Equipo del circuito de datos, siendo este un dispositivo que transmite o recibe los datos de manera analógica o digital, a través del medio.
Estándares: Cada estándar proporciona un modelo para las características mecánicas, eléctricas y funcionales de la conexión. La EIA y la ITU-t están involucradas en el desarrollo de los estándares de la interfaz DTE-DCE. Los estándares de la EIA se denominan EIA-232, EIA 442, EIA-449, etc. Los de la ITU-T se denominan serie V y serie X.

CABLE V.24 (RS-232) DTE Y V.24 (RS-232) DCE

–El standard ITU-T, desarrolló diversas recomendaciones, basadas en la interfaz RS-232, que fueron la v.24 que especifica los aspectos funcionales y operacionales y la v.28, que recoge los aspectos eléctricos de la interfaz.
–En los extremos del cable se utiliza un conector DB-25 macho y en el otro, otro conector DB-25 hembra, aunque dicho estándar no obliga a su utilización, ya que puede ser reemplazado por una variante como es la conexión DB-9 hembra más simplificada.
–La conexión DB-9 con 9 pines, se ha reemplazado, debido a que todos los circuitos conductores del conector DB-25 no se utilizan, se ha simplificado dicho conector.
–Igualmente se puede encontrar este cable serial con los 2 conectores DB-25 al DCE y DB-9 hembra para la conexión al DTE. La longitud del cable, no puede exceder de 15 metros.

CABLES SS V.35 DTE, SS V.35 DCE, SS V.24 (RS-232) DTE Y SS V.24 (RS-232) DCE

Estos cables, poseen una particularidad que los diferencia de las versiones que no son SS (Smart Serial) y es que el conector de un extremo es de tipo Smart serial, que es un conector inteligente de nueva generación de 26 pin outs.

CABLES OCTAL-V.35 DTE, OCTAL-V.35 DCE, OCTAL-V.24 (RS-232) DTE Y OCTAL-V.24 (RS-232) DCE

–Estos cables, poseen diferencias importantes en sus conectores, que va en un extremo de un cable 8 octal (68 pines) y 8 conectores V.35 DTE macho en el otro extremo.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

CABLE E1 PRI

–Este es un estándar de interfaz de telecomunicaciones usado en tecnología ISDN, para llevar múltiples DS0 de voz y datos, transmitidos entre la red y el usuario.
–E1, es el estándar E-carrier en Europa que provee servicios de telecomunicaciones a oficinas.
–La nomenclatura PRI, abastece de un gran número de canales, dependiendo del estándar en el país de la implementación, donde en Europa y Australia son 30 canales B y 2 canales D sobre una línea E1 2048 Mbit/s.
–En este tipo de líneas, se considera un timeslot que es usado con fines de sincronización, y no pertenece a ninguno de los canales B o D.
–La interfaz PRI, es utilizado para organizaciones extensas.

CABLE HSSI

–Es una estándar de interfaz serial de alta velocidad, desarrollado por Cisco Systems y T3 plus Networking, principalmente para usarlo en enlaces WAN, con capacidades de velocidad de hasta 52 Mbit/s, con cables de hasta 15 metros de longitud.
–Este cable, usa un conector macho de 50 pines, similar al que usa SCSI-2.
–La capa física del estándar está definida en la EIA-613, y la capa eléctrica en la EIA-612.

CABLE HSSI Null MODEM

Este tipo de cable, en cuestión de conectores, es idéntico al anterior, pero tiene algunas diferencias, como por ejemplo la longitud que es de 3 metros, y que el cable no está cruzado, es recto.
En una arquitectura de un dispositivo de interconexión de redes, los medios de transmisión guiados por cables, el ancho de banda o velocidad de transmisión dependen de la distancia y de si el enlace es punto a punto o multipunto.

–V.35 DTE
  CAB-V35MT: V.35 Cable, DTE, Male, 10 Feet
–V.35 DCE
  CAB-V35FC: V.35 Cable, DCE, Female, 10 Feet
–V.24 (RS-232) DTE
  CAB-232MT: RS-232 Cable, DTE, Male, 10 Feet
–V.24 (RS-232) DCE
  CAB-232FC: RS-232 Cable, DCE, Female, 10 Feet
–SS V.35 DTE
  CAB-SS-V35MT: V.35 Cable, DTE, Male to Smart Serial, 10 Feet
–SS V.35 DCE
  CAB-SS-V35FC: V.35 Cable, DCE, Female to Smart Serial, 10 Feet
–SS V.24 (RS-232) DTE
  CAB-SS-232MT: RS-232 Cable, DTE, Male to Smart Serial, 10 Feet
–SS V.24 (RS-232) DCE
  CAB-SS-232FC: RS-232 Cable, DCE, Female to Smart Serial, 10 Feet
–OCTAL-V.35 DTE
  CAB-OCT-V35-MT: 8 Lead Octal Cable and 8 Male V35 DTE Connectors
–OCTAL-V.35 DCE
  CAB-OCT-V35-FC: 8 Lead Octal Cable and 8 Female V35 DCE Connectors
–OCTAL-V.24 (RS-232) DTE
  CAB-OCT-232-MT: 8 Lead Octal Cable and 8 Male RS232/V.24 DTE Connectors
–OCTAL-V.24 (RS-232) DCE
  CAB-OCT-232-FC: 8 Lead Octal Cable and 8 Female RS232/V.24 DCE Connectors
–E1 PRI
  CAB-E1-PRI: E1-ISDN PRI Cable, 10 feet
–E1 BNC
  CAB-E1-BNC: E1 Cable BNC 75 ohm/Unbal 5 m
–Conversor de 120 a 75 ohmios

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

CAB-ADPT-75-120: 75-120-Ohm Adapter Cable on E1 Multichannel Port Adapters
–HSSI
CAB-HSI1: HSSI Cable, Male to Male Connector
–HSSI Null MODEM
CAB-HNUL: Cabasy,Null Modem, DTE, HSSI

2.4. Conceptos de encaminamiento

Concepto genérico de encaminamiento

El encaminamiento es la función que poseen los protocolos de enrutamiento para buscar un camino de entre todos los posibles de una red de paquetes, donde las diversas topologías existentes, proporcionan una excelente conectividad entre ellas.
El proceso de búsqueda de un camino, se basa en la búsqueda de la mejor ruta posible de entre todas, donde los parámetros de mejor ruta y métrica, juegan un papel decisivo en esta función. Debido a la existencia de diferentes algoritmos de encaminamiento, podemos distinguir en algoritmos de encaminamiento estático y dinámico.
El concepto de encaminamiento estático, se trata de un método manual que no tiene en cuenta el estado del enlace, permaneciendo inalterable hasta que se actúa sobre el manualmente.
El concepto de encaminamiento dinámico o adaptativo, se trata de un método que se hace más tolerante a los cambios producido en la red, como congestión del tráfico, fallos o retardos.
Este encaminamiento dinámico, da lugar a otros 3 conceptos de encaminamiento dinámico o adaptativo, dependiendo del lugar donde se tomen las decisiones y el origen de la información intercambiada.
–Concepto de encaminamiento adaptativo centralizado:
Este concepto de encaminamiento, define un nodo central, donde el resto de nodos lo nutren de información de la red y todos ellos calculan la tabla de enrutamiento, consumiendo muchos recursos de la red.
–Concepto de encaminamiento adaptativo distribuido:
Este concepto de encaminamiento, se basa en la propia autogestión y procesamiento de la información de red, y cada nodo calcula y genera su propia tabla de enrutamiento.
–Concepto de encaminamiento aislado:
Este concepto de encaminamiento, se caracteriza por su sencillez para adaptarse al estado cambiante de una red. Su información la obtiene de forma propia y local, cuyo funcionamiento consiste en dar respuesta a paquetes recibidos por todos los enlaces, excepto por el que llegó inicialmente.

Encaminamiento

Características
La función de encaminamiento tiene estos requisitos:
1.Exactitud.
2.Sencillez.
3.Robustez: es la capacidad para redirigir el tráfico a zonas seguras cuando hay fallos.
4.Estabilidad es posible que si un sistema es muy robusto, se convierta en inestable al reaccionar demasiado bruscamente ante situaciones concretas.
5.Imparcialidad: hay sistemas que premian, en aras de optimalidad, las conexiones cercanas frente a las más lejanas, con lo que la comunicación entre estaciones alejadas se dificulta.
6.Optimización: es posible que la robustez y la imparcialidad reporten un coste adicional de cálculo en cada nodo, lo que implica que ya no es el sistema más óptimo.
7.Eficiencia: lo mismo ocurre con la eficiencia.
Criterios sobre prestaciones
–Hay dos formas de elegir un encaminamiento eficiente:
–Una es elegir el camino más corto (la distancia entre la estación emisora y la receptora es la mínima) y otra es elegir el menor número de saltos (entre la estación emisora y la receptora hay el menor número de nodos).
–En aplicaciones reales se suele elegir la del camino más corto.
Lugar e instante de decisión

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

–El instante en que se decide hacia dónde se enviará un paquete en un nodo es muy importante.
–En datagramas, esto se produce una vez por paquete.
–En circuitos virtuales se produce una vez por petición de llamada.
Hay dos lugares donde se puede decidir hacia dónde debe enviarse un paquete desde un nodo:
Una es en el propio nodo (encaminamiento distribuido) y otra en un nodo señalado para esta tarea (encaminamiento centralizado).
Esta última forma tiene el inconveniente de que si este nodo se estropea, el encaminamiento de todos los nodos que dependen de este nodo de encaminamiento es imposible, y todos los nodos serán inservibles.
Hay otra forma de controlar el encaminamiento, y es en la propia estación de origen.

Estrategias de encaminamiento

1.Encaminamiento estático
·Cada nodo encaminará sus datos a otro nodo adyacente y no cambiará dicho encaminamiento nunca (mientras dure la topología de la red).
·Existe un nodo de control que mantiene la información centralizada.
·Como cada nodo encaminará sus datos sólo a un nodo adyacente para cada nodo de destino posible, sólo es necesario almacenar estos contactos entre nodos adyacentes y no todos los caminos entre todos los nodos de la red.
·En el nodo central se almacenan todas las tablas de encaminamientos, pero en cada nodo sólo hay que almacenar las filas que conectan ese nodo con el siguiente para conseguir el encaminamiento a cada nodo posible destino de la red.
·Este sistema es muy eficiente y sencillo pero poco tolerante a fallos en nodos adyacentes, ya que sólo puede encaminar a uno.
2.Inundaciones
·Consiste en que cada nodo envía una copia del paquete a todos sus vecinos y éstos lo reenvía a todos sus vecinos excepto al nodo del cuál lo habían recibido.
·De esta forma se asegura que el paquete llegará a su destino en el mínimo tiempo posible.
·Para evitar que a un nodo llegue un paquete repetido, el nodo debe guardar una información que le haga descartar un paquete ya recibido.
·Esta técnica, al ser muy robusta y de coste mínimo, se puede usar para mensajes de alta prioridad o muy importante.
·El problema es la gran cantidad de tráfico que se genera en la red.
·Esta técnica libera de los grandes cálculos para seleccionar un encaminamiento.
3.Encaminamiento aleatorio
·Consiste en que en cada nodo, elegirá aleatoriamente el nodo al cual se va a reenviar el paquete.
·De esta forma, se puede asegurar que el paquete llegará al destino pero en un mayor tiempo que en el de inundaciones.
·Pero el tránsito en la red es mucho menor.
·Esta técnica también libera de cálculos para seleccionar el encaminamiento.
4.Encaminamiento adaptable
·Consiste en que la red va cambiando su sistema de encaminamiento conforme se cambian las condiciones de tráfico de la red.
·Para conseguir esto, los nodos deben de intercambiar información sobre congestión de tráfico y otros datos.
·En estas técnicas de intercambio de información entre nodos, pueden hacerse intercambios entre nodos adyacentes, todos los nodos, o incluso que haya un nodo central que coordine todas las informaciones.
–Los inconvenientes principales son:
·El costo de procesamiento en cada nodo aumenta.
·Al intercambiar información de nodo en nodo, aumenta el tráfico.
·Es una técnica muy inestable.
–Las ventajas:
·El usuario cree que aumentan las prestaciones.
·Se puede ayudar en el control de la congestión.

Características

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

La función de encaminamiento tiene estos requisitos:
1.Exactitud.
2.Sencillez.
3.Robustez: es la capacidad para redirigir el tráfico a zonas seguras cuando hay fallos.
4.Estabilidad es posible que si un sistema es muy robusto, se convierta en inestable al reaccionar demasiado bruscamente ante situaciones concretas.
5.Imparcialidad: hay sistemas que premian, en aras de optimalidad, las conexiones cercanas frente a las más lejanas, con lo que la comunicación entre estaciones alejadas se dificulta.
6.Optimización: es posible que la robustez y la imparcialidad reporten un coste adicional de cálculo en cada nodo, lo que implica que ya no es el sistema más óptimo.
7.Eficiencia: lo mismo ocurre con la eficiencia.

2.4.1. Segmentación de redes

Segmentación

Segmentar una red consiste en dividirla en subredes para poder aumentar el número de ordenadores conectados a ella y así aumentar el rendimiento, tomando en cuenta que existe una única topología, un mismo protocolo de comunicación y un solo entorno de trabajo. Un segmento es un bus lineal al cual están conectadas varias estaciones. Las características son:
–Cuando se tiene una red grande se divide en trozos llamados segmentos.
–Para interconectar varios segmentos se utilizan bridges o routers.
–Al dividir una red en segmentos, aumenta su rendimiento.
–A cada segmento y a las estaciones conectadas a él se le llama subred.
Cuando se segmenta una red, se están creando subredes que se autogestionan, de forma que la comunicación entre segmentos solo se realiza cuando es necesario, mientras tanto, la subred está trabajando de forma independiente.
El dispositivo utilizado para segmentar la red debe ser inteligente, ya que debe ser capaz de decidir a qué segmento va a enviar la información que llego a él. Se pueden utilizar hubs, repetidores, bridges, routers, gateways.
La segmentación de una red se hace necesaria cuando:
–Se va a sobrepasar el número de nodos que la topología permite.
–Mejorar el tráfico de una red.
Por norma general, las redes suelen segmentarse. Existen dos motivos por los que es útil o necesario segmentar una red:
–Para unir dos topologías distintas.
–Para eliminar el tráfico de broadcast (colocando un router físico o un equipo con dos tarjetas de red).
El subnetting consiste en la creación de múltiples redes lógicas a partir de una sola clase de direcciones IP, reduciendo así el coste que supondría la obtención de otra clase de direcciones.
Para implementar esta técnica existen dos métodos:
–Subnetting con máscaras equivalentes: Consiste en partir del número de redes que deseamos conseguir y sin importarnos el número de nodos que podremos recedente por cada una de las subredes lógicas.
–Subnetting con máscaras variables. Sistema que se utiliza cuando si nos importa el número de nodos que debe resultar por subred.
A continuación, voy a explicar mediante una serie de ejemplos, el mecanismo de la segmentación de redes, es decir el subnetting.

Ejemplo 1

Red segmentada
Equipo1 ---------- Router1 ---------- Equipo2
En este ejemplo tenemos una red segmentada mediante un router, por lo que el direccionamiento ya no será igual. Primero será preciso determinar el número de redes que queremos obtener. En este caso serán dos.
La IP que utilizaremos será: 195.135.120.10
La máscara: 11111111.11111111.11111111.00000000

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Cogeremos 2 bits de Host para recedente las subredes. De esta manera obtendremos 4 subredes con la máscara 255.255.255.192.

DIRECCIÓN DE RED	BITS DE SUBRED	BITS DE HOST		
195.135.120.	00	000000	192.35.120.0	Dirección de Subred
195.135.120.	00	000001	192.35.120.1	1ª dirección de Host Válida
195.135.120.	00	111110	192.35.120.62	Última dirección de Host Válida
195.135.120.	00	111111	192.35.120.63	Dirección de broadcast
195.135.120.	01	000000	192.35.120.64	Dirección de Subred
195.135.120.	01	000001	192.35.120.65	1ª dirección de Host Válida
195.135.120.	01	111110	192.35.120.126	Última dirección de Host Válida
195.135.120.	01	111111	192.35.120.127	Dirección de broadcast
195.135.120.	10	000000	192.35.120.128	Dirección de Subred
195.135.120.	10	000001	192.35.120.129	1ª dirección de Host Válida
195.135.120.	10	111110	192.35.120.190	Última dirección de Host Válida
DIRECCIÓN DE RED	BITS DE SUBRED	BITS DE HOST		
195.135.120.	10	111111	192.35.120.191	Dirección de broadcast
195.135.120.	11	000000	192.35.120.192	Dirección de Subred
195.135.120.	11	000001	192.35.120.193	1ª dirección de Host Válida
195.135.120.	11	111110	192.35.120.254	Última dirección de Host Válida
195.135.120.	11	111111	192.35.120.255	Dirección de broadcast

Como se puede apreciar se obtienen cuatro subredes. Cada una de estas, está compuesta por una dirección de red, una de broadcast y 62 disponibles para hosts o clientes.
El número de clientes se obtendrá de la fórmula 2 elevado al número de bits disponibles para host y al resultado de esta operación le restaremos dos direcciones: la de red y la de broadcast.

Ejemplo 2

Subnetting con máscara variable. En este caso se plantea el siguiente ejemplo:

Red1 ---------- Router1 ---------- Red2
75 Host 28 Host
Para entender el funcionamiento de esta red es muy importante destacar que en el caso anterior lo que nos importaba era el número de subredes y por tanto el número de clientes de cada red era irrelevante. En el caso que nos ocupa ahora lo importante no es el número de redes sino el número de host o clientes que tendrá cada red. Por lo tanto deberemos jugar con los bits que componen la máscara para ajustarnos lo máximo posible a lo que nos piden.
–RED1 --- 75 Host. Necesitaremos una red de 128 – 2 Host, o lo que es lo mismo una red con máscara 255.255.255.128. En este caso hemos cogido un sólo bit del último octeto.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

–RED2 --- 28 Host. Necesitaremos una red de 32 –2 Host. En este caso cogeremos 3 bits para red ya que necesitamos un mínimo de 5 bits de host para poder recedente los 32 – 2 Host. En este caso la máscara será 255.255.255.224.
Otras máscaras válidas serían la 255.255.255.128 y la 255.255.255.192, pero como es un ejercicio lo interesante es ajustar al máximo. Otra ventaja de utilizar la máscara es que nos permitiría afrontar posibles ampliaciones a más redes.

Ejemplo 3

Partimos de la situación planteada en el ejercicio 2 pero esta vez añadiremos la RED3, la RED4 y RED5 a las redes que ya teníamos anteriormente. La RED3 será una Red WAN que nos conecte con la central, que es otro router. La RED4 será una red de backup RDSI que nos conecta con la central. La RED5 será una red formada por 49 Host.
A partir de estos datos se deberán calcular las máscaras y los rangos de red que compondrán cada subred. En este caso empezaremos por la red que tiene mayor número de host:
–RED1 --- 75 Host Necesitaremos una red de 128 – 2 Host, o lo que es lo mismo una red con máscara 255.255.255.128, en este caso hemos cogido un sólo bit del último octeto.

DIRECCIÓN DE RED	BITS DE SUBRED	BITS DE HOST		
195.135.120.	0	0000000	192.35.120.0	Dirección de Subred
195.135.120.	0	0000001	192.35.120.1	1ª dirección de Host Válida
195.135.120.	0	1111110	192.35.120.126	Última dirección de Host Válida
195.135.120.	0	1111111	192.35.120.127	Dirección de broadcast

–RED5 --- 49 Host Necesitaremos una red de 64 – 2 Host, o lo que es lo mismo una red con máscara 255.255.255.192, en este caso hemos cogido 2 bits del último octeto. Necesitamos un mínimo de 6 bits de host para poder tener 49 hosts.

DIRECCIÓN DE RED	BITS DE SUBRED	BITS DE HOST		
195.135.120.	10	000000	192.35.120.128	Dirección de Subred
195.135.120.	10	000001	192.35.120.129	1ª dirección de Host Válida
195.135.120.	10	111110	192.35.120.190	Última dirección de Host Válida
195.135.120.	10	111111	192.35.120.191	Dirección de broadcast

–RED2 --- 28 Host Necesitaremos una red de 32 –2 Host. En este caso cogeremos 3 bits para red ya que necesitamos un mínimo de 5 bits de host para poder recedente los 32 – 2 Host. En este caso la máscara será 255.255.255.224.

DIRECCIÓN DE RED	BITS DE SUBRED	BITS DE HOST		
195.135.120.	110	00000	192.35.120.192	Dirección de Subred
195.135.120.	110	00001	192.35.120.193	1ª dirección de Host Válida
195.135.120.	110	11110	192.35.120.222	Última dirección de Host Válida
195.135.120.	110	11111	192.35.120.223	Dirección de broadcast

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

–RED3 --- 2 Host Necesitaremos una red de 4 –2 Host. En este caso cogeremos 6 bits para red ya que necesitamos un mínimo de 2 bits de host para poder recedente los 4 – 2 Host. En este caso la máscara será 255.255.255.253.

DIRECCIÓN DE RED	BITS DE SUBRED	BITS DE HOST		
195.135.120.	111000	00	192.35.120.224	Dirección de Subred
195.135.120.	111000	01	192.35.120.225	1ª dirección de Host Válida
195.135.120.	111000	10	192.35.120.226	Última dirección de Host Válida
195.135.120.	111000	11	192.35.120.227	Dirección de broadcast

–RED 4. Dos Host como en el caso anterior y misma máscara.

DIRECCIÓN DE RED	BITS DE SUBRED	BITS DE HOST		
195.135.120.	111001	00	192.35.120.228	Dirección de Subred
195.135.120.	111001	01	192.35.120.229	1ª dirección de Host Válida
195.135.120.	111001	10	192.35.120.230	Última dirección de Host Válida
195.135.120.	111001	11	192.35.120.231	Dirección de broadcast

2.4.2 Algoritmos de encaminamiento

Enrutamiento estático

–El enrutamiento es fundamental para cualquier red de datos, ya que transfiere información a través de una internetwork de origen a destino.
–Los routers son dispositivos que se encargan de transferir paquetes de una red a la siguiente.
–Los routers obtienen información sobre redes remotas ya sea de manera dinámica, utilizando protocolos de enrutamiento, o de manera manual, utilizando rutas estáticas.
–En muchos casos, los routers utilizan una combinación de protocolos de enrutamiento dinámico y rutas estáticas. Este capítulo trata sobre el enrutamiento estático.
–Las rutas estáticas son muy comunes y no requieren la misma cantidad de procesamiento y sobrecarga que, según veremos, requieren los protocolos de enrutamiento dinámico.
–Los routers aprenden sobre redes remotas ya sea de manera dinámica o utilizando protocolos de enrutamiento o de manera manual, utilizando rutas estáticas.

Enrutamiento dinámico

–Los protocolos de enrutamiento se usan para facilitar el intercambio de información de enrutamiento entre los routers.
–Estos protocolos permiten a los routers compartir información en forma dinámica sobre redes remotas y agregar esta información automáticamente en sus propias tablas de enrutamiento.
–Esto se muestra en la animación.
–Los protocolos de enrutamiento determinan el mejor camino hacia cada red, que luego se agrega a la tabla de enrutamiento.
–Uno de los principales beneficios de usar un protocolo de enrutamiento dinámico es que los routers intercambian información de enrutamiento cuando se produce un cambio de topología.
–Este intercambio permite a los routers obtener automáticamente información sobre nuevas redes y también encontrar rutas alternativas cuando se produce un fallo de enlace en la red actual.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

–En comparación con el enrutamiento estático, los protocolos de enrutamiento dinámico requieren menos sobrecarga administrativa.
–Sin embargo, el costo de usar protocolos de enrutamiento dinámico es dedicar parte de los recursos de un router para la operación del protocolo, incluso el tiempo de la CPU y el ancho de banda del enlace de red.
–Pese a los beneficios del enrutamiento dinámico, el enrutamiento estático aún ocupa su lugar.
–En algunas ocasiones el enrutamiento estático es más apropiado, mientras que en otras, el enrutamiento dinámico es la mejor opción.
–Muy a menudo, se encontrará una combinación de los dos tipos de enrutamiento en una red que tiene un nivel de complejidad moderado.

Análisis de las ventajas y desventajas del enrutamiento estático y dinámico

En la actualidad, el enrutamiento estático, se usa en las redes de hoy en día, sin embargo, la mayoría del enrutamiento de las redes, es dinámico, ya que proporciona múltiples beneficios en comparación con el estático, aunque bien es cierto que actualmente en las redes se usa una combinación de ambos enrutamientos.

Objetivo del enrutamiento estático

–Facilita y consume menos cálculos de proceso en los routers, en redes pequeñas, donde la previsión de crecimiento es casi insignificante.
–Enrutamiento hacia y desde redes de conexión única.
–Uso de la ruta predeterminada, la cual se usa, en ausencia de una ruta más específica en la tabla de enrutamiento, hacia cualquier red que no tenga coincidencia.

Ventajas del enrutamiento estático:

a)El procesamiento de la CPU es mínimo.
b)Es más fácil de comprender para el administrador.
c)Es fácil de configurar.

Desventajas del enrutamiento estático:

a)La configuración y el mantenimiento son prolongados.
b)La configuración es propensa a errores, especialmente en redes extensas.
c)Se requiere la intervención del administrador para mantener la información cambiante de la ruta.
d)No se adapta bien a las redes en crecimiento; el mantenimiento se torna cada vez más complicado.
e)Requiere un conocimiento completo de toda la red para una correcta implementación.

Ventajas del enrutamiento dinámico:

a)El administrador tiene menos trabajo en el mantenimiento de la configuración cuando agrega o quita redes.
b)Los protocolos reaccionan automáticamente a los cambios de topología.
c)La configuración es menos propensa a errores.
d)Es más escalable, el crecimiento de la red normalmente no representa un problema.

Desventajas del enrutamiento dinámico:

a)Se utilizan recursos del router (ciclos de CPU, memoria y ancho de banda del enlace).
b)El administrador requiere más conocimientos para la configuración, verificación y resolución de problemas.

Algoritmos en el encaminamiento dinámico

Vector distancia

Más antiguo, se suele utilizar en pequeñas redes, cada router difunde su tabla completa periódicamente, el router que recibe la tabla, comprueba su tabla y la modifica. Ejemplo RIP, IGRP.

Estado de enlace

Más nuevo, para grandes redes, si un enlace se cae, el Router que lo detecta envía LSA a todos los equipos. Todos los routers intercambian LSA´s, completan Cambios y recalculan SPF. Ejemplos OSPF NLSP.

Comparativa entre las técnicas de encaminamiento vector distancia y estado del enlace

Vector distancia

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España

–Un router aprende un cambio, envía a sus vecinos la tabla entera de routing, el vecino la incorpora, calcula el algoritmo y hace un forward de su tabla, esto se realiza hasta que se logra la Convergencia.
–Si no hay cambios se envía la tabla periódicamente cada 60 s.
–No sabe cómo están sus vecinos de hello. Detecta que se ha caído sólo cuando el vecino envía su tabla cada 10-90s.
–Cada router crea una tabla de estado de enlace. Cada router propaga por la red su información.
–Cada vecino copia el contenido y lo envía. Métrica, número de salto, mejor camino menor número de saltos. Utiliza el algoritmo Bellman-Ford. Se puede hacer balanceo.

Estado de enlace

–Cada router recibe un update, con la información de los enlaces, y envía el mismo update SPF elige el mejor camino.
–Si no hay cambios se envían updates entre 30 minutos y 2 horas. Los vecinos incorporan las tablas "rehacen" la suya. Cada router crea su tabla que incluye las redes directas de estado de enlace y las envía a sus vecinos. Métrica bandwidth del enlace. Mejor camino menor coste. Utiliza algoritmo SPF Shortest path first. Se puede hacer balanceo.
–Tiene una relación con sus vecinos, utilizan el protocolo hello. Detecta pérdida de vecino, cuando no recibe update.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

3. Dispositivos de interconexión de redes

3.1. Interfaces más habituales de interconexión de redes

En la interconexión de redes, las interfaces más habituales son:
–Ethernet 10BASET
–FastEthernet 100BASETX
–FastEthernet 100BASEFX
–Ethernet 1000-BASE-LX
–Ethernet 1000-BASE-SX
–Ethernet 1000-BASE-ZX
–Ethernet 1000-BASE-T
–Interfaz WAN Serial (Interfaz DSL WAN, Interfaz T1, E1 WAN, Interfaz V.92 modem WAN)
–Interfaz ISDN - BRI WAN
La familia Ethernet, está presente tanto en entornos de área local como en entornos MAN o WAN. Como hemos visto las distintas interfaces enumeradas anteriormente, vemos que más de la mitad, son tecnología ethernet, donde su radio de acción en la actualidad va creciendo de manera exponencial.
Como resulta del todo muy útil, debido a su gran difusión e implementación en estos entornos, vamos a realizar una breve introducción a Ethernet, para situar al estudiante en esta tecnología, que poco a poco, se va adentrando en entornos MAN y WAN, acaparando una importante cuota de mercado.

Introducción a ETHERNET

Ethernet es un término genérico que se usa para hacer referencia al estándar IEEE 802.3, y especialmente al protocolo CSMA/CD.
Consiste en un Bus donde se conectan las distintas estaciones, donde se usa un protocolo MAC llamado CSMA-CD (Carrier Sense Multiple Access with Collision Detection).
El protocolo CSMA-CD funciona de la siguiente manera: un nodo que desea transmitir espera a que el canal esté aislado, una vez que se encuentra en este estado empieza la transmisión.
Si otro nodo empezara también a transmitir en este instante se produciría colisión, por lo tanto se detiene la transmisión y se retransmite tras un retraso aleatorio. En una red CSMA/CD la única circunstancia en la que puede producirse una colisión es cuando dos ordenadores empiezan a transmitir a la vez, o con una diferencia de tiempo lo bastante pequeña como para que la señal de uno no haya podido llegar al otro antes de que éste empiece a transmitir.
Ejemplo:
Supongamos que tenemos dos ordenadores A y B situados en extremos opuestos de la red, y que el tiempo que la señal tarda en propagarse de un extremo a otro de la red es t; cabría pensar que pasado ese tiempo t desde que A empieza a transmitir ya puede estar seguro de que no se producirán colisiones; sin embargo esta suposición es incorrecta, ya que B podría haber empezado a transmitir justo en el instante t -e, o sea inmediatamente antes de que le haya llegado la trama de A; por tanto sólo después de un tiempo 2t puede A estar seguro de haberse `apoderado' del canal de transmisión.
El protocolo ethernet es un protocolo no orientado a la conexión.
Es decir, que en una trama Ethernet irá incluida la dirección de origen y la de destino de un paquete y cada nodo por el que pase este paquete, decidirá por donde lo reenvía para alcanzar el destino.
Para poder tomar esta decisión, los switches hacen uso de su tabla de forwarding. Esta tabla no es ni más ni menos que un registro donde se almacenarán todas las direcciones MAC que se reciben por cada puerto. Estableciéndose una relación entre puerto y dirección MAC que se conoce por dicho puerto (Sería algo similar a la tabla de rutas en un Router).

3.1.1. Interconexión de área local (RAL-RAL)

A continuación, se va a proceder a realizar una explicación de cada una de las interfaces para el acceso a servicios e interconexión de redes, mediante el uso e implementación de tecnologías del tipo RAL.
–Ethernet 10BASET
–FastEthernet 100BASETX
–FastEthernet 100BASEFX

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Las características de estas interfaces, están recogidas en los estándares IEEE 802.3: Ethernet a 10Mbps y el IEEE 802.3u: Ethernet a 100 Mbps, donde su mecanismo de acceso al medio es CSMA/CD.

ETHERNET 10BASET

Esta modalidad de ethernet, soporta una velocidad de 10 mbps sobre 2 pares de cable de cobre trenzado, donde un par es dedicado a la transmisión de datos y el otro par a la recepción de los mismos.
El cableado de esta modalidad de ethernet, utiliza categoría 3 o superior para su cableado de par trenzado, utilizando un conector de 8 pines tipo RJ-45. Este interfaz, soporto los modos half-duplex y full-duplex.

Tasa de transmisión	10 Mbps (20 Mbps en full-duplex)
Tipo de cable	2 pares de cable UTP (sin apantallar) categoría 3 o superior de impedancia 100 ohmios
Longitud máxima del segmento	100 metros
Nº máximo de transceptores por segmento	2
Tecnología de conector	RJ45 (8 pins)
Codificación	Manchester

FASTETHERNET 100BASETX

Esta modalidad de ethernet, soporta una velocidad de 10 mbps sobre 2 pares de cable de cobre trenzado, donde un par es dedicado a la transmisión de datos y el otro par a la recepción de los mismos.
El identificador 100 BASET, es referido al conjunto del estándar ethernet para velocidades de 100 mbps, compartiendo la misma especificación MAC (control de acceso al medio), pero conservando cada uno su propia especificación de nivel físico (PHY).
El cableado de esta modalidad de ethernet, utiliza categoría 3 o superior para su cableado de par trenzado, según norma EIA / TIA 568 A y ANSI TP-PMD. Utiliza un conector de 8 pines tipo RJ-45. Este interfaz, soporto los modos half-duplex y full-duplex. Soporta transmisiones de hasta 100 metros de distancia, utilizando cable UTP de categoría 5 de 100 ohmios.
Este estándar utiliza la codificación 4B/5B para transmitir datos, según el estándar ANSI X3T9.5 a una frecuencia de 62.5 Mhz.

Tasa de transmisión	100 Mbps (200 Mbps en full-duplex)
Tipo de cable	2 pares de cable UTP (sin apantallar) categoría 5 o superior de impedancia 100 ohmios según ISO/IEC 11801. Opcionalmente: cable STP (apantallado) de 150 ohmios
Longitud máxima del segmento	100 metros
Nº máximo de transceptores por segmento	2
Tecnología de conector	RJ45 (8 pins) Opcionalmente: tipo-D de 9 pins
Codificación	4B/5B

FASTETHERNET 100BASEFX

Esta modalidad de ethernet, permite una velocidad igual que el resto de implementaciones, es decir 100 mbps, pero la diferencia es que esta implementación, utiliza un par de cables de fibra óptica, permitiendo una longitud máxima de 412 metros para enlaces half-duplex y de 2 km o más para enlaces full-duplex. La codificación utilizada para la transmisión de datos es 4B/5B.
Con respecto al cableado de fibra óptica, el tradicionalmente utilizado es el multimodo MMF del tipo 62.5/125 a una longitud de 1300 nm, donde el tipo de conector de fibra utilizado es el SC.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España

Tasa de transmisión	100 Mbps (200 Mbps en full-duplex)
Tipo de cable	2 fibras ópticas multimodo (MMF) 62.5/125 a 1300 nm según ISO 9314
Longitud máxima del segmento	Half-duplex: 412 metros Full-duplex: 2000 metros
Nº máximo de transceptores por segmento	2
Tecnología de conector	Conectores SC
Codificación	4B/5B

3.1.2. Interconexión de área extensa (RAL-MAN o RAL-WAN)

En este apartado, vamos a describir las diferentes interfaces que se utilizan en el acceso e interconexionado de redes, mediante tecnologías de red de área extensa, como por ejemplo Gigabit Ethernet. Gigabit ethernet, es una tecnología de transmisión, capaz de llegar a 1 gbps de velocidad en un medio compartido. Esta tecnología se utiliza en redes de área metropolitana o más extensa. Sus características, estás recogidas en los estándares IEEE 802.3z y IEEE 802.3ab.

ETHERNET 1000-BASE-LX

Esta implementación, utiliza un láser de largo alcance, operando en una longitud de onda entre 1270 y 1355 nm, las cuales hacen soportar tanto fibras monomodo como multimodo.
Para la transmisión de los datos, utiliza la codificación 8B/10B y las especificaciones físicas, están recogidas en el estándar ANSI X3.230-1994.

Tasa de transmisión	1000 Mbps (2000 Mbps en full-duplex)
Tipo de cable	2 fibras ópticas multimodo (MMF) 62.5/125 o 50/125 o fibra monomodo (SMF) de 10 micras a longitudes de onda entre 1270 y 1355 nm
Longitud máxima del segmento	Half-duplex MMF & SMF: 316 metros Full-duplex MMF: 550 metros Full-duplex: SMF: 5000 metros
Nº máximo de transceptores por segmento	2
Tecnología de conector	Conectores SC
Codificación	8B/10B

Características Técnicas

Longitud de onda	1300nm
Tipo de fibra	MMF
Tamaño del núcleo	62.5 / 62.5 / 50 micras
Ancho de banda modal	500 / 400 / 500 MHz/Km
Distancia de cable máxima	550 m
Potencia de salida del transmisor (min/max)	-3/-9.5 dBm
Potencia máxima de entrada al receptor	-3 dBm
Sensibilidad del receptor	-19 dBm
Pèrdidas de inserción: 50/125 micras MMF 62.5/125 micras MMF	4.4 dBm 6 dBm

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

ETHERNET 1000-BASE-SX

Esta implementación, utiliza un láser de corto alcance, operando en una longitud de onda entre 770 y 860 nm, las cuales hacen soportar fibras multimodo.
Para la transmisión de los datos, utiliza la codificación 8B/10B y las especificaciones físicas, están recogidas en el estándar ANSI X3.230-1994.
–Tasa de transmisión. 1000 Mbps (2000 Mbps en full-duplex).
–Tipo de cable. 2 fibras ópticas multimodo (MMF) 62.5/125 o 50/125 o fibra monomodo (SMF) de 10 micras a longitudes de onda entre 1270 y 1355 nm.
–Longitud máxima del segmento
·Half-duplex MMF & SMF: 316 metros
·Full-duplex MMF: 550 metros
·Full-duplex: SMF: 5000 metros
–Nº máximo de transceptores por segmento. 2
–Tecnología de conector. Conectores SC
–Codificación. 8B/10B
Características técnicas

Longitud de onda	850nm
Tipo de fibra	MMF
Tamaño del núcleo	62.5 / 62.5 / 50 / 50 micras
Ancho de banda modal	160/200/400/500 MHz/Km
Distancia de cable máxima	220 / 275 / 500 / 550 m
Potencia de salida del transmisor (min/max)	0/-9.5 dBm
Potencia máxima de entrada al receptor	0 dBm
Sensibilidad del receptor	-17 dBm
Pèrdidas de inserción: 50/125 micras MMF 62.5/125 micras MMF	3.4 dBm 3.2 dBm

ETHERNET 1000-BASE-ZX

Características técnicas
–Longitud de onda. 1550 nm.
–Tipo de fibra. SMF.
–Tamaño del núcleo. 9/10 micras.
–Ancho de banda modal
–Distancia de cable máxima. 70 / 100 Km

ETHERNET 1000-BASE-T

Basado en el estándar IEEE 802.3ab, soporta Gigabit Ethernet sobre 100 metros de cable balanceado de cobre categoría 5 de acuerdo con la normativa ANSI/TIA/EIA- 568-A.
–Tasa de transmisión. 1000 Mbps (2000 Mbps en full-duplex).
–Tipo de cable. 4 pares de cable categoría 5 o superior de 100 ohm.
–Longitud máxima del segmento. 100 metros.
–Nº máximo de transceptores por segmento
–Características técnicas.

Temperatura operación	0 a 45º C
Temperatura almacenamiento	-10 a 65º C
Humedad	10 a 85% sin condensación
Altitud	Hasta 3000 metros
Estándar	IEEE 802.3ab
Certificaciones de seguridad	UL 1950 CSA 22.2 Nº 950 EN 60950 IEC 950 AS/NZS 3260, TS001 CE
EMI	FCC Parte 15 clase A EN 55022B clase A (CISPR 22 clase A) VCCI clase A BCMI CE

Los routers tienen tanto interfaces LAN y WAN, y que un router segmentos LAN, también se utiliza como dispositivo de acceso a la conexión WAN. En esta sección, vamos a hablar acerca de las interfaces WAN del router y el cableado WAN. En términos generales, el router Cisco tienen tres tipos de interfaces:

1.Interfaces LAN (Ethernet AUI, BD-9) - Permitir el router para conectarse a la LAN a través de los medios de comunicación Ethernet o alguna otra tecnología inalámbrica, tales como Token Ring o ATM.

2.Puertos de gestión (Console, Auxiliar) - Proporcionar una conexión basada en texto para la configuración y solución de problemas del router.

3.Interfaces WAN (serie, ISDN BRI) - se realizan a través de una interfaz WAN del router a un proveedor de servicios o el sitio distante a Internet.

Algunos routers tienen puertos adicionales, tales como BD-9 puerto para la red token ring y puerto RDSI Basic Rate Interface (BRI) de bajo costo dial-on-demand conexión WAN

Para comunicación a larga distancia, las WAN utilizan la transmisión serial. La transmisión en serie es un método de transmisión de datos en la que los bits de datos se transmiten secuencialmente en un canal único. Por el contrario la transmisión, transmite bits de datos en paralelo de varios a la vez con la transmisión de datos en paralelo. Los puertos seriales de los routers Cisco utilizan 60-pin conector DB-60 o el más pequeño “smart-serial” conector con el propósito de conexiones WAN. Puertos serie en el otro extremo de la conexión de WAN depende de los proveedores de servicios y el tipo de su equipo DCE.

Algunos de los diferentes estándares de señalización y conectores que se pueden encontrar en el equipo DCE incluyen EIA/TIA-232, EIA/TIA-449, V.35, X.21, y EIA-530.

Cuando usted ordene el cable de conexión WAN, recibirá un cable de transición serial con un conector DB-60 (también llamado cinco en un conector serie) en un extremo y el conector adecuado para los estándares especificados en el otro extremo.

Si bien el conector cinco-en-uno se conecta al puerto DB-60 en una tarjeta de interfaz serial WAN (WIC) en el DTE (router), el conector especificado se enchufa en el WIC específico en el DCE (módem proveedor o CSU / DSU).

En algunos casos como el back-to-back conexión, el router puede actuar como DCE, en lugar de DTE. por lo tanto, además de determinar el tipo de cable, es necesario determinar si necesita equipo terminal de datos (DTE) o de terminación de circuito de datos (DCE) para conexiones de su equipo WAN.

Cuando un router se conecta directamente a una red de datos tal como un proveedor de servicios de enlace WAN, el router se conoce como equipo terminal de datos, o DTE.

Tenemos que seleccionar cable serial DTE en este caso.

En algunos casos, si está realizando un escenario enrutador back-to-back) en un entorno de prueba, uno de los routers es un DTE y el otro es un DCE.

Para implementar esto, se necesita un cable DTE para un router, y un cable DCE para otro router.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

También podría ser capaz de comprar cable especial back-to-backe, que se conecta con un lado a DTE y DCE por el otro.

INTERFAZ WAN SERIAL

Las WAN utilizan la transmisión serial. La transmisión en serie es un método de transmisión de datos en la que los bits de datos se transmiten secuencialmente en un canal único.
Por el contrario la transmisión, transmite bits de datos en paralelo de varios a la vez con la transmisión de datos en paralelo.
Los puertos seriales de los routers Cisco utilizan 60-pin conector DB-60 o el más pequeño “smart-serial” conector con el propósito de conexiones WAN.
Puertos serie en el otro extremo de la conexión de WAN depende de los proveedores de servicios y el tipo de su equipo DCE.
Algunos de los diferentes estándares de señalización y conectores que se pueden encontrar en el equipo DCE incluyen EIA/TIA-232, EIA/TIA-449, V.35, X.21, y EIA-530.
En cuanto se vayan a efectuar conexiones con el cable de conexión WAN, tendrá un cable de transición serial con un conector DB-60 (también llamado cinco en un conector serie) en un extremo y el conector adecuado para los estándares especificados en el otro extremo.
Si bien el conector cinco-en-uno se conecta al puerto DB-60 en una tarjeta de interfaz serial WAN (WIC) en el DTE (router), el conector especificado se enchufa en el WIC específico en el DCE (módem proveedor o CSU / DSU).
Existen diversas interfaces, que se sustentan bajo tarjetas de interfaz WAN (WIC o HWIC), como son:
–Interfaz dsl wan
–interfaz t1, e1 wan
–interfaz v.92 modem wan

INTERFAZ ISDN - BRI WAN

El interfaz ISDN BRI de los Routers permite manejar un acceso básico de RDSI que incluye un canal D y dos canales B. Generalmente el canal D se utiliza para enviar mensajes de señalización de establecimiento y liberación de llamadas.
Los canales B se usan para la transmisión de datos de otros protocolos.
Los routers soportan RDSI conmutada o semipermanente y se adaptan a muchos de los distintos estándares de RDSI que existen.
Además, se pueden configurar una serie de parámetros que determinan el comportamiento del interfaz y que permiten que estos routers puedan ser utilizados en la mayoría de los escenarios y lugares del mundo.
El interfaz ISDN BRI asegura el acceso a la RDSI para la transmisión de datos sobre los canales B, soportándose en ellos distintos protocolos. Se puede considerar este interfaz como un intermediario entre la RDSI y otros interfaces usuarios que solicitan sus servicios.
Sobre el interfaz ISDN BRI se pueden configurar tantos interfaces usuario como se quiera (de tipo FR Generic o PPP Generic).
Al arrancar el equipo, cada interfaz usuario se registra sobre el interfaz base ISDN BRI.
En la información de registro se le indica al ISDN BRI qué canal B se quiere utilizar y se le proporciona un nombre de perfil de llamada.
El ISDN BRI utiliza ese perfil cuando realiza llamadas salientes por encargo del interfaz usuario y también para filtrar las llamadas entrantes y poder así asignarlas al interfaz que corresponda.
Cuando un interfaz usuario quiere establecer un enlace, se lo solicita al interfaz base ISDN BRI mediante un comando interno.
El ISDN BRI, cuando tenga disponible el enlace (por ejemplo, cuando haya conseguido establecer una llamada), informará al interfaz usuario mediante el correspondiente evento.
Una vez establecido el enlace, comienza el intercambio de datos.
Naturalmente, si varios interfaces usuario, ya sean FR Generic o PPP Generic, compiten por el mismo canal B, el interfaz ISDN BRI asignará el enlace al primer usuario que se lo haya pedido, teniendo que esperar el otro a que se libere el recurso.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Cuando se trabaja con una RDSI donde los dos canales B son semipermanentes, no es necesario el establecimiento de llamada y tampoco que el interfaz usuario solicite la activación del enlace mediante comando.
Ésta se produce de manera automática en el momento del registro y, en consecuencia, sólo dos interfaces usuario podrán conseguir la activación de sus enlaces.
En los apartados que siguen a esta introducción se explica la configuración específica del interfaz ISDN BRI.
No obstante, un operador que desee configurar un router, del fabricante Teldat, para que maneje enlaces Frame Relay o PPP por RDSI deberá también dominar la configuración de los perfiles de llamada y de los interfaces usuario FR Generic y PPP Generic.

3.2. Características de los servicios de interconexión de redes

Los servicios más comunes de interconexión de redes privadas con redes públicas, son entre otros:

- Datainternet.
- InterLAN.
- LAN Integrada.
- MacroLAN.
- MetroLAN.
- Vpn-IP.

Definición y características del servicio data internet

El servicio Data Internet se define como un servicio de conexión a Internet sin restricciones a través de la Red Multiservicio de cualquier operador de telecomunicaciones.
El servicio ofrece diferentes tecnologías de acceso (ATM, FR, IP Nativo y ADSL).
La propuesta de servicio DataInternet tiene como objetivo la evolución del servicio hacia la solución integral para el Cliente de la conexión con Internet de su red corporativa, con las máximas garantías de seguridad y fiabilidad.
Desde el punto de vista de comunicación de la Corporación con Internet:
–Por defecto: Posibilita el acceso a Internet desde todas las ubicaciones del Cliente
–Bajo petición específica: Permite la visibilidad (presencia) de determinados Servidores de Cliente desde Internet
–Servicio. El Cliente, a través del Servicio DataInternet podrá contratar tantos Caudales, de tipo Internet o Internet Agregado, como requiera para completar su solución.
Las oficinas hacen uso de los Caudales a través de Conexiones (ADSL, ATM, Frame Relay o PPP).
La comunicación con Internet requiere el empleo de un rango de direccionamiento público exclusivo del Cliente.
Estas direcciones podrán ser de Cliente o cedidas.
Para la comunicación de corporaciones con Internet, será necesaria la traslación de direccionamiento privado a público.
·Un Caudal Internet implica la conexión directa con Internet de una única ubicación u oficina del cliente. Para ofrecer soluciones de redundancia se pueden contratar dos Caudales Internet en modo backup o en modo reparto de carga. Si el cliente dispone de soluciones RPV gestionadas, puede utilizar el Caudal Internet para dotar de conexión a Internet a la misma.
·Un Caudal Internet Agregado contempla la conexión directa con Internet de un determinado número de oficinas del cliente. El requisito previo para su contratación es que dichas oficinas ya formen parte de un servicio de RPV (InterLAN, VPN IP) o del servicio de Acceso a Intranet.
En general, para la conexión de cada oficina existen diferentes modalidades de redundancia. En el caso de Caudal Internet en Interlan, aparece un nuevo concepto de caudal, denominado Caudal Básico y que es el caudal de acceso a Internet de cada oficina con salida a través del Caudal Internet Agregado. Este caudal, a diferencia del Caudal Internet y el Caudal Internet Agregado, puede tomar valores inferiores a 64 Kbps (8,16,32 y 48 Kbps).
Por defecto, se configurará este caudal a la totalidad de la línea, aunque el cliente podrá definir un caudal básico inferior. Los caudales básicos tienen también la particularidad de que no se quiere, comercialmente,

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

aportar la opción de redundancia por circuito lógico y la única opción de redundancia posible para los caudales básicos será por circuito físico.
·Simetría o Asimetría de Caudales
Cada Caudal puede ser asimétrico, por lo que para distinguir el sentido, usaremos la siguiente nomenclatura:
Sentido Ascendente = “upstream” = Cliente->Red = entrada a la Red
Sentido Descendente = “downstream” = Red -> Cliente = salida de la Red
Comercialmente, se impone el requisito de que el Caudal Ascendente debe ser mayor o igual al Descendente.
–Línea de Acceso o Acceso: Un circuito físico o línea de acceso, se caracteriza por una velocidad física bidireccional. En ningún caso, la velocidad de transmisión o recepción puede ser mayor a la velocidad de la línea
–Conexión: Circuitos lógicos mediante los que las oficinas hacen uso del caudal. Una línea o circuito físico, puede soportar, (o no) en función del protocolo varias conexiones (circuitos lógicos). Las conexiones a la Red de Multiservicio de DataInternet pueden ser de los siguientes tipos:
·Frame Relay: Conexión = CVP (Circuito Virtual Permanente), de un determinado caudal menor o igual a la velocidad de línea. Los CVP se identifican mediante un campo de la cabecera FR denominado DLCI. En una línea se pueden soportar distintos CVPs, y por tanto conexiones de distintos servicios.
·ATM: Conexión = CVP (Circuito Virtual Permanente), de un determinado caudal menor o igual a la velocidad de línea. Los CVP se identifican mediante dos campos de la cabecera ATM denominados VPI.VCI. En una línea se pueden soportar distintos CVPs, y por tanto conexiones de distintos servicios.
·IP Nativo: Conexión = Línea Punto a Punto, por lo que en este caso, la conexión lógica es igual a la conexión física.
Al coincidir conexión y línea, la línea no puede soportar conexiones de distintos servicios. Sin embargo, mediante mecanismos de control de caudal, se puede limitar el caudal por debajo de la velocidad de línea.
·ADSL: Conexión = Línea ADSL, por lo que en este caso, la conexión lógica es igual a la conexión física. Al coincidir conexión y línea, la línea no puede soportar conexiones de distintos servicios. Tampoco se aplican mecanismos de control de caudal por debajo de la velocidad de línea.
–Redundancia: se definen 2 tipos de redundancia en el caso de Caudal Internet:
·Backup: 2 Caudales Internet asociados a sendas conexiones.
·Balanceo: 2 Caudales Internet asociados a sendas conexiones. Esta modalidad NO es posible junto con la funcionalidad de Firewall en Red.
En el caso de Caudal Internet Agregado, la redundancia será la suministrada por el servicio de VPN IP en el acceso a la VPN. Para incrementar la disponibilidad del Servicio, y de forma transparente al Cliente, toda VPN IP tendrá asociadas 2 salidas agregadas en modo Backup por Shastas diferentes. Los Caudales Básicos emplean la misma solución técnica que en el servicio VPN IP.
–Router: Se trata de un Router (equipo de conmutación IP) con las Interfaces adecuadas para cada tipo de conexión.
–Oficina: Una oficina puede tener uno o varios, routers, Caudales, Conexiones o Líneas de Acceso.
–RPV: Red Privada Virtual. Con este término nos referimos a la Intranet

Definición y características del servicio de InterLAN

InterLAN es un servicio de creación de redes privadas virtuales sobre infraestructura perteneciente a un operador de telecomunicaciones. Las conexiones se realizan de modo cerrado, permitiendo únicamente las comunicaciones entre las redes de área local del cliente que se especifiquen.
Se basa en la conexión permanente de las oficinas a la Red y su integración mediante enlaces permanentes (CPVs-PVCs) de Frame Relay. Permite la utilización de facilidades de equipos multiplataforma aún con protocolos distintos de IP y su gestión centralizada. El servicio se caracteriza por una capacidad de transmisión de datos (CIR) y la prioridad de transmisión que se da a los datos de un enlace en particular.

Funciones del servicio interLAN a nivel corporativo

Interconexión de Redes Locales
–Crea las bases necesarias para la implementación de una Intranet
–Correo electrónico

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

–Voz Corporativa
–Acceso remoto a servidores
–Transferencia de archivos
–Comunicaciones Corporativas seguras
–Centralización de la información
–Priorización según el tipo de tráfico
La Red Multiservicio de un operador de telecomunicaciones
–Tiene un alto grado de robustez y seguridad, que le permite soportar servicios con altas prestaciones y disponibilidad.
–Mecanismos de respaldo a nivel de Red.
–Disponibilidad global del servicio garantizada mediante SLA.
–Gestión permanente desde el Centro Nacional de Control de la Red.
–Informes de cliente con datos contratables y cuantificables del servicio prestado.
–Servicio multifabricante, dispone de los routers de los fabricantes con mayor presencia en el mercado.

Elementos del servicio de interlan

Tipo de Acceso: Frame Relay CIRs ofrecidos: 16, 32, 48, 64, 96, 128, 192, 256, 384, 512, 1024, 1536 y 1984 Kbps para datos. Para voz, los mismos anteriores, desde 32 Kbps.
–Accesos a: 64, 128, 192, 256, 384, 512, 1024, 1536, 1984, 2048 Kbps.
–Acceso: Permanente directo a Red o en cascada:
–Se incluye:
·Puerto de acceso a la Red IP
·PVC (s) de conexión nacional
›CAC
›SLAs
›Informes de Disponibilidad.
›DLSW, XOT, seguridad IPSec,
·Módulos de Voz, Backup
›CVPs prioritarios

Backup ISDN extremo a extremo

La facilidad de “Backup ISDN Extremo a Extremo” se define por CVP. La velocidad del circuito de backup se determinará en función del CIR, estableciéndose para ello los canales B necesarios. Los protocolos soportados sobre la conexión de backup están limitados a IP e IPX.

Definición y características del servicio de LAN integrada en router

La solución persigue cubrir escenarios de oficinas pequeñas en las que un único router proporciona simultáneamente la infraestructura LAN de la oficina y el acceso al servicio de RPV, teniendo como objetivo reducir el número de dispositivos electrónicos e integrar la gestión de las comunicaciones.
Para ello, se usan routers modulares capaces de integrar en sus chasis módulos o tarjetas que emulen pequeños switches que den cobertura de acceso LAN Ethernet al cliente.
Dichos routers son elementos de gama media y baja que junto con los módulos LAN Ethernet darán conectividad a equipos finales del cliente pero nunca a una red de switches en cascada y por tanto no tiene sentido el estudio de determinadas funcionalidades propias de un switch como QoS, separación de VLAN, etc. La solución “LAN integrada en el router” es un concepto basado en la existencia de módulos integrables en los routers capaces de proporcionar parte de las funcionalidades que caracterizan un switch para dar acceso a la LAN del cliente.

Cisco denomina a estos módulos o tarjetas, entre otros, como EtherSwitch HWIC , siglas de High Speed WAN Interface Card y dispone en su catálogo de módulos HWIC de 4 y 9 puertos FastEthernet 10/100.

Definición y características del servicio de macroLAN

MacroLAN es un servicio de Red Privada Virtual de Banda Ancha que permite la conexión de redes de área local remotas con prestaciones similares a las que se obtendrían si estuvieran dentro de un mismo edificio, con elevada fiabilidad, escalabilidad y simplicidad.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

El servicio requiere de Accesos Ethernet Ópticos, proporcionados por el Proveedor de Acceso Ethernet (Servicio MetroLAN).
Escenario general que incluye sedes del cliente en varias capitales y en TI MacroLAN es un servicio de RPV en el que:
–Parte de la infraestructura sobre la que se sustenta es exclusiva de un cliente.
–Otra parte es compartida por varios clientes.
Tecnologías utilizadas para separar tráfico entre clientes:
–VLAN en entorno metropolitano (IEEE 802.1Q)
–MPLS IP VPN a nivel nacional (RFC 2547)
Los orígenes de este servicio se remontan a un proyecto especial: "Interconexión de Redes de Área Local (LAN)". En este proyecto, se pretendía dar conectividad a nivel Ethernet entre dos sedes de un cliente, gracias a la utilización de enlaces de fibra óptica.
Establecer un enlace de fibra entre las dos sedes a conectar era la solución más sencilla, pero conlleva los siguientes problemas:
–No se optimiza el recurso del acceso óptico, por parte del operador de telecomunicaciones, puesto que este enlace sería utilizado exclusivamente para la conexión de un cliente.
–La gestión de este servicio sería muy complicada y sin jerarquía ninguna.
–Con este esquema no se consigue una uniformidad en las soluciones, por lo que se tendería a la personalización de los proyectos de las redes de los clientes.
Todas estas razones dan lugar al nacimiento de un proyecto piloto llamado e-BA (e-Soluciones de Banda Ancha).
En este proyecto, se montará una red Ethernet de ámbito metropolitano, que utilizará la tecnología de tramas extendidas (802.1Q/p).
Esta tecnología permite la creación de múltiples redes virtuales de área local (VLANs) con la utilización de una única red de soporte. Sobre estas redes ethernet permiten crear redes virtuales de nivel dos, con lo que se podrá ofrecer un servicio de conectividad a nivel provincial totalmente privado para cada cliente, es decir a través de redes privadas. Este servicio se llama Metrolan.

Definición y tipos de acceso

–Enlace entre el cliente y el puerto de acceso a la red MAN
–Está constituido por toda la infraestructura y equipamiento desde el convertidor de medio en domicilio de cliente hasta el puerto de acceso en el nodo de la MAN
–Interfaz Ethernet con etiquetado 802.1Q
–Identificadores de VLAN asignados por el servicio
–El tráfico no etiquetado se descarta en el nodo de acceso (salvo las BPDUs de Spanning Tree en accesos con en tunelado de BPDUs)

Protección frente a bucles RSTP de red

–Arquitectura de red con enlaces redundantes à Peligro de bucles
–Rapid Spanning Tree (IEEE 802.1d) en la red para proporcionar una topología libre de bucles
–El RSTP de la red no se propaga hacia los accesos de cliente
–En los accesos diversificados se habilita un mecanismo de entunelado de BPDUs de cliente
–Las BPDUs recibidas por un acceso se entunelan por la MAN y se entregan en el otro acceso
–Es responsabilidad del cliente implementar un protocolo de Spanning Tree que rompa el bucle
–Protección de la red frente a bucles provocados por equipos de cliente mal configurados (STP mal configurado o sin configurar)
–Si se supera el umbral de movimientos de una dirección MAC entre distintos puertos se bloquean los puertos afectados
–En los accesos diversificados se configura un acceso como primario (mayor umbral y desbloqueo automático) y el otro como secundario (menor umbral y desbloqueo manual)

Definición y características del servicio de VPN-IP

–Las redes tradicionales basadas en routers conectaban a los clientes mediante circuitos dedicados punto a punto.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

–Las redes privadas virtuales (VPN´s) reemplazan a las anteriores con circuitos virtuales (PVC´s o SVC´s) punto a punto compartiendo una infraestructura común.
·Los clientes utilizan esta estructura porque el coste es menor.
–Los servicios VPN pueden ser ofrecidos basados en dos axiomas:
·Overlay VPN´s donde el proveedor de servicios proporciona enlaces virtuales punto a punto entre redes de clientes
·Peer-to-Peer VPN´s donde el proveedor de servicios participa en el routing del cliente.

VPN IP

–Es eficiente en precios para topologías altamente malladas
–Distingue tráfico de diferentes clases de servicio
–Permite la salida a Internet desde la propia red IP

El Servicio VPN IP se define como un servicio de constitución e interconexión de Redes Privadas Virtuales sobre Redes IP.
Una Red Privada Virtual o VPN ("Virtual Private Network") es una red privada de una organización utilizada para interconectar varias de sus oficinas distantes y que utiliza para ello una infraestructura de red pública.
La forma más común de implementar este tipo de VPNs es mediante el empleo de túneles encapsulando el tráfico IP generado por las oficinas sobre otro paquete IP que es transportado desde el origen del túnel hasta el destino siendo encaminado por la Red pública IP.
Es decir, los paquetes transmitidos incluyen dos cabeceras IP, una es la original generada por los sistemas finales de la corporación, y la otra es la que permite encaminar los paquetes IP desde el origen del túnel hasta el punto de salida del túnel.
Con este mecanismo de túneles conseguimos los dos objetivos básicos de las VPNs:
a)El tráfico de cada VPN no se mezcla con el resto, es decir, el tráfico perteneciente a una VPN va únicamente dirigido a delegaciones que pertenecen a esa VPN.
b)El direccionamiento de cada VPN es indiferente respecto a las demás VPNs.
Es decir, cada VPN puede tener su propio esquema de direccionamiento (generalmente correspondiente a direcciones IP privadas), y además puede solaparse con el direccionamiento de otras VPNs.
Generalmente los mecanismos de "tunelling" empleados para implementar VPNs son L2TP ("Layer 2 Tunelling Protocol") e IPSec ("IP Security"). La ventaja de IPSec sobre L2TP es que los paquetes pueden ir cifrados. El inconveniente de este modelo de implementar VPNs mediante túneles es la escalabilidad, ya que se necesita generalmente un túnel (configurado estáticamente) entre cada dos delegaciones de la corporación.
Para un proveedor de servicio puede ser complicado configurar cientos de túneles en sus routers frontera de acceso a la red para dar servicio a las VPNs de los clientes.
Para evitar esta problemática el servicio VPN IP se basa en MPLS como tecnología idónea para implementar VPNs.
MPLS es una tecnología de conmutación de datagramas basada en etiquetas (labels) que tuvo su origen en la combinación de IP y ATM en una única tecnología (tag switching).
Esta tecnología ha evolucionado fruto del proceso de estandarización, de tal manera que en la actualidad las etiquetas pueden ser tanto las originales asociadas a la red de transporte ATM como nuevas etiquetas añadidas al datagrama IP e independientes del nivel de transporte.
Dado que en MPLS la asignación de etiquetas a los datagramas IP se puede realizar de acuerdo con una gran variedad de criterios (interfaz/subinterfaz de acceso, dirección IP, puerto y protocolo…), el proceso de conmutación del datagrama MPLS y el contenido de la cabecera IP del datagrama transportado están desacoplados, propiedad esencial para la implementación de RPVs con calidades de servicio basadas en criterios de ingeniería de tráfico diferenciados.
MPLS evita la necesidad de utilizar túneles gracias a que los routers del backbone de la red IP-MPLS no necesitan examinar la cabecera IP para tomar una decisión respecto al reenvío del paquete, sino que lo hacen a través de la etiqueta que lleva incorporado el paquete IP.
Por este motivo, si los routers frontera de entrada a la Red IP son capaces de colocar las etiquetas adecuadas a los paquetes de tal modo que el tráfico de cada VPN se encamine únicamente a puntos pertenecientes a la misma VPN habremos conseguido establecer VPNs totalmente transparentes de cara al backbone de la red, que no necesita tener información del direccionamiento de cada VPN, y además

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

evitamos el tener que configurar múltiples túneles estáticos entre las distintas delegaciones de una misma VPN.

Las RPV basadas en MPLS ofrecen los siguientes beneficios

–Escalabilidad: las redes privadas virtuales basadas en MPLS emplean el modelo 'peer' y la arquitectura de nivel 3 no orientada a conexión para conseguir una solución altamente escalable. Para el modelo 'peer' sólo es necesario establecer una sesión del router con el router del lado del proveedor de servicios y no con el resto de routers pertenecientes a la misma red privada virtual. La arquitectura no orientada a conexión permite la creación de redes privadas virtuales en el nivel de red, eliminando la necesidad de túneles o circuitos virtuales.

–Privacidad y seguridad: las redes privadas virtuales basadas en MPLS ofrecen el mismo nivel de privacidad y seguridad que las equivalentes basadas en conexión mediante la limitación de distribución de rutas de una RPV a únicamente aquellos routers que son miembros de esa RPV.

–Facilidad en su creación: proporcionan una plataforma para el rápido desarrollo de servicios IP de valor añadido, incluyendo intranets, extranets, voz, multimedia y comercio electrónico, y esto es debido a que MPLS no está orientado a conexión, no se necesitan topologías o mapas de conexión punto a punto específicos. Se pueden añadir sitios a las intranets y extranets y crear grupos cerrados de usuario Cuando se gestiona la red de esta forma, se posibilita la agrupación de cualquier sitio en múltiples redes privadas virtuales, maximizando la flexibilidad a la hora de creación de intranets y extranets.

–Simplicidad en la Migración: las redes privadas virtuales con MPLS son únicas para el proveedor de servicios porque se pueden construir sobre cualquier arquitectura de red, incluyendo IP, ATM, Frame Relay y redes híbridas.

Del lado del usuario final, la migración se simplifica en cuanto a que no hay requerimientos de soportar MPLS en los routers del cliente ni tampoco es necesaria modificación alguna en la intranet del cliente.

3.3. Tecnologías empleadas

Introducción tecnología xDSL

La explosión en la demanda por nuevos servicios es el factor definitivo en el desarrollo de tecnología de transmisión de voz y datos de hoy en día.

Los usuarios requieren actualmente servicios que necesitan gran ancho de banda, como lo son acceso a Internet, Intranets, teleconmutación (acceso a servicios de oficina desde el hogar) y acceso remoto a Redes de Área Local.

Afortunadamente, las nuevas tecnologías proveen soluciones de gran ancho de banda sobre la red telefónica de cobre existente, permitiendo a los carriers de telecomunicación y a las compañías que poseen redes privadas de cobre, rápidamente cubrir sus demandas y requerimientos sin necesidad del recableado costoso y consumidor de tiempo.

Los beneficios de este renacimiento tecnológico son inmensos.

Los Proveedores de Redes de Servicios pueden ofrecer nuevos servicios de avanzada de inmediato, incrementando las ganancias y complementando la satisfacción de los usuarios.

Los propietarios de redes privadas pueden ofrecer a sus usuarios los servicios expandidos que juegan un papel importante en la productividad de la compañía y los impulsa a mejorar su posición competitiva.

Los costes de inversión son relativamente bajos, especialmente comparados con los costes de recableado de la planta instalada de cobre.

Adicionalmente a esto, la facilidad en la instalación de los equipos xDSL permite la reducción de costes por tiempo de instalación para la puesta en marcha de los nuevos servicios.

Bajo el nombre xDSL se definen una serie de tecnologías que permiten el uso de una línea de cobre para transmisión de datos de alta velocidad y, a la vez, para el uso normal como línea telefónica.

Se llaman xDSL ya que los acrónimos de estas tecnologías acaban en DSL, que está por "Digital Subscriber Line" (línea de abonado digital): HDSL, ADSL, RADSL, VDSL.

Cada una de estas tecnologías tiene distintas características en cuanto a prestaciones (velocidad de la transmisión de datos) y distancia de la central (ya que el cable de cobre no estaba pensado para eso, a cuanta más distancia peores prestaciones).

Entre estas tecnologías la más adecuada para un uso doméstico de Internet es la llamada ADSL.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Clasificación de los servicios xDSL

La "x" en xDSL define diversas categorías de tecnologías de línea de abonado digital o de acceso al bucle local, como por ejemplo, IDSL, HDSL, SDLS, ADSL, ADSL-Lite, R-ADSL, VDSL, etc., que difieren en parámetros como distancia de la señal, velocidad, simetría en el tráfico saliente y entrante al usuario, etc.
Los definidos son:
a)**ADSL-Lite**. Es una versión de baja velocidad de ADSL que eliminará la necesidad de que las Empresas de Telecomunicaciones instalen y mantengan un "splitter del POTS" o "repetidor del local del abonado".
La eliminación del splitter del POTS simplifica la instalación y reduce los costes para los NSPs (Provedores de Servicios de Red). ADSL-Lite también soporta trabajar sobre distancias mayores que el ADSL completo.
Esta tecnología opera a velocidad de hasta 1 Mbps entrante desde la red hacia el abonado y hasta 512 Kbps saliente desde el abonado a la red. Limitación de distancia 5,5 Km con hilo de calibre 24 AWG.
Aplicaciones: Acceso a Internet/Intranet, vídeo bajo demanda, acceso a LANs remotas, VPNs y VoIP (Voz sobre IP).
b)**R-ADSL** (Rate Adaptative Digital Subscriber Line). Funciona dentro de las mismas tasas de ADSL pero se ajusta dinámicamente a longitudes que varían y a calidades de líneas de acceso local de pares trenzados.
Con R-ADSL es posible conectar diferentes líneas a velocidades variables. La velocidad de conexión puede seleccionarse cuando la línea se sincroniza durante una conexión, o como resultado de una señal de la Oficina Central. Opera a velocidad de hasta 8 Mbps de la red al abonado y 1,544 Mbps del abonado a la red. Limitación de distancia 5,5 Km con hilo de calibre 24 AWG. Si se reduce la longitud se puede aumentar la velocidad.
Aplicaciones: Acceso a Internet/Intranet, vídeo bajo demanda, acceso a LANs remotas, VPNs (Redes Privadas Virtuales), VoIP (voz sobre IP), multimedia interactiva.
c)**IDSL** (ISDN Digital Subscriber Line). A diferencia de ADSL, IDSL sólo puede transportar datos. IDSL utiliza el mismo código de modulación que ISDN/RDSI (Red Digital de Servicios Integrados), denominado 2B1Q para la entrega de servicios sin condicionamiento de la línea especial; difiere de ISDN/RDSI en aspectos como: IDSL es un servicio no conmutado a diferencia de ISDN/RDSI, no causa congestión del conmutador en la Oficina Central del Proveedor de Servicios. ISDN/RDSI requiere establecimiento de la llamada mientras que IDSL no, es un servicio siempre activo. Proporciona un caudal dúplex de hasta 144 Kbps.
Limitación de distancia con hilo de 24 AWG 5,5 Km (con equipo especial se puede extender la distancia).
Aplicaciones: Acceso a Internet/Intranet, Navegación Web, Telefonía sobre IP, vídeo-teléfonos.
d)**HDSL** (High bit rate Digital Subscriber Line). Tecnología simétrica, proporciona la misma cantidad de ancho de banda de la red al abonado y viceversa. HDSL es la tecnología xDSL más madura y ya se ha implementado en líneas que se extienden desde las Oficinas Centrales a los nodos remotos y también en entornos de campus universitarios.
Debido a su velocidad 1,544 Mbps (T1) sobre dos pares de Cobre y 2,048 Mbps (E1) sobre tres pares, las Empresas de Telecomunicaciones utilizan HDSL como una alternativa a enlaces T1/E1. La distancia a la que opera HDSL (de 3,7 Km a 4,6 Km) es menor que proporcionada por la tecnología ADSL. HDSL permite conectar sistemas PABX/PBX, lazos locales digitales, servidores Internet, POPs (Points Of Presence).
HDSL II es la siguientes generación de HDSL ofrecerá el mismo rendimiento que HDSL pero sobre un único par trenzado de Cobre (definiéndose en ANSI/ETSI).
e)**SDLS** (Single-Line Digital Subscriber Line). Al igual que HDSL, SDSL soporta transmisiones T1/E1 simétricas, pero SDSL difiere de HDSL en estos aspectos: Utiliza un único par de Cobre.
·Posee un rango máximo de operación de 3 Km.
·Dentro de la limitación de distancia, SDSL puede acomodarse a aplicaciones que precisen idénticas velocidades de red a abonado y viceversa como videoconferencia o computación colaborativa.
·SDSL es un precursor de HDSL-II.
f)**VDSL** (Very high bit rate Digital Subscriber Line). Está pendiente de estandarizarse.
·Es la tecnología xDSL más rápida, soporta una velocidad de red a abonado de hasta 53 Mbps y de abonado a red de hasta 6,4 Mbps sobre un único par de Cobre (en la modalidad simétrica hasta 34 Mbps).
·La distancia máxima operativa para esta tecnología asimétrica es para la máxima velocidad de 0,3 Km.
·Como futuras aplicaciones de VDSL figuran las mismas que ADSL más HDTV (TV de alta definición).

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Introducción tecnología ATM

El Modo de Transferencia Asíncrono (ATM) es la tecnología para el despliegue de servicios troncales más extendida en la actualidad.

–Es utilizada tanto en el núcleo como en el acceso a sistemas de telecomunicación de alta velocidad.
–Permite ofrecer un contrato de servicio.
–Orientado a la conexión.
–Calidad del servicio (QoS) entre extremos garantizada.
–Escalable en velocidad y distancia.
–Utilizada tanto en WANs como en LANs de altas prestaciones.

Características de ATM

–Es una técnica de transferencia orientada a paquetes, en la que el flujo de información se organiza en bloques de tamaño fijo y pequeño (celdas).
–No se garantiza la entrega al destino de todas las células generadas por una fuente de información.
–Se garantiza la secuencia de entrega de las células transmitidas por el mismo circuito virtual.
–No existe protección contra errores ni control de flujo en la transferencia entre enlaces.
–Estos se realizan extremo a extremo entre los terminales de manera transparente a la red.
–La cabecera de las celdas tiene una funcionalidad reducida: identifica las células pertenecientes a la misma comunicación (circuito virtual).
–Las celdas se transfieren usando la técnica de multiplexación asíncrona por división en el tiempo.
–Orientado a la conexión: cada llamada se constituye en un canal virtual en el multiplex ATM.
–La información de señalización va por un canal virtual diferente.
–El nivel físico especifica el medio de transmisión y el esquema de codificación de la señal.
–Velocidades típicas de acceso en la Ifz usuario-red son: 155,52 Mbps, 622.08 Mbps y 2488,32 Mbps.
–El nivel ATM es totalmente independiente del medio físico de transmisión usado para transportar las celdas ATM. Realiza las siguientes funciones:
–Transferencia de las celdas ATM por la red, independientemente del servicio final al que pertenecen esas celdas.
–El encaminamiento de las celdas se hará a través del examen del identificador de canal virtual (ICV) y del identificador de trayecto virtual (ITV), incluidos en la cabecera de cada celda.
–Multiplexación y demultiplexación de las celdas de las diferentes conexiones en un único tren de celdas.
–Añade la cabecera a la información entregada por el nivel de adaptación antes de entregarla al nivel dependiente del medio físico y luego la elimina en el otro extremo antes de entregarla al nivel de adaptación.
–Generación de información de control de flujo para colocarla en la cabecera de las celdas.
–El nivel de adaptación (AAL) es dependiente del servicio.
–Es el nivel encargado de adaptar los protocolos de transferencia no basados en ATM a celdas ATM.
–Dividido en dos subniveles:
–Convergencia y segmentación y reensamblado. Dependiendo de las características del servicio aparecen distintos protocolos.

Además, el modelo de referencia ATM contempla tres planos diferentes:

–Plano de operación y mantenimiento para permitir el control y operación de la red ATM por parte de los operadores de la red; el Plano de control para el establecimiento de comunicaciones (señalización) y el Plano del usuario donde se definen los protocolos para la transferencia del usuario.
–Tecnología de gran utilización en troncales. Aparentemente ha tocado techo en cuanto a implantación.
–En la actualidad está siendo sustituida/enmascarada por redes MPLS y Gigabit Ethernet.
–Red capaz de proporcionar servicios con QoS.
–Aparente está teniendo un cierto reverdecer en sistemas 3G
–Utilizado junto con Ethernet en los enlaces ADSL para el transporte de datos IP.
–Ofrece soluciones para prácticamente todos los tipos de tráficos y QoS existentes.
–En declive en cuanto a su aplicación en entornos LAN.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Introducción a la tecnología de FRAME RELAY

Frame Relay es un protocolo de comunicaciones, para transmisión de datos a alta velocidad, orientado a la interconexión de RAL, (Redes de Área local). El protocolo Frame Relay, se caracteriza con respecto a otros protocolos, como X25, HDLC, etc., por varios aspectos fundamentales:

–Utiliza parte del nivel de enlace.

–La gestión del nivel de enlace, se realiza mediante un procedimiento llamado LMI (Local Management Interface), que consiste en el envío de mensajes asíncronos, para verificar la integridad del enlace.

–No realiza la parte del protocolo dedicada a la corrección y retransmisión de tramas erróneas (es el ETD quien debe implementar sus propios mecanismos para controlar esto), limitándose a una simple detección de errores por medio del SVT (Secuencia de verificación de trama), descartando todas aquellas con SVT incorrecto.

Características del servicio FRAME RELAY

El servicio Frame Relay se describe haciendo referencia a dos planos de descripción diferentes, aunque estrechamente relacionados entre sí:

–El plano de usuario. En él se definen las características asociadas a la transmisión de datos en cada conexión de usuarios, son las que siguen:

·Transferencia bidireccional de tramas.

·Mantenimiento por parte de la Red del orden de la secuencia de las tramas enviadas por el Etd-origen.

·Detección y descarte de tramas erróneas por medio del código de Redundancia cíclica.

·Multiplexación estadística de diferentes flujos de datos recibidos desde un interface.

·Transparencia por parte de la Red de los diferentes protocolos de usuario.

–El plano de control. El plano de control proporciona la señalización entre la Red y el etd.

Esta señalización, consiste en un protocolo de enlace que permite al usuario obtener información, sobre el estado de sus conexiones, así como el estado de la Red. Estas conexiones se realizan a través de CVP,s (Circuito Virtual Permanente)y definen la conexión lógica permanente que se establece entre dos ETD,s.

Cada conexión entre el usuario y la red se identifica mediante DLCI,s (Data Link Connection Interface), único en cada interface, siendo solo considerado a nivel local (ETD-RED).

Este identificativo, corresponde a un destino particular y permite establecer varias conexiones lógicas, con destinos diferentes a través de un único interface. El protocolo Frame Relay dispone de un procedimiento para gestionar el enlace llamado LMI (Local Management Interface), con varias funciones fundamentales:

–Comprobación del estado del interface.

–Informar del estado de los CVP,s.

–Informar de altas y bajas en los CVP,s, así como de la actividad o inactividad de estos.

Control de la congestión

El control de la cogestión, tiene por objetivos:

–Mantener la calidad del servicio.

–Distribuir equitativamente los recursos disponibles de la red entre todos los usuarios, con respecto a las necesidades contratadas por cada usuario.

–Impedir que una minoría de usuarios monopolicen los recursos de la Red.

Los parámetros que determinan la congestión, se miden entre otros, por la ocupación de la CPU, y los bloques de mensaje ocupados.

La red define varios niveles de congestión:

a)Débil: la Red activa los bits de notificación explícita de congestión o de hacia el usuario, en las tramas que atraviesan los recursos congestionados.

b)Moderado: La Red comienza a descartar tramas con el bit de activado, en los actos con prioridad de descarte normal.

c)Fuerte: se descartan todas las tramas con de activo, tanto en los actos con prioridad de descarte normal, como los de alta.

d)Severo: se descartan todas las tramas que llegan al elemento congestionado.

El mecanismo que permite el control de la congestión se denomina Rate adaptation

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Introducción a la tecnología MPLS

MPLS son las siglas de MultiProtocol Label Switching (Conmutación de Etiquetas Multiprotocolo), y es un mecanismo de transporte mediante conmutación de etiquetas, estandarizado en la RFC 3031 del IETF, que se basa en el Tag Switching de CISCO.

MPLS opera entre los niveles de Enlace de Datos y de Red del modelo OSI (entre los niveles 2 y 3) y fue diseñado para unificar redes basadas en paquetes y redes basadas en circuitos.

La tecnología IP ofrece un transporte No Orientado a la Conexión mediante el transporte de Datagramas:

–No mantiene un estado de la comunicación entre nodos.

–No ofrece Circuitos Virtuales (cada datagrama puede viajar por caminos distintos)

MPLS introduce mejoras a IP:

–Mecanismos de protección frente a fallos.

–Ingeniería de Tráfico.

–Redes Privadas Virtuales.

Aplicaciones de MPLS

–La Ingeniería de Tráfico busca adaptar flujos de tráfico a recursos físicos de la red, de tal forma que exista un equilibrio entre dichos recursos.

–Así conseguiremos que no haya recursos muy utilizados mientras existan otros recursos poco utilizados.

–En las redes IP por ejemplo, los paquetes suelen seguir el camino más corto, provocando que algunos trayectos se saturen mientras otros casi no se utilizan.

Ejemplo

El camino más corto entre A y C en una red IP será como hemos dicho el que tiene menos saltos, es decir A-B-C, pero puede que, el exceso de tráfico sobre estos enlaces o la carga en los routers, hagan aconsejable la utilización de un camino alternativo como A-D-E-C.

MPLS nos va a permitir:

–Establecer rutas (o LSPs) explícitos, indicando el camino exacto a seguir.

–Permite obtener estadísticas de los LSPs.

–Permite usar encaminamiento basado en restricciones, de manera que la red pueda seleccionar determinadas rutas según el nivel de calidad requerido (ancho de banda, retardo, …)

–MPLS nos va a permitir emplear un sistema Peer-to-Peer VPN.

–Lo que haremos será que los routers de los clientes tengan un único circuito, el cual les unirá con la red.

–La red trabajará empleando Protocolo IP a Nivel 3, con lo que todos los routers se conocerán entre sí (como en Internet).

–Haremos que la red, de forma interna, trabaje como una red completamente mallada; todos los PEs estarán unidos con todos mediante LSPs, de esta forma, cuando un PE quiera enviar un datagrama a otro PE, lo primero que hará será obtener la etiqueta MPLS a utilizar para enviárselo al destino.

Introducción a la tecnología X.25

X.25 es un estándar para el acceso a redes públicas de conmutación de paquetes. No especifica cómo está la red implementada interiormente aunque el protocolo interno suela ser parecido a X.25.

El servicio que ofrece está orientado a conexión (previamente a usar el servicio es necesario realizar una conexión y liberar la conexión cuando se deja de usar el servicio), fiable, en el sentido de que no duplica, ni pierde ni desordena (por ser orientado a conexión), y ofrece multiplexación, esto es, a través de un único interfaz se mantienen abiertas distintas comunicaciones.

El servicio X.25 es un diálogo entre dos entidades DTE Y DCE.

Nomenclatura

–DTE (Data Terminal Equipment): Es lo que utiliza el usuario final (PC con placa X.25 por ejemplo). Es el equipo terminal de datos. Incorpora los niveles 2 y 3.

–DCE (Data Circuit Terminating Equipment): Podemos interpretarlo como un nodo local. A nivel de enlace (LAPB) las conexiones se establecen DTE-DCE. Ahora con el nivel de red, ampliamos las comunicaciones más allá del DCE, que hace de interconexión.

Sólo incluye el nivel 1. Con X.25 no hay conexiones multipunto. Es un servicio punto a punto, por lo que sólo puedo conectar un DTE con otro DTE.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

En X.25 se regulan:
·Interfaz a nivel físico.
·Protocolo de enlace.
·Protocolo de red.

Introducción a la tecnología RDSI

La red telefónica que todos conocemos está sufriendo en los últimos años una profunda transformación debido a la introducción en la misma de técnicas digitales en la transmisión y la conmutación, que presentan una mayor eficacia y capacidad de tratamiento de información.
La primera etapa de esta progresiva introducción, ha sido la digitalización de las centrales de conmutación de la red y de los sistemas de transmisión, permaneciendo como único elemento todavía analógico el acceso del cliente, incluyendo bucle y equipo terminal.
La tecnología RDSI, se le denomina Red Digital Integrada (RDI).
El paso siguiente es la digitalización del bucle de usuario o elemento de unión entre la central telefónica y el domicilio del cliente.
De esta manera se obtiene una vía de conexión digital entre el usuario y la red, y por lo tanto, entre los usuarios extremos de cada comunicación.
Con la digitalización de las líneas de acceso se consigue la prestación de gran diversidad de servicios (voz, datos, imágenes, etc.) por una única línea de cliente, entre los cuales estarían la mayoría de los que actualmente se ofrecen de una manera dispersa a través de las redes existentes (Red Telefónica Analógica, Red Iberpac, etc).
El tratamiento integrado de todos estos servicios en una única red, precisa de un importante intercambio de información de control entre los usuarios y la red, y entre los propios elementos de la red. Se hace necesaria la introducción de mecanismos de señalización más potentes adecuados a las nuevas necesidades.
La transmisión digital de señales desde y hacia los terminales de usuario hace igualmente necesario un nuevo sistema para intercambiar las informaciones de direccionamiento y señalización entre el usuario y la red.
El sistema tradicional de selección por impulsos o multifrecuencias se sustituye por un protocolo de comunicación, basado en el intercambio de mensajes entre la central y el terminal de usuario.
Es el denominado protocolo de canal D o señalización del interfaz usuario/red.

Esta estructura de red con conectividad digital extremo a extremo, potente sistema de señalización binado en intercambio de mensajes, disponibilidad de diversidad de servicios y acceso de usuario único conforman la Red Digital de Servicios Integrados.

Características principales

–Digitalización de la línea del acceso de usuario.
–Acceso por una única línea a todos los servicios.
–Posibilidad de varias comunicaciones simultáneas por la misma línea.
–Conexiones por conmutación de circuitos a 64 Kbit/s y hasta 2 Mbit/s.
–Incorporación de nuevos servicios y facilidades.
–Interfuncionamiento con las otras redes existentes.

La red telefónica que todos conocemos está sufriendo en los últimos años una profunda transformación merced a la introducción en la misma de técnicas digitales en la transmisión y la conmutación, que presentan una mayor eficacia y capacidad de tratamiento de información.
La primera etapa de esta progresiva introducción, ha sido la digitalización de las centrales de conmutación de la red y de los sistemas de transmisión, permaneciendo como único elemento todavía analógico el acceso del diente, incluyendo bucle y equipo terminal.
La RDSI es una red que procede por evolución, de la red telefónica existente y por tanto está basada en conexiones por conmutación de circuitos de 64 Kbit/s, que al ofrecer conexiones digitales extremo a extremo, permitiendo la integración de multitud de servicios en un único acceso, independientemente de la naturaleza de la información a transmitir, y del equipo terminal que la genere.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Inicialmente el funcionamiento estaba soportado por las centrales de conmutación RDI / Red Digital Integrada (AXE, 1240 y 5ESS), incorporando nuevas funciones de operación y mantenimiento para su explotación.
La RDSI convivirá con las redes convencionales de telefonía y datos (RTB e Iberpac), pero incorporando elementos interfuncionales de interconexión con dichas redes, convirtiéndose en la red Universal de Telecomunicaciones.
La RDSI se identificaba como (RDSI-BE) de Banda Estrecha, puesto que trabaja básicamente con conexiones conmutadas de 64 Kbit/s hasta 2 Mbit/s.
A partir de ahora veremos como la RDSI incorporará elementos conmutadores a velocidades superiores, lo que propiciará la aparición de nuevos servicios como la distribución de TV o la transmisión de datos a muy alta velocidad. Tendremos así la RDSI de Banda Ancha (RDSI-BA).

3.4. Identificación de los servicios de conexión

SERVICIOS DE CONEXIÓN ARP

El protocolo ARP (address resolution protocol), es un servicio adicional relacionado con IP, el cual es usado para traducir una dirección IP en una dirección MAC, es decir una dirección de hardware.
El protocolo ARP es un mecanismo que proporciona la conversión de una dirección IP en una dirección MAC, para que un paquete pueda conseguir que llegue a su destino, un dispositivo debe poseer un mecanismo que le proporcione ese emparejamiento de una dirección IP de destino con una dirección MAC de destino, para cumplir el propósito de poder entregar el mensaje al dispositivo destino.
Todo lo anterior en referencia a las direcciones MAC, se relaciona con las interfaces de red, las cuales poseen una dirección física o de hardware MAC, donde cada dispositivo en una red Ethernet u otra LAN, se comunican sobre la misma red Ethernet.
ARP está definido en la RFC 826, la cual contiene algunas ambigüedades que han sido corregidas por la RFC 1122. Es por ello, para que ARP trabaje consistentemente y con confiabilidad con otras implementaciones, es necesario incorpora ambas RFCs para poder operar en este entorno.
Como vemos, ARP es una forma útil para los dispositivos de localizar la dirección MAC de otro host IP, sobre la misma red local.
Todos los medios LAN, usan ARP para localizar la dirección hardware de otros dispositivos IP sobre la misma red local, incluso entornos WAN, ya están utilizando el protocolo ARP para estos asuntos.

Descripción de su funcionamiento

En un entorno de red local, cuando un dispositivo necesita enviar un paquete a otro dispositivo sobre el medio de red, comprueba el software IP si conoce la dirección MAC asociada con la dirección IP de destino (esta información normalmente ya está presente en caché de otras peticiones realizadas), por lo tanto el emisor transmite los datos al dispositivo destino, usando los protocolos y direccionamiento apropiados conforme al entorno de red local en el cual 2 dispositivos se comunican.
En caso contrario, el software IP, tiene que localizar la dirección MAC asociada con la dirección IP de destino, antes de que los datos puedan ser transmitidos.
Es aquí, donde ARP entra en juego, haciendo las consultas necesarias a los hosts de la red local, para poder asociar la dirección MAX a la dirección IP de destino.
A modo introductorio, ARP usa los tipos de comunicación broadcast para la emisión de la petición de dirección MAC, e unicast, para dirigirse exclusivamente al dispositivo al cual pertenece la dirección MAC localizada a través del proceso ARP.

SERVICIOS DE CONEXIÓN RARP

Este protocolo, proporciona un mecanismo para la resolución de direcciones IP, cuando se conoce su dirección MAC.
Este proceso se hace necesario, porque de lo contrario y en supuestos donde sucedan estos casos, las capas superiores no les serían servidas la información requerida, por lo que esto sería un grave problema para TCP/IP.
El protocolo lleva el mismo proceso que ARP, pero la información que solicita es la dirección IP, a partir de la dirección MAC conocida, mientras que en ARP, la información que se solicita es la inversa, es decir, se conoce la dirección IP de destino, pero se requiere averiguar la dirección MAC de dicha dirección lógica.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Cuando el protocolo RARP, confecciona un paquete, donde el campo dirección IP origen se queda tal cual porque es lo que necesitamos averiguar y con respecto a la dirección MAC origen y destino, deben de ser cumplimentadas.

Servidor RARP

A diferencia del procedimiento de ARP, el cual cada dispositivo posee una tabla ARP en caché local de memoria volátil (se pierde la información, cuando se reinicia el equipo), en este caso, la existencia de un servidor RARP dedicado a este servicio es necesario, donde contiene una tabla ARP, la cual es no volátil (no se pierde la información aun reiniciando el dispositivo).

El servidor RARP, es designado específicamente para abastecer este servicio, cuya dirección IP es 200.59.4.50. Todas las peticiones de los dispositivos, van dirigidas a esta dirección, donde el servidor RARP consultará su tabla ARP para proporcionar la información necesaria.

El servicio RARP en la actualidad parecerá algo sin sentido, pero su cometido es proporcionar la dirección IP desconocida, a equipos cuya configuración es gestionada por DHCP y no poseen disco duro, también conocidos como terminales dump o tontos.

SERVICIOS DE CONEXIÓN BOOTP

Servidor BOOTP

El servidor BOOTP, es un servicio parecido a DCHCP, el cual forma parte de la familia de protocolos IP, cuya función es proporcionar la información pertinente de red, tales como la dirección IP, a estaciones de trabajo y a hub de LANs.

BOOTP es un cliente/servidor, donde su operativa consiste en clientes BOOTP, los cuales intercambian mensajes entre los clientes BOOTP y el servidor BOOTP, el cual este último, ha sido configurado como servidor de la información necesaria para los clientes BOOTP.

El servidor BOOTP, utilizar el protocolo de la capa de transporte UDP para la entrega de los mensajes de configuración de red a los clientes BOOTP.

BOOTP "predecesor de DHCP"

El servidor BOOTP, fue el predecesor del protocolo DHCP, el cual fue inventado para abastecer de la configuración necesaria de red, tal como dirección IP y otra información necesaria, para convertirse en un verdadero dispositivo de red. Aquel entonces, los dispositivos o estaciones de trabajo, no poseían unidades de almacenamiento, donde pueden leer hoy día esa información relevante para convertirse en un dispositivo operativo de red.

Al no poseer este almacenamiento, se hizo necesaria la invención de BOOTP para solventar estos problemas.

SERVICIOS DE CONEXIÓN NAT

NAT es un protocolo similar a CIDR, originalmente para reducir el agotamiento de espacio de direccionamiento IP, permitiendo así la creación de múltiples direcciones privadas, y ser estas últimas representadas por unas pocas direcciones IP públicas.

Acabamos de ver, como el objetivo tanto de NAT como de CIDR, tiene que ver con el espacio de direccionamiento IP.

Desde la creación de NAT, se han observado los múltiples beneficios que comporta NAT en diferentes situaciones, como por ejemplo, para las migraciones de red, equilibrio de carga de servidores y la creación de servidores virtuales, todo esto puesto al servicio de organizaciones e incluso de ISPs.

El protocolo de traducción de direcciones de red (NAT), se ubica en los routers fronterizos de las redes, es decir, que esté directamente conectado a internet.

Si no fuera por los mecanismos de NAT y PAT, las direcciones IPv4, hubieran estado agotadas hace décadas.

NAT es el Protocolo de traducción de direcciones de red. PAT es el protocolo de traducción de direcciones de puerto.

SERVICIOS DE CONEXIÓN DNS

Permite a los usuarios de red utilizar nombres jerárquicos sencillos para referirse a otros equipos.

De esta forma, el usuario puede obviar la dirección IP asociada al equipo y referirse a él con un nombre más fácil de memorizar.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Además, facilita el cambio en la dirección IP de un equipo: los cambios de dirección sólo deben notificarse al servidor DNS encargado de ese equipo, siendo transparentes para el usuario, que sigue refiriéndose al equipo con el mismo nombre.
DNS es un protocolo de aplicación y usa tanto UDP como TCP. Los clientes solicitan a los servidores de DNS sus consultas por medio de UDP para hacer más rápida la comunicación y utilizan TCP sólo en caso de que llegara a ocurrir una respuesta truncada.
El DNS usa el concepto de espacio de nombres distribuido. Los nombres simbólicos se agrupan en zonas de autoridad, o más comúnmente, zonas. En cada una de estas zonas, uno o más equipos tienen la tarea de mantener una base de datos de nombres simbólicos y direcciones IP y de suministrar la función de servidor para los clientes que deseen traducir nombres simbólicos a direcciones IP.
Estos servidores de nombres locales se interconectan lógicamente en un árbol jerárquico de dominios.
Cada zona contiene una parte del árbol o subárbol y los nombres de esa zona se administran con independencia de los de otras zonas.
La autoridad sobre zonas se delega en los servidores de nombres.
En los puntos en los que un dominio contiene un subárbol que cae en una zona diferente, se dice que los servidores de nombres con autoridad sobre el dominio superior delegan autoridad a los servidores de nombres con autoridad sobre los subdominios.
Los servidores de nombres también pueden delegar autoridad en sí mismos; en este caso, el espacio de nombres sigue dividido en zonas, pero la autoridad para ambas la ejerce el mismo servidor.
El resultado de este esquema es:
–En vez de tener un servidor central para la base de datos, el trabajo implicado en mantenerla se reparte entre los host si lo largo y ancho del espacio de nombres.
–La autoridad para crear y cambiar nombres simbólicos de hosts y la responsabilidad de mantener una base de datos para ellos le corresponde a la organización propietaria de la zona que los contiene.
–Desde el punto de vista del usuario, hay una sola base de datos que trata la resolución de las direcciones.

SERVICIOS DE CONEXIÓN DHCP

El protocolo DHCP (Dynamic Host Configuration Protocol) proporciona un mecanismo para intercambiar información de configuración a los distintos clientes en una red TCP/IP.
DHCP tiene dos componentes principales:
–Un protocolo para entregar los datos de configuración a los distintos clientes desde un servidor DHCP.
–Un mecanismo para almacenar las direcciones de red servidas a los distintos clientes.
DHCP se construye sobre un modelo cliente-servidor, donde un servidor DHCP se encarga de asignar direcciones de red y entregar los parámetros de configuración a los clientes que se van a configurar de forma dinámica.
El protocolo DHCP se construye con una arquitectura cliente/servidor.
La interacción entre ambos se describe a continuación. Algunos pasos se omiten cuando el cliente conoce su dirección.
–Lo primero que hace el cliente es enviar un mensaje DHCPDISCOVER de broadcast en su subred física.
–Este mensaje puede tener opciones de tiempo de cesión de dirección o incluso valores para la dirección.
–Si el servidor no está en la misma subred se envía a él a través de un Relay (un equipo encargado de trasladar las peticiones al servidor de la subred a la que él está conectado).
–Cada servidor puede responder con un mensaje DHCPOFFER que incluye una dirección de red válida y otros parámetros de configuración.
–El DHCP, utiliza la identidad del cliente, para decidir la forma de proceder.
–Cuando un cliente contacta con un servidor DHCP, envía un identificador, por lo general, la dirección de hardware del cliente.
–El servidor utilizar el identificador del cliente y la red a la que el cliente se ha conectado, para determinar cómo asignar el cliente y la dirección IP.
–Un servidor, puede configurarse para asignar direcciones a computadoras específicas de manera estática, mientras que por otro lado, permite a otras computadoras obtener direcciones dinámicamente de manera permanente o temporal.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Servicios de PROXY

Un servidor proxy es una aplicación que actúa como intermediario entre dos sistemas finales. Los servidores proxy funcionan en la capa de aplicación (nivel 7) de los cortafuegos, donde se obliga a los extremos de una conexión a canalizar la sesión a través del proxy.
Esto se realiza creando y ejecutando un proceso en los cortafuegos que crea una imagen espejo de un servicio como si estuviera ejecutándose en todos los equipos finales.
Un servidor Proxy esencialmente convierte una sesión de dos partes en una sesión de cuatro partes, donde los procesos intermedios emulan los dos equipos reales. Como operan en el nivel 7, los servidores proxy también se conocen con el nombre de cortafuegos de la capa de aplicación. Es necesario ejecutar un servicio proxy por cada tipo de aplicación.
Como los servidores proxy centralizan toda la actividad para una aplicación en un solo servidor, éstos presentan la oportunidad ideal de realizar varias funciones útiles.
Tener la aplicación ejecutándose justo delante de los cortafuegos ofrece la oportunidad de inspeccionar los paquetes para buscar más cosas que las direcciones origen/destino y los números de puerto. Esta es la razón por la que prácticamente todos los cortafuegos modernos incorporan alguna forma de arquitectura de servidor proxy.
Las peticiones recibidas de los clientes al servidor proxy, son reenviados al servicio, y los resultados, son reenviados de vuelta al proxy, donde es reenviado al cliente.
El servicio proxy ejecuta una función de redirección, no hace nada en referencia al procesamiento de peticiones, es el único sistema que el cliente ve, durante esta transacción.
Un servidor proxy, también puede ser llamado un gateway o un proxy tunneling.

Un servidor proxy, no encamina paquetes a nivel de red, sino que actúa como retransmisor a nivel de aplicación. Los usuarios de la red contactarán con el servidor intermediario, que a su vez estará ofreciendo un servicio proxy, asociado a una o más aplicaciones determinadas.
El concepto genérico de proxy, viene dado por la necesidad de conectar varios equipos de una red de una organización o corporación, hacia internet, donde solamente se dispone de una dirección IP pública para realizar tal operación.
La función principal de un servidor proxy, es la de interceptar todo el tráfico de red de la organización o corporación que sale desde dicha organización hacia internet y viceversa, sirve de intermediaria entre el tráfico que se produce dentro de una red protegida e Internet.
Los proxies habitualmente se utilizan como sustitutos de routers o controladores de tráfico para prevenir el tráfico que pasa directamente entre las redes. Un proxy sirve para permitir el acceso a Internet a todos los equipos de una organización cuando solamente se puede disponer de un único equipo conectado, eso es, una única dirección IP. Es decir, intercepta el tráfico en la red.

3.4.1. Interrelación de los servicios

La interrelación de los servicios anteriormente descritos, resultan muy importantes para poder saber cuál va a ser el comportamiento de dichos servicios en lo relacionado a la conexión y a la interacción de los equipos pertenecientes a una red local.
En la implementación del servicio de DNS junto con DHCP, sabemos que los servicios DNS, proporcionan la resolución de nombres de dominio para los diferentes recursos de red, asociando la dirección asignada por el servicio de DHCP.
Cuando existe un cambio en la dirección o en el nombre asociado a la dirección, se debe actualizar dicha información del DNS, ya que el servicio DHCP, no actualiza automáticamente el DNS, en el supuesto caso, de que la información que ha variado sea la dirección IP proporcionada por el servicio DHCP.
Los servidores Windows server 2008 y DHCP, junto con los clientes que ejecutan DHCP, pueden asociarse o registrarse con el DNS, con el objetivo de facilitar la interacción de estos 2 servicios.
La facilitación de esta interacción, daría lugar a que si cambia la información de DHCP, las actualizaciones de DNS, sincronizarían con la información existente, y las actualizaría con la asociación de nombre y dirección del equipo. En el proceso de interrelación de los servicios de NAT con ARP, sabemos que ambos servicios tiene una especial interrelación entre ambos, para lograr el cometido final, que no es otro que proporcionar

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

conectividad entre 2 hosts en ubicaciones distintas, aprovechando los beneficios de NAT para lograr conectividad con otros equipos fuera de la red local.
–Una vez se haya recibido respuesta de un paquete desde el exterior, una vez enviado una petición por parte de un host de la red interna, NAT mapea dicho paquete, para después poder encontrar la asociación correcta entre el puerto y la dirección IP local.
–Una vez encontrado un mapeo válido para la respuesta de un paquete, entra en juego en proceso ARP, con el firme objetivo de mapear igualmente en su tabla ARP, las direcciones IP locales con las direcciones físicas MAC.
–Una vez encontrado un mapeo válido, entre una dirección IP local y una dirección física MAC, el paquete entonces es procesado por el host legítimo.

3.4.2. Implementación en los equipos de la red local

Implementación del servicio de conexión ARP

En una sola red física, los hosts individuales se conocen en la red a través de su dirección física. Los protocolos de alto nivel direccionan a los hosts de destino con una dirección simbólica (en este caso la dirección IP).
Cuando tal protocolo quiere enviar un datagrama a la dirección IP de destino w.x.y.z, el dispositivo final, no entiende dicho datagrama.
En consecuencia, se suministra un módulo (ARP) que traducirá la dirección IP a la dirección física del host de destino. Utiliza una tabla (llamada a veces caché ARP) para realizar esta traducción.
Cuando la dirección no se encuentra en la caché ARP, se envía un broadcast en la red, con un formato especial llamado petición ARP.
Si una de las máquinas en la red reconoce su propia dirección IP en la petición, devolverá una respuesta ARP al host que la solicitó.
La respuesta contendrá la dirección física del hardware así como información de encaminamiento (si el paquete ha atravesado puentes durante su trayecto) tanto esta dirección como la ruta se almacenan en la caché del host solicitante. Todos los posteriores datagramas enviados a esta dirección IP se podrán asociar a la dirección física correspondiente, que será la que utilice el dispositivo para mandar el datagrama a la red.
El módulo ARP intenta hallar la dirección en su caché.
Si encuentra el par buscado, devuelve la correspondiente dirección física de 48 bits al dispositivo.
Si no lo encuentra, descarta el paquete (se asume que al ser un protocolo de alto nivel volverá a transmitirlo) y genera un broadcast de red para una solicitud ARP. Cuando un host recibe un paquete ARP (bien un broadcast o una respuesta punto a punto), el dispositivo receptor le pasa el paquete al módulo ARP. El host solicitante recibirá esta respuesta ARP.
Como resultado, el protocolo, la dirección de protocolo, dirección hardware para el host en cuestión se añadirá a la caché ARP.
La próxima vez que un protocolo de nivel superior quiera enviar un paquete a ese host, el módulo de ARP encontrará la dirección hardware, a la que se enviará el paquete. ARP se emplea en redes IEEE 802 además de en las viejas redes DIX Ethernet para mapear direcciones IP a dirección hardware.
Para hacer esto, ha de estar estrechamente relacionado con el dispositivo de red. De hecho, las especificaciones de ARP en RFC 826 sólo describen su funcionalidad, no su implementación, que depende en gran medida del dispositivo para el tipo de red correspondiente, que suele estar codificado en el microcódigo del adaptador.
En el proceso de ejecución del mecanismo ARP, toman juego diversos tipos de mensajes, por un lado referente al tipo de comunicación llevada a cabo, y por otro, dentro de un tipo de comunicación específico, emanan otros tipos de mensajes inherentes al proceso ARP para llevar a cabo su función.
Con respecto al tipo de comunicación, nos encontramos un broadcast IP, mediante un mensaje propio de ARP, ARP request, peticiona que el dispositivo que esté usando la dirección IP especificada, responda con su dirección MAC. Todos los hosts de la red local verán el mensaje broadcast, pero solo responderá el host legítimo con su dirección MAC, utilizando o en este caso un mensaje propio del proceso ARP llamado ARP response.
En el mensaje ARP response de vuelta al dispositivo emisor, ello, no se transmite por un broadcast sobre la red. El mensaje se envía directamente al dispositivo emisor mediante un mensaje unicast.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

El contenido del paquete de respuesta, consistirá en la dirección IP del dispositivo local y la dirección MAC. En el campo tipo de mensaje del ARP response, será marcado como tal.
Cuando el dispositivo solicitante recibe un ARP response, almacena el par de la dirección IP junto con la dirección MAC del dispositivo solicitante en una caché local, con el objetivo de no tener que hacer uso nuevamente con mensajes broadcast para inundar la red. De esta forma se minimiza los efectos adversos inherentes al broadcast.
Por último los mensajes ICMP echo response, son utilizados por aquellos dispositivos que respondieron al ARP broadcast originariamente, pero no almacenaron en caché las direcciones IP y MAC, por lo tanto tendrá que enviar su propio ARP broadcast para encontrar donde enviar el mensaje ICMP echo response.

Tabla ARP y el direccionamiento estático

La tabla ARP, es caché local de memoria volátil, donde se almacena las direcciones MAC junto con su dirección IP correspondiente, con el objetivo de mejorar el procesamiento de peticiones ARP y así eliminar en la medida de lo posible, un excesivo tráfico de broadcast.
Esto último, mejora notablemente el rendimiento de la red, ya que dichas entradas están almacenadas en la tabla ARP, y lo único que deben de hacer los host solicitantes, en primer lugar es consultar la tabla para ver si hay alguna coincidencia con la dirección IP de destino.
Estas tablas se construyen a partir de un mecanismo de forma dinámica, de modo que cada cierto tiempo, si una concreta tabla no se usa, el mecanismo de ARP, eliminará dicha entrada por obsoleta y la dejará libre, para el almacenamiento de nuevas entradas recientes.

62.99.16.1	00:23:EB:a
192.168.0.1	E4:48:C7:b
192.168.0.2	90:2B:34:c
192.168.0.10	00:50:56:d
192.168.0.12	00:50:56:d

La tabla arp y el direccionamiento dinámico

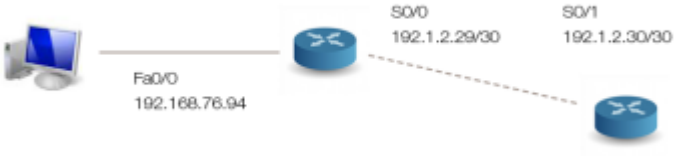
En ocasiones, las direcciones IP que son asignadas a los dispositivos, pueden que no sean asignadas de manera estática, sino que sean asignadas de forma dinámica, mediante un servicio DHCP destinado a tal fin. De modo que, las direcciones podrán recorrer varios dispositivos, sin tener asignado un dispositivo concreto, por lo que esto afectará a la estructura de la tabla ARP y al contenido de su tabla.
Para esta situación, ARP contiene un mecanismo que determina la validez de la entrada ARP (dirección IP / dirección MAC), estableciendo un cierto período de tiempo, el cual una vez haya expirado, la entrada correspondiente en la tabla ARP será eliminada

Implementación del servicio de conexión NAT

En este apartado, vamos a observar distintos escenarios de uso de NAT, para asentar los conocimientos sobre este mecanismo, a la hora de comprender su funcionamiento y los objetivos para el cual ha sido diseñado e implementado, con independencia del lado oscuro resultante de la implementación de NAT.
En este ejemplo sencillo, vemos como el router fronterizo, implementado entre la red de área local e internet, está realizando las tareas de NAT, para que todos los hosts pertenecientes a la red 172.16.1.0/24 puedan tener acceso a internet.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Aquí vemos, como el router se encargará de traducir las diferentes direcciones inside local address a inside global address para su salida a internet tal y como se refleja.
Una vez los hosts de destino hayan procesado los mensajes, estos devolverán a los hosts de la subred 172.16.1.0/24, con la dirección outside local, este es la dirección de la interfaz del router que está directamente conectado al router del ISP.
Este a su vez, traduce esta dirección a una inside local address, almacenada en la tabla NAT del router, el cual enviará el mensaje al host origen correspondiente. Aquí, podemos ver otro ejemplo simple y claro sobre el proceso que se lleva a cabo dentro del router fronterizo mediante el mecanismo de NAT.



En este ejemplo, el proceso es exactamente igual al anterior, donde la configuración de NAT en el router fronterizo corp, realiza la función de traducción de las direcciones pertenecientes a la subred 192.168.76.94 a una dirección IP global, para que dichos host puedan tener acceso a internet.
Para que esto tenga lugar, se usará solo las siguientes direcciones inside, tanto locales como globales, para que todos los hosts, puedan tener acceso directo a internet.

Inside globals: 198.18.41.129 a través 198.18.41.134
Inside locals: 192.168.76.65 a través 192.168.76.94

Implementación del servicio de conexión DNS

Ya visto en las prácticas de Redes
Tras iniciar sesión en Windows, procedemos a configurar los parámetros necesarios para que el equipo cliente funcione para la resolución de nombres.
1.Abrir control de panel/red e internet/conexiones de red
2.Se elige la interfaz de red donde configurar los parámetros DNS, por ejemplo la ethernet.
3.Seleccionamos propiedades de ethernet
4.Seleccionamos propiedades de TCP/IPv4
5.Seleccionar la pestaña avanzadas
6.Rellenar los siguientes campos:
a)En “Direcciones de servidores DNS, por orden de utilización” hay que consignar las direcciones IP de los servidores DNS.
b)Para ello hacer clic sobre el botón “Agregar...” y rellenar con las direcciones IP en la ventana que se visualiza.
c)Marcar “Anexar estos sufijos DNS (en este orden)”, hacer clic sobre el botón “Agregar...” y consignar.
Desmarcar la opción “Registrar estas direcciones de conexiones en DNS”.
7.Pulsar aceptar en todas las ventanas, para que los cambios surtan efecto de inmediato

Implementación del servicio de conexión DHCP

Ya visto en las prácticas de Redes
Desde el apartado anterior, seleccionamos obtener IP automáticamente

Implementación del servicio de conexión PROXY

Configurar un proxy en explorer
Lo primero que debes tener claro son los datos de conexión del proxy:

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

–Dirección. Lo más normal es que el proxy se identifique mediante su IP. Es un número de cuatro cifras separadas por puntos (82.165.35.26, por ejemplo). Pero a veces utiliza un nombre.
–Puerto. Es algo así como la vía de entrada que usa el proxy para conectarse. Se indica con un número (80, 6515, 3128, etc.).
Es habitual que los datos de un proxy se representen juntos. Primero la dirección y luego el puerto, separados por dos puntos.
Ejemplo:
Un ejemplo, 89.188.141.51:80 quiere decir que la dirección es 89.188.141.51 y el puerto el 80.
4.Abre Explorer y haz clic en el botón Herramientas. Luego pincha en el menú Opciones de Internet.
5.Haz clic en la solapa Conexiones. Abajo encontrarás el botón Configuración de LAN. Púlsalo.
6.Comprueba que está seleccionada la casilla Usar un servidor proxy para la LAN…Pincha en ella para habilitarla si no lo está.
7.Rellena los campos de Dirección y Puerto del proxy. Pulsa Aceptar. Y luego otra vez en la ventana de Opciones de Internet a la que regresas.
En una sola red física, los hosts individuales se conocen en la red a través de su dirección física. Los protocolos de alto nivel direccionan a los hosts de destino con una dirección simbólica (en este caso la dirección IP).
Cuando tal protocolo quiere enviar un datagrama a la dirección IP de destino w.x.y.z, el dispositivo final, no entiende dicho datagrama. En consecuencia, se suministra un módulo (ARP) que traducirá la dirección IP a la dirección física del host de destino. Utiliza una tabla (llamada a veces caché ARP) para realizar esta traducción.
Cuando la dirección no se encuentra en la caché ARP, se envía un broadcast en la red, con un formato especial llamado petición ARP. Si una de las máquinas en la red reconoce su propia dirección IP en la petición, devolverá una respuesta ARP al host que la solicitó.
La respuesta contendrá la dirección física del hardware así como información de encaminamiento (si el paquete ha atravesado puentes durante su trayecto) tanto esta dirección como la ruta se almacenan en la caché del host solicitante. Todos los posteriores datagramas enviados a esta dirección IP se podrán asociar a la dirección física correspondiente, que será la que utilice el dispositivo para mandar el datagrama a la red.

3.5. Los proveedores de servicios de comunicaciones

Los proveedores de servicios de comunicaciones, de entre los servicios que ofrecen, están las instalaciones de redes o de servicios de telecomunicaciones, disponible a las empresas, organizaciones, particulares, es decir al público en general.
Estas instalaciones de redes o servicios de telecomunicaciones, deberán ser suministrados por un proveedor de comunicaciones predominante, o por un número limitado de proveedores, cuya sustitución de uno o algunos de ellos, no tenga ninguna repercusión en lo factible en lo económico o en lo técnico.
Los proveedores de comunicaciones interconectan redes públicas de telecomunicaciones para el público en general, cuyo objeto es permitir que los usuarios de un proveedor, puedan comunicarse con los usuarios de otros proveedores de comunicaciones.
Existen proveedores de comunicaciones con poder sustancial en un mercado relevante de servicios de telecomunicaciones, siempre y cuando, sea declarado con poder sustancial mediante resolución firme de la autoridad competente en este sentido.
La capacidad de este o estos proveedores, que normalmente son 1 o 2, tienen la capacidad de afectar materialmente con respecto al precio y suministro de los servicios de la red pública de telecomunicaciones, donde no se contemplan ni los terminales de los usuarios, ni las redes privadas de telecomunicaciones, que se sitúan más allá de la conexión terminal.
Los proveedores de comunicaciones, pueden y tienen derecho a negociar la interconexión de redes con otros proveedores de comunicaciones, con el objetivo de interconectarlas y que estén disponibles al público de manera transparente para ellos.
Esta negociación comercial deberá sustentarse sobre una base comercial, sin perjuicio de la autoridad reguladora que puede intervenir en dicho proceso de negociación.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

La información que se ha facilitado en dicho proceso negocial, deberá mantener su derecho a la confidencialidad, quedarán obligados a utilizarla para el fin para las que se facilitaron y respetarán la confidencialidad de la información transmitida o almacenada.
Los acuerdos en los que hayan llegado con respecto al resto de proveedores de comunicaciones en materia de interconexión de redes o sus ofertas de interconexión de referencia, deberán ser puestos a conocimiento público conforme a la legislación pertinente y competente en la materia.
En materia de la universalización de los servicios de comunicaciones, los proveedores de comunicaciones, podrán ser elegibles para asegurar el servicio universal, por medios y procedimientos eficientes, transparentes y no discriminatorios.
Por otro lado, los proveedores de comunicaciones, están sujetos a todas las normas y recomendaciones que efectúe la autoridad reguladora, tomando decisiones vinculantes que afecten a los servicios de interconexión de redes, al público en general, a la competencia, etc.
En definitiva a cualquier controversia que se pudiera dar entre proveedores, o entre proveedores y usuarios, siempre en cumplimiento de los derechos públicos y privados.
Antes de profundizar en los diferentes servicios de interconexión que se implementan en la actualidad, aunque con total probabilidad con diferentes nombres de los servicios de interconexión a ofrecer por los operadores de telecomunicaciones, es de recibo, realizar una introducción a los conceptos generales de interconexión y sus diferentes capas en los que se basa el modelo.

3.5.1. Servicios de interconexión

Para construir una red de forma eficaz, es necesario entender en primer lugar cómo se utiliza el internetworking de redes, las necesidades corporativas y las demandas de los usuarios.
Estas necesidades pueden ser adaptadas a un modelo que pueda usarse para construir el internetworking de redes.
Una de las mejores formas de comprender cómo construir un internetworking de redes pasa por asimilar la forma en que el tráfico circula a través de la red.
Esto se consigue por medio de un marco de trabajo de red conceptual, el más popular de los cuales es el modelo de referencia OSI.
Los servicios más comunes de interconexión de redes privadas con redes públicas, son entre otros:

- Datainternet.
- InterLAN.
- LAN Integrada.
- MacroLAN.
- MetroLAN.
- Vpn-IP.

Vistos en el capítulo anterior 3.2. Características de los servicios de interconexión de redes

3.5.2. Perfiles de los servicios

Perfiles de protocolos ISO y ARP

Se le llama protocolo de red o protocolo de comunicación al conjunto de reglas que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red.
En este contexto, las entidades de las cuales se habla son programas de computadora o automatismos de otro tipo, tales y como dispositivos electrónicos capaces de interactuar en una red. Los protocolos de red establecen aspectos tales como:
–Las secuencias posibles de mensajes que pueden arribar durante el proceso de la comunicación.
–La sintaxis de los mensajes intercambiados.
–Estrategias para corregir los casos de error.
–Estrategias para asegurar la seguridad (autenticación, encriptación).
En el campo de las redes informáticas, los protocolos se pueden dividir en varias categorías, una de las clasificaciones más estudiadas es la OSI.
El modelo de interconexión de sistemas abiertos, también llamado OSI (en inglés open system interconnection) es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización en el año 1984.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Es decir, es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones. Siguiendo el esquema de este modelo se crearon numerosos protocolos.
El advenimiento de protocolos más flexibles donde las capas no están tan demarcadas y la correspondencia con los niveles no era tan clara puso a este esquema en un segundo plano. Sin embargo es muy usado en la enseñanza como una manera de mostrar cómo puede estructurarse una "pila" de protocolos de comunicaciones.
El modelo especifica el protocolo que debe ser usado en cada capa, y suele hablarse de modelo de referencia ya que es usado como una gran herramienta para la enseñanza de comunicación de redes.
Este modelo está dividido en siete capas como ya hemos visto a lo largo del curso.
Los protocolos de cada capa tienen una interfaz bien definida y sólo poseen conocimiento de las capas directamente inferiores.
Esta división de los protocolos ofrece abstracción tanto de los mecanismos de bajo nivel responsables por la transmisión de datos sobre las informaciones intercambiadas.
Ejemplo:
Así, por ejemplo, un navegador web (HTTP, capa 7) puede utilizar una conexión Ethernet o PPP (capa 2) pare acceder a Internet, sin que sea necesario cualquier tratamiento para los protocolos de este nivel más bajo.
De la misma forma, un router sólo necesita de las informaciones del nivel de red para enrutar paquetes, sin que importe si los datos en tránsito pertenecen a una imagen para un navegador web, un archivo transferido vía FTP o un mensaje de correo electrónico.

ARP Address resolution protocol

ARP son las siglas en inglés de Address Resolution Protocol (Protocolo de resolución de direcciones).
Es un protocolo de nivel de enlace responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP.
Para ello se envía un paquete (ARP request) a la dirección de difusión de la red (broadcast (MAC = FF FF FF FF FF FF)) que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (ARP reply) con la dirección Ethernet que le corresponde.
Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo y la carga.
ARP permite a la dirección de Internet ser independiente de la dirección Ethernet, pero esto sólo funciona si todas las máquinas lo soportan.
En Ethernet, la capa de enlace trabaja con direcciones físicas. El protocolo ARP se encarga de traducir las direcciones IP a direcciones MAC (direcciones físicas).
Para realizar ésta conversión, el nivel de enlace utiliza las tablas ARP, cada interfaz tiene tanto una dirección IP como una dirección física MAC.
ARP se utiliza en 4 casos referentes a la comunicación entre 2 hosts:
1.Cuando 2 hosts están en la misma red y uno quiere enviar un paquete a otro.
2.Cuando 2 host están sobre redes diferentes y deben usar un gateway/router para alcanzar otro host.
3.Cuando un router necesita enviar un paquete a un host a través de otro router.
4.Cuando un router necesita enviar un paquete a un host de la misma red.
Funcionamiento I
Ejemplo:
Si A quiere enviar una trama a la dirección IP de B (misma red), mirará su tabla ARP para poner en la trama la dirección destino física correspondiente a la IP de B.
De esta forma, cuando les llegue a todos la trama, no tendrán que deshacerla para comprobar si el mensaje es para ellos, sino que se hace con la dirección física

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

4. Protocolos de interconexión de redes

4.1. Protocolos utilizados en la interconexión redes privadas y públicas

RIP

Este protocolo por lo tanto no tiene en cuenta otros factores como pueden ser la velocidad o la carga del enlace por poner un ejemplo.
Los routers que utilizan RIP envían sus tablas completas cada 30 segundos via broadcast UDP.
El router receptor por su parte espera 180 segundos a recibir una actualización, y si en este tiempo no la recibe marca esta red como no operativa.
Si finalmente a los 240 segundos contínua sin haber recibido ningún tipo de actualización acaba por borrar dicha red de la tabla.
También es importante destacar que hay dos versiones de RIP, RIP I y RIP 2 este último descrito en la RFC 1723 y 1388.
La última versión de RIP incorpora algunas mejoras como son por ejemplo que la versión 2 permite utilizar máscaras variables y crear subredes (anteriormente RIP no enrutaba subredes).
Esta versión anuncia el número de saltos, a parte del número de red.

Configuración.

Consiste básicamente en activar RIP mediante el comando "router rip" y en anunciar las redes directamente conectadas por las que se desea que se envíen y reciban paquetes de actualización mendiante el comando "network X.X.X.X".
En el ejemplo sólo conoce la red 10.0.0.0 que es una clase A.
Es importante destacar que con el comando network sólo se anuncia la clase entera.

Ejemplo:

```
conf t
RouterA (config) #router rip
RouterA (config-router) #network 10.0.0.0
RouterA (config-router) #^Z
RouterA#show running
hostname RouterA
!
interface serial0
ip address 10.1.0.1 255.255.255.0
!
interface serial1
ip address 10.2.0.1 255.255.255.0
!
router rip
network 10.0.0.0
!
no ip classeless
end
```

Comandos de verificación.

- **debug ip rip:** Si activamos el comando "debug ip rip" en el router1 podemos obtener la siguiente información:

  Ejemplo:

  ```
  router1#debug ip rip
  router1#show log
  RIP: received v1 update from 131.108.2.2 on Serial0
  131.108.5.0 in 1 hops
  137.99.0.0 in 1 hops
  RIP: sending v1 update to 255.255.255.255 via Serial0 (131.108.2.2)
  subnet 131.108.5.0, metric 1
  ```

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

network 137.99.0.0, metric 1

- **sh ip protocols**: Este comando nos muestra como está configurado el protocolo de ruteo en el interfaz. A continuación se muestra un ejemplo.

  Ejemplo:

  Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 24 seconds
  Invalid after 180 seconds, hold down for 180, flushed after 240
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Default version control: send version 1, receive any version
  Redistributing: rip
  Default version control: send version 1, receive any version
  InterfaceSendRecvkey-chain
  Bri0 11 2
  Ethernet011 2
  Serial0 11 2
  Serial1 11 2
  Routing for Networks:
  131.108.0.0
  192.31.7.0
  Routing Information Sources:
  GatewayDistanceLast Update
  131.108.2.2011200:00:08
  131.108.200.21205d15
  131.108.2.2001200:00:09
  131.108.2.2031200:00:11
  Distance: (default is 120)

- **sh ip route:** Este comando nos muestra información sobre todas las rutas que el router conoce para enrutar paquetes ip.

  Ejemplo:

  Codes: I - IGRP derived, R - RIP derived, H - HELLO derived
  C - connected, S - static, E - EGP derived, B - BGP derived
  ** - candidate default route*
  Gateway of last resort is 131.108.1.6 to network 129.140.0.0
  R 10.0.0.0 [120/1] via 192.31.7.130, 11 sec, Serial2
  R 129.140.0.0 [120/1] via 131.108.1.6, 21 sec, Ethernet0
  C Net 192.31.7.0 is subnetted (mask is 255.255.255.240), 3 subnets
  R 192.31.7.144 [120/2] via 192.31.7.114, 30 sec, Serial6
  C 192.31.7.16 is directly connected, Ethernet2
  C 192.31.7.48 is directly connected, Serial0

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

IGRP

Al igual que RIP, IGRP es un protocolo vector distancia que utiliza varias métricas distintas como pueden ser el retardo o el ancho de banda.
IGRP fue desarrollado por CISCO como sustituto de RIP.
Este nuevo protocolo de ruteo incorpora algunas mejoras respecto a RIP que le hacen ser un protocolo vector distancia avanzado.
Como principal característica se puede decir que el cálculo de la métrica es algo más complejo que con RIP, ya que este protocolo no utiliza el número de saltos para calcular la métrica, para ello tiene en cuenta otros factores como el ancho de banda, el retardo, la fiabilidad, la carga y MTU.
Aunque IGRP no utiliza el número de saltos como métrica puede proporcionar información de encaminamiento para una ruta de hasta 255 saltos, lo que le convierte en un protocolo idóneo para grandes redes.
Otra característica importante es que las actualizaciones de tablas se realizan cada 90 segundos y que en estas actualizaciones no siempre se envía el contenido completo de la tabla de ruteo, esto hace que la convergencia sea más rápida que en el caso de RIP.
Por último es importante destacar que también soporta lo que se denomina Balanceo de Carga Multipath.
Al igual que RIP, IGRP es un protocolo vector distancia que utiliza varias métricas distintas como pueden ser el retardo o el ancho de banda.
IGRP fue desarrollado por CISCO como sustituto de RIP.
Este nuevo protocolo de ruteo incorpora algunas mejoras respecto a RIP que le hacen ser un protocolo vector distancia avanzado.
Como principal característica se puede decir que el cálculo de la métrica es algo más complejo que con RIP, ya que este protocolo no utiliza el número de saltos para calcular la métrica, para ello tiene en cuenta otros factores como el ancho de banda, el retardo, la fiabilidad, la carga y MTU.
Aunque IGRP no utiliza el número de saltos como métrica puede proporcionar información de encaminamiento para una ruta de hasta 255 saltos, la cual cosa le convierte en un protocolo idóneo para grandes redes.
Otra característica importante es que las actualizaciones de tablas se realizan cada 90 segundos y que en estas actualizaciones no siempre se envía el contenido completo de la tabla de ruteo, esto hace que la convergencia sea más rápida que en el caso de RIP.
Por último es importante destacar que también soporta lo que se denomina Balanceo de Carga Multi path.

Configuración.

Consiste básicamente en activar IGRP mediante el comando “router igrp XXX” y en anunciar las redes que conoce mediante el comando “network X.X.X.X “.
Como en el caso de RIP sólo anunciamos las redes directamente conectadas por las que se desee que se envíen y reciban paquetes de actualización de rutas.
Otro parámetro que es importante destacar es que cuando utilizamos IGRP se ha de indicar el AS o número de sistema autónomo (que por defecto es uno).
Este número es importante porque cada router sólo intercambiará las actualizaciones entre los routers con su mismo AS.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Ejemplo:

conf t
Router A (config) #router igrp 100
Router A (config-router) #network 172.31.0.0
Router A (config-router) #network 172.41.0.0
Router A (config-router) #^Z
RouterA#show running
hostname Router A
!
interface serial0
ip address 172.31.0.1 255.255.255.0
!
interface serial1
ip address 172.41.0.1 255.255.255.0
!
router igrp 100
network 131.41.0.0
network 172.31.0.0
!
no ip classless
!
end

Comandos de verificación.

Se utilizan básicamente los mismos que en RIP:

- **sh ip protocols:** Este comando nos muestra como está configurado el protocolo de ruteo en el interfaz. A continuación se muestra un ejemplo:

Ejemplo:

Routing Protocol is "igrp 100"
Sending updates every 90 seconds, next due in 88 seconds
Invalid after 270 seconds, hold down for 280, flushed after 630
Outgoing update filter list for all routes is not set
Incoming update filter list for all routes is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
IGRP maximum hopcount 100
Redistributing: igrp 109
Routing for Networks:
131.108.0.0
192.31.7.0
Routing Information Sources:
Gateway Distance Last Update
131.108.2.201 100 0:00:08
131.108.200.2 100 5d15
131.108.2.200 100 0:00:09
131.108.2.203 100 0:00:11

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

- **sh ip route:** Este comando nos muestra información sobre todas las rutas que el router conoce para enrutar paquetes ip.
  Ejemplo:
  Codes: I - IGRP derived, R - RIP derived, H - HELLO derived
  C - connected, S - static, E - EGP derived, B - BGP derived
  ** - candidate default route*
  Gateway of last resort is 131.108.1.6 to network 129.140.0.0
  *I*Net 10.0.0.0 [100/28476] via 192.31.7.130, 11 sec, Serial2*
  *I*Net 129.140.0.0 [100/9576] via 131.108.1.6, 21 sec, Ethernet0*
  via 131.108.2.6, 21 sec, Ethernet1
  via 192.31.7.26, 21 sec, Ethernet2
  I Net 128.18.0.0 [100/8576] via 192.31.7.130, 11 sec, Serial2
  C Net 192.31.7.0 is subnetted (mask is 255.255.255.240), 3 subnets
  I 192.31.7.144 [100/1002100] via 192.31.7.114, 30 sec, Serial6
  C 192.31.7.16 is directly connected, Ethernet2
  C 192.31.7.48 is directly connected, Serial0
  I Net 192.12.33.0 [100/8576] via 192.31.7.130, 11 sec, Serial2
  C Net 131.108.0.0 is subnetted (mask is 255.255.255.0), 1 subnet
  I 131.108.205.0 [100/1004200] via 131.108.1.6, 21 sec, Ethernet0
- **debug ip igrp transactions y debug ip igrp events**. El primer comando nos muestra todos los updates de igrp transmitidos y enviados. El segundo comando sin embargo nos enseñará un resumen de todos los updates.

EIGRP

EIGRP (Enhanced Interior Routing Protocol) es un protocolo híbrido de routing propietario de CISCO, basado en la tecnología vector distancia y estado de enlace que soporta hasta 224 saltos.
Una de las principales características es que este protocolo de routing al ser híbrido combina las cualidades de los protocolos vectores distancia y de los de estado de enlace siendo capaz de crear y mantener las tablas de forma independiente al protocolo que se quiera utilizar, ya sea IP, IPX o Appletalk.
También es importante destacar la rápida convergencia que se consigue gracias a un algoritmo llamado DUAL (diffusing update algoritm).
Este algoritmo entre otras cosas permite al router almacenar rutas de backup alternativas en caso de que la ruta principal fallase.
En el caso de que no existiese una ruta de backup alternativa EIGRP pregunta a sus vecinos una ruta alternativa.
Otra característica importante es que en los updates o intercambio de tablas este protocolo consume un menor ancho de banda debido a que nunca envía la tabla completa, solo envía los cambios.
Esto sirve para saber cuáles son los routers que están activos.
La métrica se obtiene de cálculos basados en el ancho de banda, el retardo, la fiabilidad, la carga y el MTU (máximum transmisión unit).
Los parámetros más importantes para el cálculo de la métrica son el ancho de banda y el retardo.
Configuración.
En lo correspondiente a la configuración es similar a la de IGRP, utilizaremos los comandos “router eigrp XX” y “network XXXX”.
Como en el caso de IGRP el parámetro que se le asigna al comando “router eigrp “, es el AS (autonomous system) que ha de ser el mismo para todos los routers.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Ejemplo:

```
conf t
Router A (config) #router eigrp 1
Router A (config-router) #network 172.31.0.0
Router A (config-router) #network 172.41.0.0
Router A (config-router) #network 10.0.0.0
Router A (config-router) #^Z
RouterA#show running
Hostname Router A
!
interface serial0
ip address 172.31.0.1 255.255.255.0
!
interface serial1
ip address 172.41.0.1 255.255.255.0
!
interface ethernet1
ip address 10.41.0.1 255.255.255.0
!
router igrp 100
network 172.41.0.0
network 172.31.0.0
network 10.0.0.0
!
End
```

Comandos de verificación.
Entre los comandos existentes destacan:
–show ip route eigrp: Este comando nos muestra las entradas de eigrp existentes en la tabla.
Ejemplo:

```
Router# show ip route
Codes: I - IGRP derived, R - RIP derived, O - OSPF derived
C - connected, S - static, E - EGP derived, B - BGP derived
i - IS-IS derived, D - EIGRP derived
* - candidate default route, IA - OSPF inter area route
E1 - OSPF external type 1 route, E2 - OSPF external type 2 route
L1 - IS-IS level-1 route, L2 - IS-IS level-2 route
EX - EIGRP external route
Gateway of last resort is not set
160.89.0.0 is variably subnetted, 6 subnets, 2 masks
D 160.89.90.0 255.255.255.0
[90/46251776] via 160.89.80.28, 0:04:18, Ethernet0
[90/46251776] via 160.89.81.28, 0:04:18, Ethernet1
C 160.89.81.0 255.255.255.0 is directly connected, Ethernet1
C 160.89.80.0 255.255.255.0 is directly connected, Ethernet0
D 160.89.82.0 255.255.255.0
[90/307200] via 160.89.80.31, 0:04:18, Ethernet0
C 160.89.62.0 255.255.255.0 is directly connected, Serial0
S 160.89.0.0 255.255.0.0 [1/0] via 160.89.80.240
```

–show ip eigrp neighbors: Nos muestras los vecinos descubiertos vía eigrp.
Ejemplo:

```
Router# show ip eigrp neighbors
IP-EIGRP Neighbors for process 77
```

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Address Interface Holdtime Uptime Q Seq SRTT RTO
(secs) (h:m:s) Count Num (ms) (ms)
160.89.81.28 Ethernet1 13 0:00:41 0 11 4 20
160.89.80.28 Ethernet0 14 0:02:01 0 10 12 24
160.89.80.31 Ethernet0 12 0:02:02 0 4 5 20
- show ip eigrp topology: Este comando nos muestra el árbol lógico creado a partir de la tabla topológica de EIGRP.
Ejemplo:
Router# show ip eigrp topology
IP-EIGRP Topology Table for process 77
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - Reply status
P 160.89.90.0 255.255.255.0, 2 successors, FD is 0
via 160.89.80.28 (46251776/46226176), Ethernet0
via 160.89.81.28 (46251776/46226176), Ethernet1
via 160.89.80.31 (46277376/46251776), Ethernet0
P 160.89.81.0 255.255.255.0, 1 successors, FD is 307200
via Connected, Ethernet1
via 160.89.81.28 (307200/281600), Ethernet1
via 160.89.80.28 (307200/281600), Ethernet0
via 160.89.80.31 (332800/307200), Ethernet0
–show ip protocols: Este comando nos muestra como está configurado el protocolo de ruteo en el interfaz.
Ejemplo:
Router# show ip protocols
Routing Protocol is “eigrp 77”
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: eigrp 77
Automatic network summarization is in effect
Routing for Networks:
160.89.0.0
Routing Information Sources:
Gateway Distance Last Update
160.89.81.28 90 0:02:36
160.89.80.28 90 0:03:04
160.89.80.31 90 0:03:04
Distance: internal 90 external 170
–show ip eigrp traffic: Este comando es útil para determinar si el protocolo está sobre-activo debido a inestabilidad en la red.
Ejemplo:
Router# show ip eigrp traffic
IP-EIGRP Traffic Statistics for process 77
Hellos sent/received: 218/205
Updates sent/received: 7/23
Queries sent/received: 2/0
Replies sent/received: 0/2
Acks sent/received: 21/14

OSPF

OSPF es un protocolo de link-state o estado de enlace que está definido en el RFC 1247, OSPF versión 2 se define en la RFC 1583.
Los protocolos de link-state a diferencia de los protocolos vector distancia que envían la tabla de rutas a sus vecinos, envían el estado de sus enlaces a los routers de su área jerárquica.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Es importante destacar que no solo se envía información del estado del router, sino que también se envía información con el número de saltos, la capacidad, el retardo y la fiabilidad del enlace.
En función de estos datos y utilizando el algoritmo de Dijkstra se elabora la tabla de ruteo, permitiendo elegir la mejor ruta para un mismo camino e incluso permitiendo el balanceo de carga por hasta cuatro caminos de igual métrica.
Normalmente la red suele dividirse en áreas de tal manera que sólo los routers de un área se envían paquetes con link-states.
Estas áreas se conectan entre sí mediante routers frontera.
Es importante destacar que en redes muy malladas con OSPF se consigue una velocidad de convergencia mucho mayor que con otros protocolos como por ejemplo RIP.
OSPF es un protocolo de link-state o estado de enlace que está definido en el RFC 1247, OSPF versión 2 se define en la RFC 1583.
Los protocolos de link-state a diferencia de los protocolos vector distancia que envían la tabla de rutas a sus vecinos, envían el estado de sus enlaces a los routers de su área jerárquica.
Es importante destacar que no solo se envía información del estado del router, sino que también se envía información con el número de saltos, la capacidad, el retardo y la fiabilidad del enlace.
En función de estos datos y utilizando el algoritmo de Dijkstra se elabora la tabla de ruteo, permitiendo elegir la mejor ruta para un mismo camino e incluso permitiendo el balanceo de carga por hasta cuatro caminos de igual métrica.
Normalmente la red suele dividirse en áreas de tal manera que sólo los routers de un área se envían paquetes con link-states. Estas áreas se conectan entre sí mediante routers frontera.
Es importante destacar que en redes muy malladas con OSPF se consigue una velocidad de convergencia mucho mayor que con otros protocolos como por ejemplo RIP.
–OSPF se recomienda en:
·Redes muy malladas con topología complicada en las cuales la convergencia de RIP pueda ser algo lenta.
·Cuando se necesite interconectar routers de diferentes fabricantes.
·Si se requiere balanceo de carga por líneas redundantes.

BGP

Características de BGP

Estas características demuestran por qué este protocolo es el mejor para routing exterior.
Las claves principales de BGP incluyen:
–Es un protocolo de routing path vector.
–BGP soporta VLSM, CIDR y sumarización.
–En el inicio de la sesión de envían actualizaciones completas; las actualizaciones por disparo se enviarán posteriormente.
–Se crean y mantienen las conexiones entre peers utilizando el puerto 179/TCP.
–La conexión se mantiene por keepalives periódicos.
–Cualquier cambio en la red resulta una actualización por disparo.
–Las métricas utilizadas por BGP, llamadas atributos, permiten gran granularidad en la selección del camino.
–El uso de direccionamiento jerárquico y la capacidad de manipular el flujo de tráfico son unas de las características que permiten al diseño de la red crecer.
–BGP tiene su propia tabla de routing, sin embargo es capaz de compartir y preguntar sobre la tabla de routing IP interior.
–Es posible manipular el flujo de tráfico utilizando atributos. Esto significa que una ruta no puede enviar tráfico si el siguiente salto no quiere.
–Una de las mayores caruta por defecto en el AS y una ruta estática es el AS del ISP o de la organización.
–Una característica distintiva de BGP son sus actualizaciones.
–A BGP no le interesa comunicar un conocimiento de cada subred de la organización, sólo le interesa utilizar suficiente información para encontrar un AS.
–Las actualizaciones de routing de BGP lleva la sumarización al extremo comunicando únicamente los números de los AS, prefijos de direcciones agregadas e información de routing basada en políticas.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

–BGP asegura la fiabilidad del transporte llevando sus actualizaciones de routing y sincronizando las actualizaciones de routing.
–BGP puede ser implementado de diferentes formas:
·Entre AS: En este momento actúa como un protocolo de pasarela exterior, entonces lo llamaremos eBGP.
·Dentro de una AS: BGP se puede utilizar para llevar información exterior entre routers eBGP que residen en el mismo AS, entonces lo llamaremos iBGP.
BGP es un protocolo de routing avanzado vector distancia
›Utiliza TCP para gestión de la sesión fiable
›Utiliza el puerto 179/TCP

IS-IS

IS-IS es un protocolo de enrutamiento interior desarrollado en los años 80 por Digital Equipment (DEC) y llamado originalmente DECnet Phase V.
Después fue adoptado por la International Standard Organization (ISO) como protocolo de enrutamiento para la Interconexión de Sistemas Abiertos (OSI).
Su desarrollo estuvo motivado por la necesidad de un sistema no propietario que pudiera soportar un gran esquema de direccionamiento y un diseño jerárquico.
Los grandes proveedores de servicios de Internet han venido usando IS-IS desde su introducción y recientemente se ha comenzado a implementar en otros mercados.
IS-IS permite trabajar con Type of Service (ToS) para la ingeniería de tráfico, aunque esta característica no estaba todavía implementada en la IOS de Cisco.
Al igual que OSPF, IS-IS utiliza el algoritmo Dijkstra (Shortest Path First –SPF) para el cálculo de rutas y tiene una jerarquía de dos capas; pero mientras que OSPF suele emplearse como solución empresarial (aunque también en ISPs), IS-IS sólo suele verse en ISPs.
Estos dos protocolos mantienen un buen número de similitudes pero cada uno de ellos tiene un vocabulario propio.
Existen diferencias importantes en el modo de operar de IS-IS y OSPF, por ejemplo, en el modo en que la dirección de área es asignada.
En IS-IS, la dirección de área y de host son asignados al router entero, mientras que en OSPF el direccionamiento es asignado al nivel de interfaz.
Por lo tanto un router IS-IS únicamente estará en un área (todos los routers de Nivel 1 necesitan un router de Nivel 1-2 para conectarles a otra área).
El router de Nivel 1-2 puede ver el resto del SA y se ofrece como ruta por defecto al área de Nivel 1.
El rol del DR es ligeramente diferente. El DIS en IS-IS existe para los Niveles 1 y 2 en los medios multiacceso, pero no existe un router designado de backup.
Mientras que en OSPF es elegido para “toda la vida”, en IS-IS si un router se levanta en la red con una prioridad mayor, el DIS existente es depuesto.
En IS-IS cada router formas una adyacencia con cada uno de los otros routers del medio.
Sin embargo, los paquetes de estado-enlace (LSPs, equivalentes a los LSAs de OSPF) son enviados solamente por el DIS.
Mientras que OPSF está encapsulado sobre IP, IS-IS es independiente del protocolo de Capa de Red, corre directamente en lo alto de la Capa de Enlace de Datos.

Estructura Jerárquica en IS-IS

Se definen dos tipos de routers:
Un router de Nivel 1 negocia el primer nivel de enrutamiento, encontrando el destino final dentro del área.
Un router de Nivel 2 encuentra el área dentro de la que se encuentra el destino final.
Ambos tipos de routers se combinan con los routers de Nivel 1-2 que corren ambos procesos de Nivel 1 y 2 y pueden ser considerados como un tercer tipo de router.
–Router de Nivel 1: O router Intra-área. Es similar a un Stub Router en OSPF.
Su conocimiento de la red es limitado al área y emplea una ruta por defecto al router de Nivel 2 más cercano para enrutar tráfico externo al área donde se encuentra.
Los router de Nivel 1 tienen una base de datos de estado-enlace idéntica entre ellos.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

–Router de Nivel 2: Router Inter-area. Son necesarios para el enrutamiento entra áreas distintas tal como los routers de backbone en OSPF.
Los routers de Nivel 2 se comunican via Hellos que sólo son comprendidos entre ellos.
Su base de datos de estado-enlace es también idéntica.
–Router de Nivel 1-2: Son routers tanto Intra como Inter-área, una característica similar a los routers fronterizos de área en OSPF, que pueden tener vecinos en diferentes áreas porque envían Hellos tanto de Nivel 1 como de Nivel 2 y por tanto pueden comunicarse con ambos tipos de routers.
Almacenan una base de datos de estado-enlace de Nivel 1 y otra para el Nivel 2 con la información necesaria para el enrutamiento Inter-área.
Estos routers informan a los routers de Nivel 1 de que son routers de Nivel 2 y que pueden enviar tráfico a otras áreas.
Pueden informar también a otros routers de Nivel 2 de las áreas a las que está conectado.
Esta es la configuración por defecto de un router Cisco.

Principios Básicos de Enrutamiento IS-IS

- Cuando un router recibe tráfico que enrutar a un destino remoto, realiza una consulta a su tabla de enrutamiento.
- El router extrae del paquete la información relativa al System ID y SEL para revelar la información de área de la dirección de destino. Si la dirección de destino de área es la misma que la suya, enruta el paquete hacia el System ID usando su base de datos de Nivel 1.
- Si el área de destino es diferente:
    - Si es un router de Nivel 1 envía el paquete al router de Nivel 2 más cercano.
    - Si se trata de un router de Nivel 2, busca la ruta en la base de datos de envío.
    - Resuelve la dirección al emparejamiento más largo (tendrá las rutas externas sumarizadas).

Áreas en IS-IS

Las áreas en IS-IS están definidas en el enlace, lo que significa que el router entero está en un área, al contrario que en OSPF, donde las áreas se definen el nivel de interfaz.
Para que las actualizaciones de enrutamiento de Nivel 2 puedan ser intercambiadas, todos los routers de Nivel 2 deben ser contiguos.
Redes e Interfaces
Los routers con una capa de enlace de datos común se convierten en vecinos IS-IS si los paquetes Hello que ambos intercambian cumplen ciertos criterios.
El proceso difiere ligeramente dependiendo del medio, pero la información que viaja en los paquetes Hello es esencialmente la misma.
Cada paquete declara el origen y las capacidades de la interfaz.
Una vez formada la adyacencia se produce el intercambio de información de enrutamiento en forma LSPs, de esta manera, cada router recaba la información de las redes conectadas de cada router para crear una tabla de topología detallada e idéntica.
Para crear o mantener una adyacencia, ambas interfaces deben concordar en lo siguiente:
–El tamaño máximo del paquete (MTU) debe ser el mismo.
–Cada uno de los routers debe estar configurado en el mismo Nivel de Enrutamiento (Niveles 1 ó 2) de manera que puedan decodificar los Hellos enviados por el otro router.
–Si ambos routers son de Nivel 1 deben estar configurados en la misma área.
–Para que un router de Nivel 1 pueda comunicarse con un router de Nivel 2, uno de ellos debe estar configurado como un router de Nivel 1-2.
–El System ID debe ser único para cada router.
–Si la autenticación está configurada, debe ser idéntica en ambos routers.
–Los intervalos de envío de Hellos (incluido el Holddown timer) deben coincidir, de otra manera resultaría en un enlace que flapea o cálculos DPF interminables.
IS-Is define dos tipos de red: subredes broadcast y redes punto-a-punto.
Adyacencias en Enlaces Punto-a-Punto: Un enlace punto-a-punto conecta dos routers.
Después de que cada uno de los routers reciba un paquete Hello, cada uno declara el otro extremo como alcanzable y cada extremo envía un CSNP, que contiene una lista de todos los enlaces almacenados en la BBDD de estado-enlace, lo que conlleva una sincronización de las BBDD de estado-enlace de cada máquina.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Los Hellos periódicos mantienen la adyacencia.
Si un router no recibe un Hello dentro del tiempo de espera (holdtime) el vecino es declarado caído y la BBDD purgada de cualquier entrada asociada a ese router.
El intervalo de Hellos por defecto es cada 10 seg. El holdtime es de 30 seg.
Adyacencias en enlaces Broadcast: En estos enlaces cada router sólo recibe paquetes enviados por el DIS (Designated Intermediate System) –esto se hace para controlar la cantidad de tráfico que necesita ser generada y mantener las adyacencias y las BBDD.
El DIS tiene la responsabilidad de inundar con LSPs a todos los sistemas IS-IS conectados, más exactamente, el DIS inyecta los LSPs para el pseudónimo.
El pseudónimo representa la LAN, con cada router simulando una interfaz en un router imaginario.
Este router imaginario es el llamado pseudónimo.
Como si fuera un router real, el pseudónimo inyecta un LSP cuando existe un cambio en el status de sus conexiones.
Las adyacencias con los otros routers son mantenidas por el DIS.
Si hay un problema con éste o un router con prioridad más alta aparece en la red, es identificado rápidamente y un nuevo router es elegido en lugar del viejo DIS.
La elección está basada en la prioridad y declarada en la interfaz.
En el caso de que todas estén configuradas por defecto a 64, el mayor número SNPA (dirección de enlace de datos) determina el DIS.
Adyacencias en enlaces NBMA: Un enlace NBMA no es ni un medio de Broadcast ni un enlace punto-a-punto.
Usando PVCs, las redes NBMA (FR, ATM, X.25) proporcionan múltiples conexiones con una sola interfaz, lo que puede ser visto como una forma de LAN.
La confusión surge cuando IS-IS ve que el enlace es multiacceso, como no tiene conocimiento de nubes WAN multiacceso, cree que el medio es alguna forma de LAN con capacidad de Broadcast.
Cisco recomienda que los enlaces sean configurados como una serie de enlaces punto-a-punto.

Tipos de paquetes IS-IS

Existen 3 tipos de paquetes:
–Hello. Crean y mantienen relaciones entre vecinos y adyacencias.
Pueden ser:
LAN Nivel 1. Generados por routers de Nivel 1 o 1-2.
LAN Nivel 2. Generados por routers de Nivel 2 o 1-2.
Punto-a-Punto. Generados por routers de Nivel 1, 2 y 1-2.
–LSP. Llevan información sobre los vecinos conectados al router. Pueden ser de dos tipos:
Nivel 1. Generados por routers de Nivel 1 o 1-2.
Nivel 2. Generados por routers de Nivel 2 o 1-2.
–Parqué de Número de Secuencia (SNP). Describen los LSPs en la BBDD de estado-enlace del router que transmite.
La información es condensada y nunca inundada, sino que sólo es vista entre vecinos.
Los SNP aseguran la sincronización de la BBDD de estado-enlace mediante grupos de distribución del LSPs en LAN y sin ACKs explícitos individuales, ACKs de LSPs individuales y, por último, la petición de LSPs al iniciarse.
Existen dos tipos de SNP para cada Nivel de enrutamiento:
·SNP Completo (CSNP), que incluye cada LSP en la BBDD: Nivel 1 y Nivel 2.
·SNP Parcial (PSNP), Incluye un subconjunto de LSPs, empleado para solicitar LSPs individuales y agradecer la recepción de estos LSPs: Nivel 1 y Nivel 2.

Operación de IS-IS Integrado

1.Los Routers IS-IS envían paquetes Hello por todas sus interfaces para descubrir vecinos y forma adyacencias.
2.Los routers que comparten un mismo enlace de datos se convierten en vecinos.
3.Crean paquetes de estado-enlace (LSPs) basados en las interfaces locales y en los prefijos de red aprendidos de los routers adyacentes.
Estos paquetes son enviados a todos los vecinos, excepto al vecino del que se recibió.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

4.Cuando se reciben nuevos o diferentes LSPs se añaden a la BBDD de estado-enlace.
5.Los routers calculan el algoritmo SPF para cada destino y construye el Shortest Path Tree (SPT) y la BBDD de envío (o tabla de enrutamiento).
Esto asegura que cada router tiene el mismo conjunto de LSPs y que las BBDD de estado-enlace son idénticas entre ellos.
Los LSP´s son generados ante los cambios en la red:
·Cuando una adyacencia se levanta o se cae.
·Cuando la interfaz de un router cambia de estado o se le asigna una nueva métrica.
·Cuando una ruta IP cambia (a causa de la redistribución, por ejemplo).

Métrica

IS-IS tiene cuatro métricas definidas en ISO 10589:
1.Default. Llamada Coste. Es la única que se establece obligatoriamente en el Standard. Cisco configura por defecto todas las interfaces con un valor de 10.
2.Delay (Retardo).
3.Expense (Gasto, costo).
4.Error (Confiabilidad de la ruta).
Las métricas ISO son configuradas en la interfaz de salida usando un entero entre 0 y 63.
Un campo de 10 bits describe la ruta total al destino, permitiendo un valor entre 0 a 1023.
Cisco incrementó el tamaño de la métrica a 24 bits.
La métrica por defecto o Coste es la única que actualmente soportan los routers CISCO que trabajan con IS-IS integrado.

Diseño de Áreas

Los típicos diseños IS-IS incluyen los siguientes:
1.Red plana con enrutamiento de Nivel 1. El diseño no es escalable pero a cambio sólo habrá una BBDD de SPF y no existirán problemas de enrutamiento subóptimo entre áreas.
2.Red plana con enrutamiento de Nivel 2. Si la red se expande se le añaden áreas de Nivel 1.
3.Red plana con enrutamiento de Nivel 1-2 (Cisco x defecto). Permite la migración sencilla a un diseño jerárquico que soluciona los problemas de enrutamiento subóptimo. Demanda más recursos de los routers al mantener dos BBDD SPF.
4.Red jerárquica donde el core corre enrutamiento de Nivel 2 y áreas de Nivel 1 conectándose al core. Routers de Nivel 1-2 crean las conexiones entre áreas.
Las desventajas son el consumo de recursos de los dispositivos y la posibilidad de enrutamiento subóptimo.
La configuración de la métrica de las interfaces de salida determinan las decisiones de enrutamiento, lo requiere un conocimiento detallado de la topología de la red.
Algunos desarrollos recientes permiten cierta filtración de rutas que permitiría a los routers de Nivel 2 pasar información de enrutamiento específica al Nivel 1.
La configuración por defecto de los routers Cisco en el Nivel 1-2 permite superar ciertas trampas potenciales, como por ejemplo el aislamiento de un área ante un problema de conexión entre routers de Nivel 1 y 2 si no existen rutas alternativas.

Sumarización de Rutas

Las reglas de sumarización en IS-IS son las mismas que en el diseño OSPF multi-área:
–Los routers de Nivel 1-2 pueden sumarizar las rutas que mantienen dentro de su área y propagarlas a los routers de Nivel 2. Similar a la sumarización que llevan a cabo los ABR en OSPF.
–Si un router de Nivel 1-2 está configurado para sumarización, esta se debe configurar en todos los routers que inyectan actualizaciones al Nivel 2 de la misma área.
Si un router no advirtiera rutas sumarizadas todo el tráfico destinado a esa área se le enviaría a él, ya que IS-IS usa enrutamiento por el emparejamiento más largo (la máxima coincidencia en la ruta para llegar al destino).
–No se pueden sumarizar rutas de Nivel 1 dentro de la misma área.

Configuración y Verificación de IS-IS Integrado

Para habilitar el proceso de enrutamiento IS-IS:
Ejemplo:

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Router(config)# router is is [optional tag]
La etiqueta (tag) es opcional y se emplea para proporcionar un nombre al proceso de enrutamiento si más de un proceso IS-IS se configura en el router.
El siguiente paso es configurar la NET para el proceso de enrutamiento:
Router(config-router)# net 00.000x.xyxy.xyxy.xyxy.00
La dirección contiene la dirección del área y el System ID para el router.
Para el que se puede utilizar una de las direcciones MAC del router.
Finalmente deben especificarse activamente las interfaces que participarán en el enrutamiento IS-IS.
Este es el equivalente al comando network de publicación de redes en otros protocolos de enrutamiento.
Ejemplo:
Router(config)# interface type number
Router(config-if)# ip router is is [tag]
Por defecto, los routers Cisco vienen configurados para participar en enrutamiento de Nivel 1-2.
El comando para designar un router como de Nivel 1, 2 o ambos es:
Ejemplo:
Router(config-router)# is-type {level-1|level-1-2|level-2-only}
Aunque el sistema esté funcionando como router de Nivel 1-2 se puede controlar el tipo de adyacencias que se establecen en base a la interfaz.
Por defecto, el router tratará de generar ambos tipos de adyacencias.
Ejemplo:
Router(config-if)# is is circuit-type {level-1|level-1-2|level-2-only}
Es posible configurar el coste para una interfaz determinada mediante la configuración de la métrica por defecto para el enrutamiento de Nivel 1 o de Nivel 2.
Ejemplo:
Router(config-if)# isis metric default-metric {level-1|level-2}
Para configurar el intervalo entre hellos en función de la interfaz:
Ejemplo:
Router(config-if)# isis hello-interval seconds {level-1|level-2}
Es posible configurar el número de segundos entre retransmisiones de las PDUs de estado-enlace (LSPs) en los enlaces punto-a-punto.
El número de segundos debe ser un número entero mayor que el round-trip delay entre cualesquiera dos ISs de la red. Debemos ser conservadores si no queremos un gran número de retransmisiones:
Ejemplo:
Router(config-if)# isis retransmit-interval seconds
Para configurar el retraso entre transmisiones de paquetes estado-enlace por interfaz:
Ejemplo:
Router(config-if)# isis lsp-interval milliseconds
Para especificar el número de paquetes hello que un vecino debe echar de menos antes de declarar la adyacencia caída (por defecto es 3):
Ejemplo:
Router(config-if)# isis hello-multiplier multiplier {level-1|level-2}
Por supuesto, es posible configurar la prioridad para determinar la elección del Sistema Intermedio Designado (DIS):
Ejemplo:
Router(config-if)# isis priority value {level-1|level-2}
Asignación de contraseñas. Se pueden asignar contraseñas diferentes para los distintos niveles de enrutamiento.
Si no se determina un Nivel particular el Nivel por defecto es 1.
La autenticación está deshabilitada por defecto, para habilitarla:
Ejemplo:
Router(config-if)# isis password password {Nivel-1|Nivel-2}
Es posible forzar una ruta por defecto dentro de un dominio de enrutamiento IS-IS.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

A menos que específicamente se configure la redistribución de rutas en el dominio, los routers Cisco no lo harán.
El siguiente comando fuerza al router fronterizo a redistribuir la ruta por defecto o generar una ruta por defecto en su LSP de Nivel 2.
Es posible también utilizar un route-map para advertir la ruta por defecto dependiendo de la existencia de otra ruta en la tabla de enrutamiento.
Ejemplo:
Router(config-router)# default-information originate [route-map map-name]
Para sumarizar direcciones de un Nivel dado:
Ejemplo:
Router(config-router)# summary-address address mask {level-1|level-1-2| level-2}
Uno de los comandos de verificación y solución de problemas más útiles en IS-IS es:
Ejemplo:
show clns {protocols|interface|neighbors}
Aunque IS-IS sólo esté funcionando con IP, es necesario inspeccionar la información CLNS como las adyacencias entre vecinos.
El comando show is is route proporciona información sobre las rutas de Nivel 1 y el comando show clns route muestra la información de Nivel 2 de la tabla de enrutamiento.
Para ver los contenidos de la BBDD de estado-enlace: show isis database.
El comando show isis spf-log proporciona información sobre la frecuencia y motivos por los que un router ha corrido una sesión de cálculo completa SPF.
Los comandos debug IS-IS más frecuentemente utilizados son debug isis adj-packets y debug isis update-packets.

4.1.1. Clasificación según sus funciones

Protocolo IGP

Diseñar redes que utilicen exclusivamente rutas estáticas, sería tedioso administrarlas y no responderían bien a las interrupciones y a los cambios de topología que suelen suceder con cierta frecuencia.
Para responder a estos problemas se desarrollaron los protocolos de enrutamiento dinámico.
Los protocolos de enrutamiento dinámico son algoritmos que permiten que los routers publiquen, o anuncien, la existencia de la información de ruta de red IP necesaria para crear la tabla de enrutamiento.
Dichos algoritmos también determinan el criterio de selección de la ruta que sigue el paquete cuando se le presenta al router esperando una decisión de switching.
Los objetivos del protocolo de enrutamiento consisten en proporcionar al usuario la posibilidad de seleccionar la ruta idónea en la red, reaccionar con rapidez a los cambios de la misma y realizar dichas tareas de la manera más sencilla y con la menor sobrecarga del router posible.
Los protocolos de enrutamiento se dividen en dos categorías principales:
protocolos de gateway interior (Interior Gateway Protocols, IGP) y protocolos de gateway exterior (Exterior Gateway Protocols, EGP).

Los protocolos IGP están diseñados para intercambiar información sobre la red y las subredes entre los routers de un sistema autónomo; es decir, entre routers que ejecutan un protocolo de enrutamiento común en el marco de un dominio administrativo.
Los protocolos EGP están diseñados para intercambiar exclusivamente información sobre la red entre routers que pertenezcan a diferentes sistemas independientes.
El protocolo EGP con mayor utilización en la actualidad es el protocolo de gateway fronterizo versión 4 (Boarder Gateway Protocol 4, BGP-4).
Es el protocolo de enrutamiento predominante utilizado para intercambiar información entre empresas, proveedores de servicios de red en Internet.
Entre los protocolos IGP; los dos atributos principales que diferencian uno de otro son la metodología de propagación y el hecho de que sean con o sin clase.
Los dos métodos más comunes de propagación son el vector de distancia y el estado de enlace.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

En el método de vector de distancia, todos los routers envían las tablas de enrutamiento, completa o parcialmente, a los routers vecinos en mensajes de actualización de intervalos de tiempo regulares.
A medida que la información de enrutamiento se va repartiendo por la red, los routers pueden calcular la distancia a todas las redes y subredes de la Intranet.
Con el método de estado de enlace, cada router envía información de conexión local completa a todos los demás routers de la Intranet.
Como cada router recibe toda la información de conexión local, puede crear una imagen completa de la Intranet al ejecutar un complejo algoritmo llamado Primero la ruta más corta (Shortest Path First, SPF) en contraste con la información de conexión.
Los protocolos IGP también se diferencian por ser con o sin clase.
Los protocolos de enrutamiento con clase no poseen la capacidad de intercambiar información de máscara de red entre los diferentes routers.
Por esa razón, estos protocolos deben asumir que se ha aplicado una máscara de red o subred uniforme al espacio de direcciones común de la red.
Esta limitación prohíbe el uso de máscaras de subred de longitud variable (VLSM), por lo que la utilización del espacio de direcciones de la red no alcanza un nivel óptimo.
Asimismo no se puede pasar entre los routers la información de máscara de red, de manera que la información de las direcciones de red se debe resumir en los límites de las direcciones de red con clase.
Los protocolos de enrutamiento con clase son entre otros, el protocolo de información de enrutamiento (Routing Information Protocol, RIP) versión 1 y el protocolo de enrutamiento de gateway interior (Interior Gateway Protocol, IGRP).
Protocolo usado por los vecinos interiores para intercambiar Información de accesibilidad, las conexiones se realizan en redes de ruteo interno.
Protocolos de ruteo interno: RIP, OSPF
RIP (Routing Information Protocol): Protocolo de información de encaminamiento, utiliza el protocolo UDP y se comunica a través del Puerto 520.
Fácil de configurar, aunque para calcular una ruta sólo tiene en cuenta por cuántas máquinas pasará, y no otros aspectos más importantes como el Ancho de banda.
OSPF (Open Shortest Path First): Utiliza el algoritmo de Dijkstra para calcular la ruta más corta.
Es el más utilizado en redes grandes, pues se puede descomponer en otras más pequeñas para facilitar la configuración.
Una red OSPF está dividida en grupos lógicos de encaminadores o áreas cuya información se puede resumir para el resto de la red.
Se basa en las normas de código abierto, lo que significa que muchos fabricantes lo pueden desarrollar y mejorar.

Protocolo EGP

EGP (Exterior Gateway Protocol) es un protocolo utilizado para el intercambio de información de encaminamiento entre pasarelas exteriores (que no pertenezcan al mismo Sistema Autónomo AS).
Las pasarelas EGP sólo pueden retransmitir información de accesibilidad para las redes de su AS.
La pasarela debe recoger esta información, habitualmente por medio de un IGP (Internal Gateways Protocol), usado para intercambiar información entre pasarelas del mismo AS.
El protocolo EGP se basa en el sondeo periódico empleando intercambios de mensajes Hello/I Hear You, para monitorizar la accesibilidad de los vecinos y para sondear si hay solicitudes de actualización.
EGP restringe las pasarelas exteriores al permitirles anunciar sólo las redes de destino accesibles en el sistema autónomo de la pasarela.
De esta forma, una pasarela exterior que usa EGP pasa información a sus vecinos EGP pero no anuncia la información de accesibilidad de estos (las pasarelas son vecinos si intercambian información de encaminamiento) fuera del sistema autónomo.
El gateway no hace (no debe hacerlo) informar rutas para otros sistemas autónomos de los cuales no forme parte.
El administrador de red decidirá que gateways informarán a cuales otros gateways en otros sistemas.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

En la práctica todos son informados de esa disponibilidad, debido a que no existe un método común para determinar rutas.
Por lo tanto los gateways centrales que reciben múltiples rutas para un gateway dado no pueden usar la información de distancia para saber cuál ruta es la mejor.
EGP se utiliza para informar de rutas hacia los gateways centrales, y estos construyen un modelo de disponibilidad de localización, el cual resulta en una topología en árbol.
Solo los gateways centrales saben cómo alcanzar cualquier red en Internet.
EGP1 y EGP2 extienden el protocolo para introducir el concepto de coste de routing y no únicamente su alcance.
Esto se realiza haciendo una escala de la información de la distancia donde se atraviesan los límites de un sistema autónomo.
Un dominio de direccionamiento es un grupo de redireccionadores que usan un IGP (Internal Gateways Protocol) común.
Una forma de reducir el volumen de información intercambiado se basa en que un dominio de redireccionamiento utilice un Gateway seleccionado para comunicar información de direccionamiento con los Gateways seleccionados de otros dominios.
El Gateways seleccionado se considera como un Gateways exterior, y el protocolo usado entre Gateways exteriores es el EGP.
–Soporta un protocolo NAP ("Neighbor Acquisition Protocol). Dos pasarelas se pueden considerar vecinas si están conectadas por una red que es transparente para ambas.
EGP no específica la forma en que una pasarela decide inicialmente que quiere ser vecina de otra.
Para convertirse en vecina, debe enviar un mensaje "Acquisition confirm" como respuesta a un Acquisition Request.
Este paso es necesario para obtener información de encaminamiento de otra pasarela.
–Soporta un protocolo NR ("Neighbor Reachability"). La pasarela lo usa para mantener información en tiempo real sobre la accesibilidad de sus vecinos.
El protocolo EGP proporciona dos tipos de mensajes para ese fin: un mensaje Hello y un mensaje I Hear You (respuesta a Hello).
–Soporta mensajes de actualización (o mensajes NR) que llevan
información de encaminamiento.
No se requiere ninguna pasarela para enviar mensajes NR a otra pasarela, excepto como respuesta a una petición de sondeo ("poll request").
–El principal inconveniente del protocolo EGP es que crea una estructura en forma de árbol, es decir que si hay problemas en Internet, los Gateways solo saben que hay problemas en el Gateways exterior.
–Entre router en sistemas autónomos diferentes
–Usualmente con conexión directa
–Con next-hop apuntando a si mismo
Un problema adicional con EGP tiene que ver con la cantidad de información intercambiada; a medida que el número de redes IP que conoce NSFNET aumenta, el tamaño de los mensajes NR aumenta también y la cantidad de tiempo necesaria para procesarlos se hace significativa.
BGP-3 ha sustituido a EGP en la troncal NSFNET por estas razones.
Sin embargo, BGP-3, no requiere que NSFNET o cualquier otra troncal juegue un papel central.
En vez de eso, BGP-3 ve Internet como una colección de Ass, y no tiene en cuenta la topología interna de un sistema autónomo ni el IGP o IGPs que utilice.

4.1.2. Servicios soportados

Tras realizar una completa descripción de los protocolos que entran en juego en la interconexión de redes privadas con las redes públicas, y su clasificación dentro de los protocolos IGP o EGP, se va a presentar las diferentes tecnologías que pueden ser soportadas por los diferentes protocolos que se han descrito en los apartados anteriores.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Tecnología xdsl (línea de subscriptor digital).

xDSL se refiere como un grupo similar de tecnologías que proveen gran ancho de banda sobre circuitos locales de cable de cobre, sin amplificadores o repetidores de señal a lo largo de la ruta del cableado, entre la conexión del cliente y el primer nodo en la red.
xDSL es proveída sobe circuitos locales de cobre no cargados (cables sin ningún tipo de inducción de voltaje o señal).
La Tecnología xDSL soporta formatos y tasas de transmisión especificados por los estándares, como lo son T1 (.1544 Mbps) y E1 (2.048 Mbps), y es lo suficientemente flexible para soportar tasas y formatos adicionales como sean especificados (ej. 6 Mbps asimétricos para transmisión de alta velocidad de datos y video).
xDSL puede coexistir en el circuito con el servicio de voz.
Como resultado, todos los tipos de servicios, incluyendo el de voz existente, video, multimedia y servicios de datos pueden ser transportados sin el desarrollo de nuevas estrategias de infraestructura.
xDSL es una tecnología "Modem-Like" (muy parecida a la tecnología de los módem), donde es requerido un dispositivo xDSL terminal en cada extremo del circuito de cobre.
Estos dispositivos aceptan flujo de datos, generalmente en formato digital, y lo sobrepone a una señal análoga de alta velocidad.
Las tres técnicas de modulación usadas actualmente para xDSL son 2B1Q (2 Bit, 1 Quaternary), "carrier-less amplitude phase modulation" (CAP) y "discrete multitone modulation" (DMT).
xDSL provee configuraciones asimétricas o simétricas para soportar
requerimientos de ancho de banda en uno o dos sentidos.
Se refiere a configuraciones simétricas si el canal de ancho de banda necesario o provisto es el mismo en las dos direcciones ("upstream": sentido cliente-red, y "downstream": sentido red-cliente).
Aplicaciones asimétricas son esas en las cuales las necesidades de ancho de banda son mayores en una dirección que en la otra.
Por ejemplo, para "navegar" en el WWW, se requiere de un ancho de banda muy pequeño desde el cliente hasta su proveedor, dado que solamente se requiere lo necesario para pasar información de control y generalmente con algunos Kbps basta.
Mientras que en el otro sentido (desde el proveedor hasta el cliente), el ancho de banda requerido se podría expresar en Mbps.
Bajo el nombre xDSL se definen una serie de tecnologías que permiten el uso de una línea de cobre (la que conecta nuestro domicilio con la central Telefónica) para transmisión de datos de alta velocidad y, a la vez, para el uso normal como línea telefónica.
Se llaman xDSL ya que los acrónimos de estas tecnologías acaban en DSL, que está por "Digital Subscriber Line" (línea de abonado digital): HDSL, ADSL, RADSL, VDSL.
Cada una de estas tecnologías tiene distintas características en cuanto a prestaciones (velocidad de la transmisión de datos) y distancia de la central (ya que el cable de cobre no estaba pensado para eso, a cuanta más distancia peores prestaciones).
Entre estas tecnologías la más adecuada para un uso doméstico de Internet es la llamada ADSL.

ATM (Asynchronous Transfer Mode)

Es una tecnología de conmutación de alta velocidad, que utiliza el método de la multiplexación por división en el tiempo asíncrona.
La unidad de información en ATM es la celda, que se caracteriza, por tener una longitud fija de 53 octetos.
Esto permite que la conmutación de dichas celdas se realice por hardware, con lo que se consiguen velocidades de transmisión de hasta 622 Mbps.
Cada una de las celdas, está formada por una cabecera de 5 octetos, seguida por otros 48 octetos que contienen la información.
Dicha cabecera, contiene la información que permite identificar una comunicación, así como el tipo de información que transporta y la prioridad de descarte.
ATM se basa en conceptos sencillos, aunque potentes y flexibles.
ATM es una tecnología de conmutación basada en celdas o células de tamaño fijo que son re-ensambladas en el destino (no en los nodos intermedios de la Red).

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Las celdas ATM tienen una longitud de 53 bytes (5 bytes de información de control o protocolo seguidos de 48 bytes de información útil -voz, datos, vídeo, etc.-).
Al tratarse de celdas de tamaño fijo, pueden ser manejadas de forma más predecible, facilitando la manipulación de distintos tipos de tráfico sobre la misma Red.
Las celdas procedentes de las distintas fuentes de tráfico, son transmitidas a través de la misma línea mediante técnicas de multiplexación estadística.
La frecuencia de llegadas de celdas de una misma fuente es directamente proporcional al ancho de banda demandado por la misma.
Hoy en día, se utilizan redes distintas para transportar distintos tipos de tráfico (voz, datos, vídeo...) ya que cada tráfico tiene requisitos distintos a la hora de ser transmitido y conmutado.
Por ejemplo, el tráfico de datos suele ser a ráfagas con periodos de actividad prácticamente nulos seguidos de picos de información que tienen que ser transmitidos lo más rápidamente posible; mientras que el tráfico de voz y vídeo genera un flujo de información más continuado, pero es muy sensible a los retardos y al orden de llegada de la información al destino.
Con ATM, no serían necesarias varias redes independientes. ATM es el único estándar que ha sido definido desde el primer momento con el objetivo de soportar cualquier tipo de tráfico.
Históricamente se han utilizado soluciones tecnológicas distintas para la red de área amplia (WAN) y la red de área local (LAN).
La aparición de nuevos tipos de redes, como las de área metropolitana (MAN) y la globalización de las comunicaciones, no han hecho más que complicar el escenario con la introducción de mayor heterogeneidad y soluciones mixtas LAN-WAN.
ATM, en cambio, es una tecnología válida tanto para los entornos locales, como los metropolitanos y los de área amplia.
A medida que avance la implantación de sistemas basados en ATM, la frontera entre la LAN y la WAN se irá haciendo más borrosa y terminará desapareciendo (podrá diferenciarse únicamente entre redes basadas en infraestructura propia e infraestructura alquilada a un operador, pero todas ellas ATM).
ATM es una tecnología orientada a la conexión (pudiendo soportar varios trayectos - paths - virtuales en cada línea ATM y varios canales virtuales en cada trayecto), y es posible especificar los requerimientos (ancho de banda, retardo, prioridad de la información que va a ser cursada, etc.) de la misma en el momento en el que se establecen.
Estos parámetros, seleccionables por el usuario en cada conexión, determinarán la calidad de servicio de la comunicación, independientemente de lo que ocurra en el resto de la Red.
De esta forma, es posible bloquear una parte del ancho de banda total a una aplicación o servicio concreto sin que el tráfico generado por otras aplicaciones o usuarios pueda interferir, retardar o interrumpir la comunicación.
Destacar que ATM presupone por un lado la fiabilidad de los medios de transmisión (no se confirma la entrega de celdas, ni se retransmite aunque sí permite la detección de errores de cabecera, notificación de congestión y prioridad de descarte de celda) y por otro que los equipos finales se ajustarán a los parámetros de tráfico negociados en la conexión (traffic shaping).

Frame relay.

El servicio Frame Relay es un servicio de red que proporciona comunicaciones de datos de alta velocidad (64 Kbps a 2 Mbps) por conmutación de tramas entre la interfaz de los equipos de usuario, por ejemplo routers, brigdes, hosts, y los equipos de la red, como nodos.
Este servicio proporciona conexiones de altas prestaciones y se adapta perfectamente a las necesidades de interconexión de la Redes de Área Local y a las arquitecturas predominantes (OSI, SNA, DECNET, etc.).
La capacidad de enviar en ciertos periodos breves de tiempo un gran volumen de tráfico (“tráfico a ráfagas”) aumenta la eficiencia de las redes basadas en Frame Relay.
Se trata de un servicio orientado a conexión, tanto en su modalidad de conexión permanente mediante CVPs -Circuitos Virtuales Permanentes-, como en la de conexión conmutada con CVCs -Circuitos Virtuales Conmutados-.
Los CVPs son configurados en el momento de contratar el servicio mientras que los CVCs permiten al cliente establecer conexiones dinámicas bajo demanda.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

El servicio FR opera en la subcapa de retransmisión de tramas de la capa 2 del modelo de referencia de OSI. Hace uso solamente de la capa física y de una parte de la capa de enlace, lo cual le confiere mayor eficiencia que otros servicios (X.25) que operan en una capa superior del modelo OSI.
Al verse liberado el ancho de banda correspondiente a la sobrecarga de funciones como control de flujo, corrección de datos erróneos y confirmación de tramas, se produce un incremento en el caudal de la conexión.
Todas estas otras funciones deberán ser realizadas por otros protocolos de niveles superiores y que caen fuera del ámbito del servicio Frame Relay.
Frame Relay permite comunicaciones de datos por conmutación de paquetes a través del interface entre dispositivos de usuario (por ejemplo routers, bridges y hosts) y equipos de red (por ejemplo los nodos de conmutación).
Los dispositivos de usuario generalmente se conocen como equipos terminales de datos (DTE), mientras los equipos de la red, que hacen de interfaces con los DTEs, se les conocen como equipos de terminación del circuito de datos (DCE).
A esta interface se le denomina FRI:
Frame Relay Interface. Este interface está basado en la estructura de la trama LAP-D del canal D de señalización de la RDSI.
La red que soporta el interface frame relay puede ser o una red pública/privada por portadora o una red de equipos de propiedad del usuario sirviendo a la empresa.
Generalmente se hace uso de una operadora que disponga de dicho servicio por cuestiones prácticas.
El término “Relay” implica que la trama de datos de la capa 2 es conmutada en los nodos y/o procesada en los puntos extremos de cada enlace de red.

X.25

X.25 es un servicio de transmisión de datos apropiado para el intercambio de tráfico transaccional, transferencias de fondos, consultas a bases de datos, teleproceso, etc.
Es extremadamente fiable, garantizando la transmisión libre de errores entre terminales conectados a una misma red de conmutación de paquetes o a redes diferentes adecuadamente interconectadas.
Ofrece múltiples facilidades y opciones de uso que permiten un adecuado control sobre aspectos tales como seguridad, distribución del tráfico, etc.
El acceso al Servicio se suministra a través de líneas dedicadas que van desde las dependencias del cliente hasta el nodo de acceso al Servicio más próximo, con la posibilidad de incluir, como parte del Servicio, equipamiento adicional en casa del cliente encaminado a:
–establecer conexiones de respaldo de las líneas dedicadas
–concentrar tráfico sobre el acceso al Servicio
–permitir al cliente la gestión de sus propias conexiones

Ventajas

Calidad:
El compromiso de Calidad del Servicio se basa en la Disponibilidad de los accesos de cliente al Servicio y se garantiza mediante:
La infraestructura de red sobre la que se soporta el Servicio, y que se traduce en una fiabilidad y una capacidad de transmisión muy elevadas mediante la utilización de nodos de red de alta tecnología, la construcción del núcleo de red (backbone) sobre enlaces a 34 Mbit/s, una arquitectura de red completamente redundante, tanto en nodos como en enlaces
En la posibilidad de contratar nodos de Red instalados en casa de cliente a través del Servicio Nodo de Red.
Normalización:
Libertad en la elección de equipos de cliente, al tratarse de un Servicio basado en un protocolo estándar soportado por la práctica totalidad de los fabricantes
Seguridad:
En el acceso al Servicio, mediante la posibilidad de respaldo RTB/ RDSI, y la contratación de accesos multienlace.
En el transporte, ya que las técnicas de conmutación de paquetes y de protección de errores utilizadas en la Red garantizan el transporte y entrega de información con total fiabilidad y seguridad.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

En las conexiones del cliente al Servicio, mediante la creación de Grupo cerrado de Usuarios, y la posibilidad de cifrar los datos que viajan por la Red.

X.25 over TCP/IP -XOT- (X. 25 sobre TCP/IP)

El Interfaz XOT permite el transporte de paquetes X.25 sobre redes TCP/IP, lo que exige la existencia de un nivel de enlace fiable por el que transmitir los paquetes.
Este enlace suele ser generalmente con protocolo LAPB (o LAPD) en las redes de conmutación de paquetes; pero cuando se trata de otro tipo de redes, por ejemplo redes de conmutación de tramas Frame Relay, es preciso sustituir el enlace LAPB por otro tipo de enlace fiable.
Si se elige como capa de enlace el TCP/IP, esto permite la interconexión de terminales que funcionan en X.25 sobre redes Frame Relay, redes locales Ethernet, Token Ring, etc., ya que las secuencias de paquetes se convierten en secuencias de datagramas que van progresando y encaminándose por todas las redes de tipo IP por las que fuera preciso hasta llegar a su destino final, donde son de nuevo recuperados los paquetes X.25.
Esta forma de encapsular X.25 sobre TCP está definida en la pauta de trabajo RFC (Request For Comments) 1613, y el XOT es compatible con ella.

4.1.3. Pila de protocolos TCP/IP

Descripción modelo tcp/ip

El modelo de arquitectura TCP/IP, está básicamente condensado en el modelo DoD, el cual contiene 4 de las 7 capas del modelo OSI.
El objetivo de esta suite de protocolos de red es definir los protocolos y las tecnologías necesarias, que soporten la interconexión de diversos sistemas y conjuntos de hardware, con el objetivo de desarrollar un amplio rango de aplicaciones sobre internet.
Esta es una forma de simplificar los complejos problemas que pueden darse en la interconexión de dispositivos y sistemas, en un reducido número de funciones más pequeñas.

Funciones del modelo tcp/ip

Las funciones del modelo TCP/IP, básicamente consiste en la entrega de paquetes hacia un mismo sistema de computadoras, donde desempaqueta y entrega un proceso individual, que contiene una porción de información.
La confiabilidad en un requisito necesario, para la completa comprensión de los paquetes recibidos en la otra computadora, sirviéndose de un mecanismo de reenvío, en caso de no recibir una notificación de entrega por parte del destinatario.

Tipo

Estas capas son:
–Network Access Layer / or Link
–Internet Layer
–Host to Host Layer / or Transport
–Process / Application Layer
Cada capa, ejecuta una función específica que contribuye al buen funcionamiento de la red.
Los sistemas que participan en los protocolos, no necesitan hacerlo en cada nivel, haciéndolo más fácil trasladar datos de un sitio a otro con un mínimo de esfuerzo.
Por un lado, la capa de aplicación provee de todos los servicios disponibles para los usuarios de internet, por ejemplo navegador web y el correo
electrónico, la capa de interfaz de red, incluye todo el hardware necesario que compone la infraestructura física de internet.
Las dos capas intermedias, la de transporte y la capa de internet, proveen servicios comunes que están disponibles para todas las aplicaciones de internet y opera sobre toda la infraestructura de hardware de internet.

El modelo TCP/IP, reemplazó al protocolo de control de red NCP y fue autorizado oficialmente para transportar datos para conectar algo a la ARPA net (Agencia de proyectos de investigación avanzada). Este modelo TCP/IP, bajo el auspicio del departamento de defensa de EEUU, creó un programa para testear

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

nuevos estándares publicados y hacerlos seguros para pasar ciertos criterios. Esto se hizo para proteger la integridad del modelo TCP/IP.

Las capas del modelo TCP / IP, son las siguientes:

a)La capa de aplicación

Las aplicaciones interactúan con protocolos del nivel transporte para recibir o emitir informaciones. Cada programa de aplicación elige el tipo de servicio de transporte deseado y transmite sus datos al nivel transporte para encaminarlos.

Los servidores DHCP, DNS, Proxy, NAT, SMTP, etc., operan en esta capa del modelo.

b)El nivel Transporte:

El nivel transporte brinda una comunicación de principio a fin entre dos programas de aplicación. Este nivel puede actuar:

·En modo conectado (TCP)

·En modo no conectado (UDP)

A los mensajes generados por la capa aplicación, la capa de transporte los encapsula en mensajes llamados "segmentos".

Para que los paquetes no se pierdan y no se duplique en la Internet, esta capa agrega un encabezado. Además, coloca un identificador para determinar cuál es la aplicación que está generando el mensaje y cuál será la aplicación que deberá recibir el mensaje generado por la computadora de origen.

c)El nivel IP:

El nivel IP encapsula los paquetes recibidos del nivel transporte en unidades llamadas "datagramas IP". Los niveles IP cooperan al encaminamiento de los datagramas según un modo no conectado (gracias a unos algoritmos de encaminamiento).

A los segmentos que envía la capa aplicación, la capa IP le agrega un encabezado para permitir que los datagramas puedan ser encaminados al pasar por varios enrutadores antes de llegar su destino final.

Los campos con los cuales más vamos a trabajar son: "IP de Origen" e "IP de Destino" y son los campos que utilizan los enrutadores para encaminar los datagramas.

d)El nivel enlace de datos:

Esta capa encapsula el datagrama que proviene de la capa de red en un paquete denominado trama".

Esta capa permite que el medio de transmisión físico sea confiable ya que agrega control y detección de errores.

En esta capa operan los Bridges y Switches de capa 2, ya que los mismos utilizan dos campos del encabezado de la trama para conmutar información desde una computadora origen hacia una de destino.

Los campos de la trama que utilizan los Bridges y Switches son la dirección "MAC de Origen" y la dirección "MAC de Destino". Los bridges y switches de capa 2 operan en esta capa del modelo.

e)El nivel Red Física:

Este nivel está en contacto con el material, es decir circuitos, cables, pach panels, conectores JACK, conectores Plug RJ-45, patch cord, etc.

Analogía con el modelo OSI

Capas 5-7: FTP, TELNET, SNMP, SMTP, DHCP, DNS, NAT, Firewalls.

Capa 4: TCP, UDP.

Capa 3: IP, ICMP, ARP, RARP

Capas 1-2: Cualquier Red Física (Ethernet, Token Ring, FDDI)

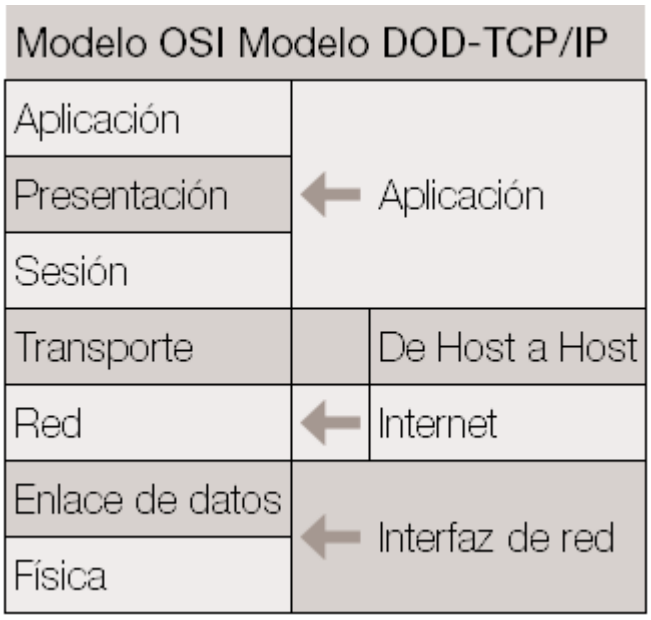
Para terminar este apartado, vamos a reflejar la correspondencia mediante un gráfico, de las capas del modelo de interconexión de sistemas abiertos (OSI) con las capas del modelo de referencia TCP/IP.

TCP/IP se desarrolló en la década de los setenta, por lo que se anticipó a la conclusión del modelo OSI (en los años ochenta).

Esto significa que los distintos protocolos que incluye la pila TCP/IP no se corresponden exactamente con una capa única del modelo de la OSI.

Este modelo divide el movimiento de datos desde un nodo emisor a otro receptor en 4 capas frente a las 7 de la OSI.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.



Capa de aplicación.

Los protocolos de la capa de aplicación proporcionan la interfaz de usuario para los distintos protocolos y aplicaciones que acceden a la red.

Los protocolos de la capa de aplicación en la pila TCP/IP gestionan la transferencia de archivos, la conexión remota con otros nodos, los servicios de correo electrónico y el control de la red. En este nivel residen los protocolos siguientes:

–FTP (File Transfer Protocol o Protocolo de Transferencia de Archivos) es un protocolo que permite transferir archivos entre dos computadoras. FTP es, en realidad una aplicación en si (se pueden descargar clientes FTP desde Internet y utilizarlos para mover archivos entre ambas computadoras) y otro protocolo que soportan otras aplicaciones como navegadores Web.

–TFTP (Trivial File Transfer Protocol o Protocolo Trivial de Transferencia de Ficheros) es en realidad una versión reducida de FTP que permite mover archivos sin ningún tipo de autentificación (es decir sin nombre de usuario ni contraseña).

Además TFTP no es orientado a conexión, por lo que utiliza UDP como protocolo de capa 4.

Se utiliza en el universo de los routers para guardar los archivos de configuración de router o actualizar el IOS (sistema operativo).

–SMTP (Simple Mail Transfer Protocol o Protocolo Simple de Transferencia de Correo) es un protocolo que permite la entrega de mensajes de correo entre dos computadoras distintas.

Este protocolo lo soportan los clientes de correo electrónico y se utiliza para enviar y recibir mensajes de correo electrónico en Internet.

–SNMP (Simple Network Management Protocol o Protocolo Simple de Gestión de Red) es un protocolo que permite recopilar información de la red.

SNMP utiliza agentes (vigilantes de software que supervisan los procesos de red) para recoger datos relativos al rendimiento de la red.

Los datos recogidos pueden después compararse en un servidor en el que se recoge toda la información.

Los paquetes de software como CISCO-WORKS utilizan SNMP para ayudar a los administradores de red a controlar el relativo volumen y riqueza de una red.

–Telnet es un protocolo de emulación de terminal que permite conectar una computadora local con una computadora remota (u otros dispositivos como por ejemplo un router).

La computadora local se convierte en una terminal virtual que tiene acceso a las aplicaciones y demás recursos que incorpora la computadora remota.

Capa de host a host.

Los protocolos de la capa de Host a Host controlan el flujo y la fiabilidad de la conexión cuando los datos se transmiten de una computadora emisora a otra receptora.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Esta capa toma los datos de los protocolos de la capa de aplicación e inicia un proceso de lectura de los mismos para transmitirlos por la red. Esta capa incluye dos protocolos TCP/IP: TCP y UDP.
–TCP (Transfer Control Protocol o Protocolo de Control de Transporte) es un protocolo orientado a la conexión que proporciona un circuito virtual (semejante al que se establece durante una conversación telefónica entre los nodos emisor y receptor) entre las aplicaciones de usuario instaladas en las máquinas emisora y receptora.
–TCP toma los datos de los protocolos de la capa de aplicación y los divide en fragmentos, y después se asegura de que vuelven a ensamblarse correctamente en la computadora receptora. TCP requiere que las computadoras emisora y receptora establezcan una conexión sincronizada que se crea al intercambiar paquetes que incluyen números secuenciales y un bit de control de sincronización.
–UDP (User Datagram Protocol o Protocolo de Datagrama de Usuario) es un protocolo de transporte sin conexión que proporciona una conexión entre los protocolos de la capa de aplicación que no requieren aceptación ni sincronización por parte de TCP.
UDP es como enviar una carta por correo.
El paquete va dirigido al nodo receptor y así es como se le envía. UDP es mucho más pasivo que TCP.
También es más rápido.
Entre los protocolos de la capa de aplicación que utilizan UDP se incluyen TFTP y SNMP.

Capa internet.

La capa Internet (que se corresponde con la capa de red del nivel OSI) se encarga de encaminar los datos a través de rutas lógicas de red y proporciona un sistema de direccionamiento a las capas superiores del modelo conceptual.
Esta capa también define el formato de paquete que debe utilizarse en los datos que se transmiten por la red.
Varios protocolos comprendidos en esta capa proporcionan soporte para el sistema de direccionamiento IP y el formato de paquetes.
Una tarea importante de la capa Internet es la resolución (conversión) de direcciones lógicas (como direcciones IP) en direcciones de hardware MAC de los nodos incluidos en la red.
–IP (Internet Protocol o Protocolo Internet). IP toma los datos de la capa Host a Host y fragmenta la información en paquetes o datagramas.
Después pasa a etiquetar cada paquete con las direcciones IP del
dispositivo emisor y receptor.
IP también se encarga de volver a ensamblar los datagramas en la máquina receptora en segmentos que utilizan protocolos de la capa superior.
IP es un protocolo sin conexión que no se preocupa por el contenido de los datagramas. Su único propósito es dirigir y mover los datagramas hacia su destino.
–ARP (rece Resolution Protocol o Protocolo de Resolución de Direcciones). Cuando IP prepara un datagrama, conoce de antemano la dirección IP de las computadoras emisora y receptora (recibe esta información de los protocolos de la capa superior, como telnet o SMTP).
Pero cuando el paquete llega a la LAN destino necesita conocer las direcciones MAC de hardware para la computadora receptora ya que tiene que suministrar esta información al protocolo de la capa de acceso a la red que se utiliza en la red.
ARP proporciona un mecanismo para resolver las direcciones IP en direcciones de hardware.
Para ello, ARP envía difusiones con la dirección IP de la computadora receptora y pide a esta computadora que responda con su dirección de hardware.
–ICMP (Internet Control Message Protocol o Protocolo Internet de Control de Mensajes).
Este protocolo es un protocolo de suministro y gestión de servicios de mensajería que utilizan los routers para enviar mensajes a las computadoras host que están enviando datos que deben encaminarse.
Los routers pueden informar a las host emisoras de cuándo no puede alcanzarse un determinado destino o de cuando la memoria intermedia del router está saturada de datos.
ICMP se utiliza básicamente como protocolo de soporte para el direccionamiento IP, lo mismo que ARP.
Ping o traceroute utilizan ICMP por poner un ejemplo.

Capa de acceso de red.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

La capa de acceso de red está formada por los protocolos que toman los datagramas de la capa Internet y los devuelven dentro de un tipo específico de trama que pasa a ubicarse en el entorno físico de la red en forma de secuencia de bits.
A este nivel se incluyen arquitecturas como Ethernet, Token Ring y FDI.

4.1.3.1 Introducción

Modelo TCP / IP
Es un modelo de interconexión lógico de redes fijas y define un conjunto de protocolos que rigen las comunicaciones en esas redes.
Este modelo opera a nivel operacional, sobre la red de internet.
Introducción.
TCP/IP (Protocolo de Control de Transferencia / Protocolo de Internet) es una suite de protocolos estándar de la industria diseñados para permitir la comunicación en redes WAN.
La agencia de Búsqueda de Proyectos Avanzados para el Departamento de Defensa de los Estados Unidos (DARPA) creó, a finales de los 70, un método de comunicación fiable y basada en el intercambio de paquetes de datos. Podríamos decir que de este experimento nació lo que hoy conocemos como TCP/IP.
Fechas importantes.
–1970. Los Host que integraban ARPANET (Red Militar de Estados Unidos) empiezan a utilizar el protocolo NCT (Network Transfer Protocol).
–1972: Aparece TELNET, contemplada en la RFC 318.
–1973: La RFC 454 introduce FTP.
–1974: Se especifica en detalle el Protocolo de Control de Transferencia (TCP).
–1981: Se pública el estándar IP en la RFC 791.
–1982: ARPA y la DCA establecen IP y TCP como una suite llamada TCP/IP.
–1983: ARPANET cambia NCT por TCP/IP.
–1984: Se introduce DNS.
Generalidades de tcp/ip.
–Es un protocolo de comunicaciones estándar con capacidades de enrutamiento.
–Tecnología para conectar distintos sistemas, permitiendo así la posibilidad de comunicación con redes UNIX o incluso LINUX.
–Es un método garantizado de acceso a Internet (funciona con este protocolo).
Es una robusta y escalable plataforma cruzada cliente / servidor. TCP/IP ofrece la interfaz Windows Sockets, lo que permite a los desarrolladores escribir aplicaciones basadas en Sockets.
El modelo TCP / IP, establece:
a)Programas de aplicaciones.
b)Protocolos de transporte.
c)Protocolos de enrutamiento de los datos

4.1.3.2. Modelo OSI

Modelo de referencia para la interconexión de sistemas abiertos (osi)
El modelo OSI, fue descompuesto en 7 capas, las cuales pasamos a describir a continuación:
a)Capa de aplicación: Gestiona los servicios a los usuarios
·Los protocolos pueden ser:
›Relativos a la gestión de aplicaciones o del propio sistema del usuario, como por ejemplo en navegador de internet, software de monitorización de sistemas o procesos, etc.
›Específicos de la aplicación del usuario, como por ejemplo, DHCP, DNS, NAT, FTP, Email, web, etc.
·Los protocolos de esta capa, deben de ser capaces de identificar y adaptar la información proveniente de las distintas aplicaciones de los usuarios, para
interactuar de forma eficaz con la terminal virtual de red. Su aplicación real, está en la transferencia de archivos, consultas de emails, navegación por internet, etc.
·Los procesadores de texto, así como cualquier otra aplicación de la suite de office, además de software que no requiera de conectividad de red, no forma parte de la capa de aplicación.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

b)Capa de presentación: Una de sus funciones más significativas, es facilitar el trabajo de la capa de aplicación, cuyos servicios son codificar y proporcionar un formato válido a los datos dados por la capa de aplicación, junto con la comprensión y si procede la encriptación de los datos.
Uno de los ejemplos más claros para esta capa, es la representación ASCII y enteros complemento a uno y a dos.
De todo esto, se deduce la finalidad de la capa de presentación, que no es otra que la de compatibilizar las diferentes representaciones que pueden darse, para adaptarla a un código estándar comprensible y legible usado dentro de cada computadora.
c)Capa de sesión: En esta capa, se establece la relación de comunicación entre las aplicaciones, donde las cuales se sincronizan, llevando a cabo la comunicación mediante alguna de los métodos disponibles, como son full dúplex o semidúplex.
Por otro lado, también gestiona la operación entre las aplicaciones y los incidentes que se puedan ocasionar en el proceso comunicativo, estableciendo el orden en los turnos de comunicación de las aplicaciones.
Dicha capa, también controla los flujos de datos en las sesiones establecidas, con el debido control de flujo.
d)Capa de transporte: Su función, es ofrecer servicios conexión de circuitos virtuales entre dispositivos, asegurando un servicio punto a punto.
Su actuación se resume en la aceptación de los datos provenientes de las capas superiores, y que lleguen en perfecto estado al otro extremo, dividiéndolos en trozos más pequeños, si fuera necesario.
La capa de transporte debe de estar lo suficientemente aislada, para que los cambios tecnológicos de las capas superiores, no afecten a la capa de transporte.
Esta capa, puede crear múltiples circuitos virtuales si fuera necesario, multiplexando varias conexiones de transporte en la misma conexión física de la red, en caso de que el tráfico sea muy alto.
A tal fin, posee un mecanismo de control de flujo, para regular el tráfico de información, de modo que no sature la conexión entre nodos, con independencia, de cuál de ellos envíe con mayor rapidez.
e)Capa de red: Ofrece los medios de comunicación de un sistema a otro extremo, ocupándose del enrutamiento necesario, para lograr alcanzar el destino deseado, ocupándose de las direcciones lógicas IP, junto con las subredes, tan necesarias para determinar el sistema remoto.
En las redes complejas, puede verse comprometido el envío de paquetes de cierto tamaño, formando cuellos de botella, los cuales deben de ser controlados por esta capa, o bien cuando atraviesan varias subredes, cuyas direcciones sean diferentes de la enviada, o que alguna que otra subred, deseche los paquetes, debido a su tamaño excesivo.
f)Capa de enlace de datos: Es la capa encargada de transformar la información de las capas superiores, en una línea libre de errores indetectables en la capa de red.
Esto se consigue, dividiendo dichos datos en tramas, de forma secuencial y ordenada, además de gestionar adecuadamente los acuses de recibo que emite el dispositivo receptor.
De los límites de estas tramas también se encarga esta capa, la cual fija una serie de patrones de inicio y fin de trama, para que puedan ser reconocidos por el dispositivo receptor, a fin de determinar el inicio y fin de cada trama, para luego pasar a la recomposición del stream de datos.
También se ocupa de la retransmisión de las tramas, además de las dañadas, perdidas y duplicadas, cuya gestión recae en la capa de enlace de datos.
·Capa física: Se encarga de la transmisión de los bits al medio físico
El modelo de la ISO para la interconexión de sistemas abiertos se convirtió en un estándar internacional en la primavera de 1983. Este modelo se basa en una estructura de siete capas.
Su objetivo principal es la interconexión de sistemas abiertos, esto es, comunicación entre sistemas distintos o de diferentes fabricantes.
La ISO (recedentel Standards Organization) es una organización no gubernamental que se encarga a nivel mundial de la coordinación y aprobación de estándares; en ISO están representadas las organizaciones de estandarización nacionales de los principales países, algunas de las cuales son: ANSI de Estados Unidos, BSI de Gran Bretaña, DIN de Alemania, JISC de Japón, AENOR de España, etc.
·Los fundamentos en los que se basaron para la utilización de siete capas fueron:
›Las capas son entidades abstractas, creándose una capa donde se necesita un estado diferente de abstracción.
›Cada una de las capas realizará una función perfectamente definida.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

›La función que realizará cada una de las capas se seleccionará para definir protocolos normalizados.
›Los límites entre capas deberán fijarse teniendo en cuenta que el flujo de información entre dichas capas sea el mínimo posible.
›El número de capas será lo suficientemente grande para que funciones muy diferentes no tengan que situarse en la misma capa y será lo más pequeño posible para que en conjunto no sea inmanejable.
›Los objetivos que se consiguen con este modelo son:
›La estandarización de la comunicación entre sistemas, (sistemas abiertos).
›Suprimir los posibles problemas técnicos para comunicar distintos sistemas que pueden ser de diferentes fabricantes.
›No tener que describir las operaciones internas que realiza cada uno de los sistemas de los distintos fabricantes.
›Conseguir unos puntos de interconexión bien definidos para el intercambio de información.
›Ser suficientemente flexible para asegurar que los elementos, hardware o software, puedan mejorarse o actualizarse sin introducir cambios totales, evitando en la medida de lo posible que afecten los cambios tecnológicos y los servicios que puedan solicitar los usuarios.

Características del modelo.

El patrón para la Interconexión de Sistemas Abiertos se basa en un modelo de protocolos estratificados, cada nivel se desarrolla sobre el anterior, proporcionando un conjunto de servicios al nivel inmediatamente superior, por lo que el nivel más alto dispondrá de los servicios que ofrecen todos los niveles inferiores.
La comunicación entre niveles equivalentes de distintos sistemas es una comunicación lógica horizontal.
Existen cuatro acciones, denominadas primitivas que son un conjunto de operaciones que sirven para ofrecer los servicios entre niveles, a estas primitivas acceden los niveles por medio de los Puntos de Acceso al Servicio o SAP (Service Access Points).
Este es un método que se utiliza para que los niveles se comuniquen entre sí.
El intercambio de información entre capas se lleva a cabo por medio de un interfaz existente entre las mismas, este interfaz puede estar compuesto por elementos lógicos y/o físicos.
Los protocolos de cada uno de los niveles pueden ser diferentes e independientes entre sí, lo único que necesitan es conocer los servicios que presta el interfaz con la capa inferior.
El modelo OSI no especifica de forma exacta los protocolos y servicios que se utilizarán en cada nivel, únicamente indica las funciones que debe realizar cada capa, por lo que este modelo no se puede considerar como una arquitectura de red.

Transmisión de datos.

Existen siete niveles o capas en el modelo OSI. El objetivo de cada una de las capas es comunicarse con su capa equivalente de otro sistema o de un nodo de la red.
Para que la comunicación sea posible cada sistema deberá tener los mismos protocolos en cada uno de los niveles.
Suponiendo que el emisor tiene datos de usuario para transmitir, éste se los entrega a la capa de aplicación.
Esta capa añadirá una cabecera “A” y entregará los datos a la capa de presentación.
La capa de presentación a su vez añadirá la cabecera de presentación “P” y el resultado se lo enviará a la capa de sesión, repitiéndose este proceso hasta llegar a la capa física.
En este nivel es donde realmente se envían los datos al otro sistema por medio de los circuitos, equipos e interfaces existentes entre los mismos.
Cuando la información llega de una capa a la capa inmediata inferior, ésta no puede diferenciar que datos son de información real y cuales son de la cabecera de la capa superior.
Cuando la información llega al sistema receptor se realiza el proceso inverso, suprimiendo cada capa la cabecera correspondiente y entregando los datos a la capa superior hasta llegar a la capa de aplicación, que será la que entregue los datos al usuario receptor.
Como se puede observar, la transmisión efectiva de datos es vertical, por lo que no existe una comunicación directa entre los niveles de los dos sistemas excepto en el caso del nivel físico.
Lo que se establece es una comunicación lógica entre niveles pares o iguales utilizando para ello el protocolo de cada nivel, que utiliza las cabeceras que se añadieron en el emisor para llamar a funciones en el receptor.
Los niveles se pueden clasificar en tres grupos o niveles globales.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Los niveles de control de usuario relacionados con las necesidades de comunicación de los usuarios, formados por los niveles de Aplicación, Presentación y Sesión.
El nivel de transporte, formado por la capa de Transporte y los niveles de transmisión encargados de transmitir los mensajes a través de la red, formados por las capas de Red, Enlace y Física.

Descripción y funciones de los niveles.

La jerarquía OSI está formada por niveles o capas que tienen asignada una serie de funciones básicas que se describen a continuación.

1)Nivel físico.

Este es el nivel más bajo del modelo; en este nivel se definen las características mecánicas, eléctricas y funcionales o de procedimiento de interfaz para un medio de transmisión específico.
Este nivel debe asegurar el envío correcto de los bits, que cuando se transmita un bit con un determinado valor en el otro extremo se reciba con el mismo valor.
Este nivel por tanto es el responsable de activar, mantener y desactivar los circuitos entre el ETD y el ETCD.

2)Nivel de enlace de datos.

Esta capa es la responsable de la integridad en la transferencia de datos por medio de transmisión, esto quiere decir que a partir de un medio de transmisión como puede ser una línea telefónica, tiene que hacer los ajustes o correcciones necesarias para que la capa 3 pueda transmitir sin fallos.
Una de las funciones más importantes de este nivel es la detección de errores en la transmisión; esta capa proporciona mecanismos para la recuperación de datos perdidos, duplicados o erróneos.
También, para que el receptor no se sature tendrá que proporcionar funciones de control del flujo de datos.
Sobre este nivel recae la creación y el reconocimiento de los límites de la trama. Esta capa ofrece diferentes clases de servicios a la capa de red.
Los protocolos del nivel de enlace de datos definen el establecimiento y la liberación del enlace, controlando el correcto envío de datos y haciendo funciones de gestión del propio nivel.
Algunos de estos protocolos son el BSC (Binary Synchronous Communications), HDLC, LAP-B (X.25 nivel 2), etc.

3)Nivel de red.

La comunicación entre dos sistemas normalmente se realiza por medio de una red, este nivel especifica el interfaz entre ETD's mediante redes de paquetes, teniendo la responsabilidad de transmitir los datos correctos a través de la red.
Por tanto esta capa tiene la responsabilidad de seleccionar la ruta que tomarán los datos o encaminamiento (función de conmutación), que está muy relacionado con el diseño de la red.
Otra función de este nivel es que cuando existe mucha información a transmitir dentro de la red y ésta se satura, realiza el control de la congestión o controla el flujo de paquetes para prevenir el bloqueo de la red.
También tiene como misión la conexión y desconexión de las redes, resolver los problemas de interconexión con otras redes (encaminamiento entre redes), e incluso la función de contabilizar la información transmitida para la facturación.
Ejemplos de protocolos de nivel de red son el IP (Internet Protocol), X.25 (nivel 3), IPX y AppleTalk.

4)Nivel de transporte.

Esta capa aísla a los niveles superiores de los elementos de comunicación que constituyen la red, independizándolos por tanto de la tecnología utilizada en la red.
Su función principal consiste en tomar los datos del nivel de sesión, dividirlos en trozos más pequeños si fuera necesario y pasarlos a la capa de red, asegurándose de que llegan correctamente a la misma capa del otro sistema, proporcionando así un mecanismo fiable para el intercambio de datos entre sistemas distintos.
Esta capa fragmenta la información en unidades más pequeñas, empleando funciones de multiplexación, direccionamiento, establecimiento y liberación de conexiones a través de la red y transferencia y control de flujo de la información.
La capa de transporte es una capa del tipo origen –destino, o extremo a extremo, la capa origen se comunica con la de destino utilizando para ello los protocolos de esta capa, que se establecen extremo a extremo.
En las capas inferiores se comunican entre cada sistema (ETD) y su conexión más próxima (la Red).

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

La capa de transporte puede ofrecer servicios de detección y corrección de errores y distintos niveles de calidad de servicio, normalmente relacionados con los costes.
El tipo de servicio se determina cuando se establece la conexión.
La complejidad de los protocolos utilizados en la capa de transporte dependerá de lo complejos que sean los que se utilicen en el nivel de red o de los servicios que ofrezcan.
Algunos protocolos utilizados en este nivel son el TCP (recedente Control Protocol) y UDP.
5)Nivel de sesión.
Proporciona los medios necesarios para controlar el diálogo entre entidades de presentación, permite que usuarios de diferentes sistemas puedan establecer sesiones entre ellos, por ejemplo para transferir archivos.
6)Nivel de presentación
Esta capa se ocupa de la sintaxis o formato de los datos de aplicación que se intercambia durante las sesiones; esta función es completamente diferente de la de las capas inferiores, cuyo trabajo principal consiste en el intercambio fiable de bits entre dos sistemas.
7)Nivel de aplicación
Es el nivel superior del modelo de ISO, sirviendo por tanto al usuario final, que es el entorno o proceso de aplicación. Controla y coordina las funciones que realizan los programas de los usuarios.
Un proceso de aplicación es un elemento dentro de un sistema abierto, que se ocupa del procesamiento de información requerido para una aplicación en particular.
Cuando dos procesos de aplicación intercambian información usan
protocolos de aplicación que utilizan servicios del nivel de presentación.
Ejemplos de protocolos de este nivel son el FTP (transferencia de ficheros), X.400 (correo electrónico), X.500 (directorio), http, DNS, SMTP, etc.
En algunos sistemas las capas pueden estar a su vez divididas en subcapas, o por el contrario no tener ninguna función, en cuyo caso no existiría dicho nivel.

Ejemplo de comunicación.

Para aclarar las funciones que realiza cada una de las capas se puede hacer de manera sencilla con un ejemplo de una llamada telefónica:
1)Una línea telefónica enlaza dos equipos de telecomunicaciones (teléfonos), la capa 1 (física) asegura que las señales de voz sean transformadas en señales eléctricas aptas para ser transmitidas al otro extremo de la línea y las señales que se reciben se conviertan en señales audibles.
Esta capa define el tipo de conector que deben tener los aparatos telefónicos (RJ-11) y los niveles de la señal en el interfaz del teléfono con la red.
2)La capa 2 (enlace) asegura que siempre que se produzcan errores y una palabra no sea correctamente recibida, se indicará al emisor para que la retransmita.
Además si el sistema permite conversaciones simultáneas de más de dos usuarios esta capa controlará quién habla.
3)La capa 3 (red) establece la llamada mediante la marcación del número distante, proporcionando un mecanismo de encaminamiento para conectar con el número de la persona con la que se desea hablar.
En el extremo distante, cuando suena el timbre, la persona descuelga el teléfono y comienza la comunicación.
4)Cuando la llamada se ha establecido, la capa 4 (transporte) se emplea para asegurar que los mensajes solicitados se envían sin pérdidas.
Si la calidad se degrada hasta el punto de que no se comprenden los mensajes, pueden acordar interrumpir la comunicación.
5)En la capa 5 (sesión), se proporcionan mecanismos que permiten al que llama establecer una conversación (sesión) con otra persona del mismo lugar al que se llama identificándose y preguntando por esa persona, también puede ser que durante un tiempo conversen dos personas y en otro momento otras distintas.
6)En la capa 6 (presentación) se resuelven los problemas del lenguaje. En el caso de que ambas partes no hablen el mismo idioma se realizaría la función de traducción, solicitando un traductor.
También si el asunto es confidencial, se puede acordar el empleo de un vocabulario especial que ambos entiendan.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

7)La capa 7 (aplicación) depende de la forma en la que las dos personas que se comunican quieran intercambiarse el mensaje, del modo de hablar o del sentido de las palabras.

Comunicación entre niveles (servicios).

Como hemos visto, las capas se comunican con sus iguales (capas gemelas de otro sistema) de manera lógica mediante protocolos de capa.

Sin embargo, la comunicación real se establece entre los distintos niveles hasta llegar al nivel físico; cada nivel proporciona una serie de servicios al nivel superior mediante un conjunto de funciones o primitivas.

La mayoría de estas primitivas pueden contener parámetros con los que pueden especificar el tipo de servicio que se desea, el tamaño del mensaje, la identidad del que llama, etc.

Las capas a su vez pueden ofrecer dos tipos de servicios: orientados a conexión y sin conexión.

Un servicio orientado a conexión es aquel que establece un camino o conexión antes del envío de información, liberando después dicha conexión.

Es como si la información fuera un líquido que fluyera por un tubo que se establece entre el origen y el destino.

En un servicio sin conexión cada mensaje se encamina de manera independiente a través de la red; en este caso cada mensaje lleva la dirección completa del destino en su propia cabecera.

Se puede hacer una analogía entre el servicio orientado a la conexión y el sistema telefónico, en el que cada vez que queremos comunicarnos se establece un circuito con el distante.

El servicio no orientado a conexión sería similar al servicio de correos en el que cada carta lleva su dirección completa del destino.

–Unidades de datos:

·Segmento: en TCP/IP se denomina segmento a la PDU del nivel de transporte.

·Paquete: unidad de datos de nivel de red (3). Normalmente se habla de paquetes de datos en redes IP. También denominado datagrama.

·Trama: unidad de datos del nivel de enlace (2). En el nivel del enlace de datos lo que tenemos son tramas (paquete con la cabecera y cola de datos añadida). Por un enlace físico lo que se transmite son tramas.

4.1.3.3 Niveles. Descripción de cada uno

Descripción del nivel físico

El nivel físico consiste en la infraestructura subyacente de la red, donde se proporciona los medios mecánicos, eléctricos y funcionales, que sirven para activar, mantener y desactivar cualquier conexión física en los procesos de transmisión de información a través de la capa de acceso a la red.

Funciones del nivel físico

Las funciones del nivel físico, están las sucesivas transformaciones que deben de sufrir una secuencia de bits, para ser transportados por el medio físico en señales eléctricas, con los debidos procedimientos incluidos, para una vez llegada la información al punto extremo o deseado, pueda volver a codificarse como una cadena de bits legibles para el otro dispositivo.

–Elementos de la capa física

·Medios y conectores

·Representación de los bits

·Codificación de los datos y la información de control

·Sensores en el transmisor y receptor

Funcionamiento de la capa física:

Referente al cableado de cobre, las señales transmitidas, son patrones de impulsos eléctricos.

Referente a la fibra óptica, las señales transmitidas, son patrones de luz.

Referente a los medios inalámbricos, las señales transmitidas con patrones de ondas de radio.

Sabías que

Las diferentes tecnologías de la capa física se definen por una serie de organizaciones, especializadas en ingeniería eléctrica y en comunicaciones, definen los diferentes estándares de la capa física. Por ejemplo El grupo de trabajo de ingeniería de internet (ETF) que define los servicios y protocolos del modelo TCP/IP en RFC.

Además de otras organizaciones encargadas del desarrollo de estándares, como puede ser:

–La organización internacional para la estandarización (ISO).

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

–El instituto de ingeniero s eléctricos y electrónicos (IEEE).
–El instituto nacional estadounidense de estándares (ANSI).
–La unión internacional de telecomunicaciones (ITU).
–La asociación de industrias electrónicas / Asociación de la industria de las telecomunicaciones (EIA/TIA).
–La comisión federal de telecomunicaciones de EEUU (FCC).

Descripción del nivel de acceso a la red.

El nivel de acceso a la red, comprende el hardware que soporta todas las interconexiones físicas de todos los dispositivos de red.

Las tecnologías de esta capa, son diseñadas en múltiples capas, donde el atributo común de todas estas tecnologías, es que son capaces de reenviar adelante, datagramas IP o paquetes de datos.

Existen muchas tecnologías que operan en esta capa, de las cuales algunas resultan ser muy complejas.

Los protocolos más usados en este nivel son Asynchronous Transfer mode (ATM), Frame Relay, point to point protocol (PPP) y ethernet. También los hay propietarios y algunos a través de estándares abiertos.

Funciones del nivel de acceso a la red.

Realiza el intercambio de datos entre un host y la red.

Supervisa el direccionamiento de hardware, y se encarga de controlar y supervisar el envío y recepción de datos al medio físico.

Las funciones clave de este nivel de acceso a la red, son la asignación de direcciones IP a las direcciones MAC (físicas), además del encapsulamiento de los paquetes IP en tramas, para su posterior puesta en el medio físico.

Proporcionan el formato necesario a los datos, para ello otra de sus funciones estrella es el conocimiento de los detalles de la red, con el objetivo de atribuir el formato adecuado a los datos para su puesta a los medios.

Subcapas del nivel de acceso a la red.

El nivel de acceso a la red, posee 2 subcapas del IEEE son:

a)Media Access Control (MAC). Se encarga de definir el procedimiento de como los paquetes son colocados en el medio. Sirve los datos conforme llegan, son enviados.

El ancho de banda es compartido. También puede ser usado en esta subcapa, un reconocimiento de entrega de frames, al igual que es posible usar control de flujo.

b)Logical Link Control (LLC). Es responsable de la identificación de los protocolos de la cada de red, al igual que su encapsulamiento.

Controla la cabecera LLC de cada frames, para buscar donde es destinado el paquete. LLC proporciona igualmente control de flujo y secuenciamiento de control de bits.

Los switches y los puentes trabajan en esta capa de nivel de acceso a la red, donde filtran la red usando las direcciones de hardware, es decir las MAC, y la latencia es un fenómeno muy crítico para estos dispositivos donde su principal función consiste en conmutar o redirigir tramas mediante una aplicación llamada ASIC.

ASIC, es un circuito integrado específico de aplicación, por el cual es usado como hardware especializado para la conmutación de capa 2 en los switches.

Descripción del nivel de internet.

El nivel de internet, es la capa responsable de transportar tráfico entre dispositivos de red, que no están localmente unidos.

Esta capa provee los servicios de enrutamiento dentro de una internetwork, con el objetivo de administrar el direccionamiento de los dispositivos, trazar la localización de los dispositivos en la internetwork y determinar la mejor manera de enrutar los datos.

Los protocolos usados para soportar el tráfico de datos son llamados protocolos enrutados, de los cuales, IP v4 e IP v6 son ejemplos claves de estos.

Funciones del nivel de internet.

El nivel de internet provee un plan de direccionamiento común a todos los hosts en internet, proporcionando un servicio no confiable de transferencias de datagramas entre esos hosts. IP es el protocolo estrella de internet, donde todo es conectado mediante él, además de definir la manera en que los paquetes son enrutados hacia su destino.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Los equipos que manejan estas funciones del nivel de internet son los routers, encargados de examinar la dirección destino y determinar cuál será el siguiente router, hasta que el paquete llegue a su destino.
Las funciones relevantes del nivel de internet son:
–Definir el datagrama.
–Definir el esquema de direccionamiento.
–Intercambiar los datos entre la capa de acceso de red y la capa de transporte.
–Enrutar los datos hacia los sistemas remotos.
–Realizar la fragmentación y el re-ensamblaje de los datos.
Los protocolos TCP/IP, fueron diseñados para el intercambio de datos en ARPANET, donde esta red era una de intercambio de paquetes. Este sistema podríamos compararlo, con el sistema de correos, donde no solo escribimos el contenido en la carta, sino que también añadimos los datos necesarios para que llegue a la persona destinataria de la carta.
El protocolo IP, es un protocolo no orientado a la conexión, por lo que no intercambia información de control para establecer una conexión, antes de empezar a transmitir los datos. Si fuese necesario, tal control de información, el protocolo IP delegará dichas funciones a otros protocolos de capas superiores, que si están orientados a conexión, como por ejemplo TCP.

Descripción del nivel de transporte.

Es la capa encargada de reemsamblar los datos en un único stream de datos, cuyos servicios localizados en la misma, son los encargados de recibir los diferentes datos de las capas más altas, y entonces combinarlo en un único stream de datos.
La capa de transporte es la responsable de proveer mecanismos para la multiplexación de las aplicaciones de la capa de aplicación, estableciendo sesiones y de destruir los circuitos virtuales creados para tal propósito.
Además de lo anteriormente dicho, es capaz también de ocultar información de detalles que depende de la red, así como proveer una transferencia de datos transparente.

Funciones del nivel de transporte.

Los protocolos de del nivel de transporte proveen servicios de datos end to end y establecen conexiones lógicas entre el host de envío y el host remoto en la internetwork.
La capa de transporte, puede funcionar en modo sin conexión u orientado a conexión.
En las comunicaciones orientadas a conexión, se establece en primer lugar una sesión de comunicación orientada a la conexión entre los 2 host y posteriormente comienzan a sincronizarse para prepararse la transferencia de datos entre los mismos.
Entre otras funciones del nivel de transporte, lo encontramos en el control de flujo, el cual asegura la integridad de los datos, permitiendo a las aplicaciones ofrecer peticiones de confiabilidad de transporte de datos entre sistemas.
Los propósitos del control de flujo, es la de proveer una manera al dispositivo que está recibiendo, de controlar la cantidad de datos enviados por el dispositivo que envía.
De esta forma, se asegura una buena comprensión de los mensajes, eliminando así, las posibles congestiones en la red que se pueden dar en un momento determinado, además de reducir los procesos de reenvío por la llegada incompleta del stream de datos o bien por errores producidos debidos a la congestión de la red.
Los protocolos que funcionan en esta capa de red son UDP y TCP, para proporcionar los servicios anteriormente mencionados, sobre la orientación a conexión o sin orientación a conexión, entre otros beneficios proporcionados por ambos, según las circunstancias requeridas.
El término confiabilidad en la red, puede ser usado en la capa de transporte. Dicho término, requiere para la prestación de los beneficios de la confiabilidad, reconocimiento, secuenciación y flujo de control. Todos deben de ser usado como un todo.
Los tipos de control de flujo en el nivel de transporte son, el windowing, buffering y la limitación de congestión. Bien pues con el windowing, se puede mejorar la sesión de comunicación, decrementando el valor de esta ventana, en caso de que un host falle en la recepción de todos sus bytes.

Descripción del nivel de aplicación.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

En este nivel, se trabaja como una interface entre los programas de aplicación y las capas más abajo, para proveer información pertinente a través del stack de protocolos establecidos.
Las diferentes aplicaciones interactúan con los protocolos relevantes para obtener información sobre el acceso a recursos remotos.
Esto es necesario, para identificar el tipo de comunicación que toma lugar en el nivel de aplicación, mediante la identificación y confirmación, además de la disponibilidad y verificación de los recursos requeridos a través de los diferentes protocolos.
Por otro lado, en este nivel de aplicación, se encarga de presentar los datos, y del formateo del código y la traducción de los datos.
Para que estas descripciones del nivel de aplicación tengan lugar, se establece otra responsabilidad de la capa la cual, configura, administra y desmonta las diferentes sesiones establecidas y mantiene los datos del usuario separados, el cual se consigue mediante un control de diálogo entre los dispositivos intervinientes.
Esta comunicación que se lleva a cabo, se establece mediante diferentes modos en un entorno cliente-servidor, donde su control y configuración, también se establecen en esta capa.

Funciones del nivel de aplicación

Una de las funciones más importantes del nivel de aplicación, es la identificación, verificación y disponibilidad de los protocolos de comunicación para proveer un tipo de comunicación en especial.
Esto se hace necesario en las funciones del nivel de aplicación, porque a veces las aplicaciones de las computadoras necesitan más recursos de
escritorio.
Básicamente trabaja como una especia de interfaz, entre el stack de protocolos de las capas inferiores, y los programas de las diferentes aplicaciones.
Otra de las funciones en combinación con el resto, es la encargada de la presentación de los datos, además de su traducción y formateo de codificación.
Como ejemplo de tipo de servicio de traducción, lo encontramos en el paso del obsoleto Extended Binary Coded Decimal Interchange Code (EBCDIC) al American Standard Code for Information Interchange (ASCII).
Por último, cabe mencionar el control del establecimiento y mantenimiento de las diferentes sesiones que se crean para interactuar entre los diferentes procesos, para posteriormente, ser coordinados y organizados en varios modos diferentes de establecimiento de las comunicaciones.

Clases de eventos:

–Transferencias de archivos
–Localización de la información
–Procesos cliente servidor
–Procesos de administración de red
–Activación del acceso remoto
–Correo electrónico

Los programas de usuario tales como Microsoft Word, Microsoft internet explorer, Firefox, etc., no residen en esta capa, solamente interfieren con los protocolos de la capa de aplicación. Los programas que realmente residen son Telnet, FTP y TFTP.

4.2. Cifrado. Redes privadas virtuales

Vulnerabilidades de acceso remoto.

Desde el mismo momento que el tráfico de la red, sale de nuestra red local, se vuelve mucho más vulnerable para los cracker, ya que esta, se vuelve mucho más vulnerable propiciando una mayor probabilidad de que el tráfico que se genera sea interceptado.
Esta presencia de accesos remotos a las redes, proporcionan a los crackers puntos de accesos adicionales que pueden ser usados para sus fines.
Los usuarios pueden realizar el conexionado de acceso remoto, de dos formas diferentes en relación al ámbito físico:
1.A través de una conexión telefónica.
2.Mediante internet.
Una vez que el usuario, se ha conectado mediante la red privada virtual, puede acceder a los recursos de la red, usando software de control remoto, una interfaz web o mediantes comandos de control remoto.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Descripción funcional.

La facilidad de cifrado para el servicio VPN IP responde a la necesidad de los clientes de complementar el servicio VPN IP con tecnologías que cubran aspectos del intercambio de datos tales como Confidencialidad, Integridad y Autenticidad.
El Servicio VPN IP por si solo tiene un nivel de seguridad similar a una Red de transporte de Nivel 2, lo que en ocasiones puede no ser suficiente para determinado tipo de clientes que obligados por Ley a cifrar sus datos (Por ejemplo el sector seguros) o que demandan mayor seguridad, nos han requerido directa o indirectamente la inclusión de estas soluciones en el Servicio.
Las técnicas de securización, y de servicio VPN IP tiene una serie de características propias que han hecho necesaria una selección y adaptación de las opciones posibles de Cifrado y el empleo de nuevas soluciones que respondan a necesidades específicas de este servicio.

Caracterización del cifrado.

La facilidad de cifrado del servicio VPN IP permite el cifrado mediante IPSec en modo túnel con secreto compartido y 3DES, del tráfico IP de cliente entre routers.
En el modo túnel, el paquete de datos que desde la LAN llega al router, es cifrado en su totalidad, incluida la cabecera original y se le añade una nueva cabecera IP con origen y destino los peers del túnel IPSEC.
El tamaño de cada paquete original aumenta en 20 bytes por la nueva cabecera IP y al menos en 8 bytes más si se emplea ESP o 24 si se emplea AH.
Los routers contemplados son Teldat y Cisco con o sin tarjeta cifradora.
El cifrado por lo tanto será SW o HW dependiendo de la existencia o no de tarjeta de cifrado específica en el router.
El tráfico de Gestión del equipo no se cifrará.
En todo caso, el cliente ha de caracterizar el tráfico que quiere que se cifre, ejemplos de caracterización son:
–Todo el tráfico entre todas las sucursales (En su caso menos el destinado a Internet)
–Todo el tráfico entre todas las sucursales que tenga ciertas características (Pto TCP/UDP origen/destino)
–El tráfico de todas las sucursales contra una sola o contra un determinado servidor (Topología en estrella)
–Designación por parejas de oficinas del tráfico a cifrar.
–Etc.
La solución de cifrado adoptada es compatible con la topología totalmente mallada natural del servicio VPN IP, es por tanto una solución que permite un mallado completo de túneles IP Sec.
La facilidad de cifrado es compatible con todos los accesos definidos en el servicio tanto dedicados como conmutados: ATM, FR, ADSL, IP Nativo, RDSI.
La facilidad de cifrado es compatible con las facilidades definidas en el servicio como son:
–CoS
–Topologías de acceso complejas (Backup y Balanceo) menos en un caso descrito a continuación.
–Acceso a Internet Integrado en Red
–Acceso a Internet por domicilio de Cliente
–Backup Integrado en Red.
Pero no es compatible con la siguiente facilidad:
–Topología en modo balanceo con un solo router. No es posible compatibilizar el balanceo en bajada hacia el router con la convergencia del routing de la Red hacia el Loopback origen del tráfico cifrado.
Hay que tener en cuenta que los routers tendrán menores prestaciones que las normalmente aceptadas para soportar IPSec puesto que a la vez ha de asumir las tareas de clasificación, marcado y encolado necesario para la implementación de las clases de servicio.

4.2.1 Descripción

Una Red Privada Virtual (VPN) es una red virtual creada dentro de otra red, generalmente Internet, por lo que los requerimientos de seguridad son de alto nivel e importancia. El intercambio efectivo de paquetes y la QoS son servicios de alta importancia en el manejo de redes virtuales privadas.
El protocolo de conmutación de etiquetas (MPLS) integra el ancho de banda, la latencia y la utilización de Capa 2 enla Capa3 para mejorar y simplificar el intercambio de paquetes.
Es decir, es una técnica que utiliza la inteligencia del ruteo y el desempeño de los conmutadores para disminuir el tráfico de rutas, la congestión, las fallas de conexión y los cuellos de botella.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

MPLS proviene de tecnologías ya existentes, como son “Tag Switching” de CISCO y ARIS ” de IBM.
En 1997 fue creado el primer grupo de trabajo de MPLS por el Grupo de Trabajo en Ingeniería de Internet (IETF).
Hoy en día lo estándares de MPLS están en fase de borrador, algunos más profundizados que otros, sin embargo es un tema de actualidad que en un futuro será un estándar de calidad y desempeño completo que permitirá formar sistemas de redes muy robustos.
En este proyecto se pretende formar una base sólida que muestre las especificaciones y características de la tecnología MPLS en redes virtuales privadas, siendo un tema de actualidad y de gran futuro.
Esto con el fin de proveer un pilar preeliminar para cualquier análisis y/o implementación del protocolo en un futuro.
El protocolo MPLS involucra diversos temas de actualidad entre los cuales se encuentra: Calidad de Servicio (QoS) e Ingeniería de Tráfico (TE).
Ambos son temas investigados hoy en día por un gran número de empresas y organizaciones gracias a las ventajas que presentan para establecer conexiones seguras sin importar la topología.

Ejemplificación de redes privadas virtuales.

Imaginemos un conjunto de ‘sedes’ conectadas a una red común o backbone.
Apliquemos algún tipo de política para crear un determinado número de subconjuntos e impongamos la siguiente regla: dos sedes podrán tener conectividad IP sobre dicho backbone sólo si al menos uno de estos subconjuntos contiene a ambos.

Tunneling

Los famosos ataques de hombre en medio se basa en que si alguien conecta su máquina a una red y utilice un sniffer recibirá y podrá ver los paquetes de datos que circulan por esta red, exponiéndose a modificaciones de datos, denegación del servicio, entre otras.
Si alguno de los protocolos que están trabajando envía sus paquetes en claro, y contiene información sensible, dicha información se verá comprometida.
tunneling es una forma de evitar este problema, sin dejar por ello de utilizar todos aquellos protocolos que carezcan de medios de cifrado, pues las comunicaciones se cifran con un sistema que permita entenderse sólo a las dos máquinas que participan en el intercambio de datos, al no poder descifrar los datos, cualquiera que intercepte desde una tercera máquina los paquetes, no podrá hacer nada con ellos.
Básicamente, esta técnica consiste en abrir conexiones entre dos máquinas por medio de un protocolo seguro, como puede ser SSH (Secure SHell), a través de las cuales realizaremos las transferencias inseguras, que pasarán de este modo a ser seguras, siendo la conexión segura (en este caso de ssh) el túnel por el cual se envían los datos para que nadie más aparte de los interlocutores que se sitúan a cada extremo del túnel, pueda ver dichos datos.
Este tipo de técnica requiere de forma imprescindible tener una cuenta de acceso seguro en la máquina con la que se quiere comunicar los datos.

VPN sitio-a-sitio

Este esquema se utiliza para conectar oficinas remotas con la sede central de organización.
El equipo central vpn, que posee un vínculo a Internet permanente, acepta las conexiones vía Internet provenientes de los sitios y establece el “túnel” vpn.
Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha.
Esto permite eliminar los costosos vínculos punto a punto tradicionales, sobre todo en las comunicaciones internacionales.

VPN de acceso remoto

Muchas empresas han reemplazado con esta tecnología VPN su infraestructura “dial-up”, donde el cliente utilizaba un modem para llamar a través de la Red Telefónica Conmutada a un nodo del Proveedor de Servicios de Internet y este con un servidor PPP establecía un enlace módem-a-módem, que permite entonces que se enrute a Internet.
Esta implementación se trata de comunicaciones donde los usuarios se conectan con la empresa desde sitios remotos (oficinas comerciales, casas, hoteles, etc.) utilizando Internet como medio de acceso.
Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

VPN Interna

Una aplicación realmente desconocida pero muy útil y potente consiste en establecer redes privadas virtuales dentro de una misma red local.

El objetivo último es aislar partes de la red y sus servicios entre sí, aumentando la seguridad.

Una aplicación muy típica de este modelo se utiliza para aumentar la seguridad en redes de acceso inalámbrico, separándolas así de la red física para evitar posibles fugas de información o accesos no autorizados.

Protocolos

PPTP

Point-to-Point Tunneling Protocol fue desarrollado por ingenieros de Ascend Communications, U.S. Robotics, 3Com Corporation, Microsoft, y ECI Telematics para proveer entre usuarios de acceso remoto y servidores de red una red privada virtual.

PPTP fue diseñado para permitir a los usuarios conectarse a un servidor RAS desde cualquier punto en Internet para tener la misma autenticación, encriptación y los mismos accesos de LAN como si discaran directamente al servidor.

IPSec

IPSec trata de remediar algunas falencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP.

Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme.

IPSec provee confidencialidad, integridad, autenticidad y protección a repeticiones mediante dos protocolos, que son Authentication Protocol (AH) y Encapsulated Security Payload (ESP).

L2TP

Layer-2 Tunneling Protocol (L2TP) facilita el entunelamiento de paquetes PPP a través de una red de manera tal que sea lo más transparente posible a los usuarios de ambos extremos del túnel y para las aplicaciones que éstos corran.

L2TP utiliza dos tipos de mensajes: de control y de datos.

Los mensajes de control son usados para el establecimiento, el mantenimiento y el borrado de los túneles y las llamadas.

Utilizan un canal de control confiable dentro de L2TP para garantizar el envío. Los mensajes de datos encapsulan los marcos PPP y son enviados a través del túnel.

Los subconjuntos creados son las Redes Privadas Virtuales (RPVs).

Dos sedes que no tengan una RPV en común no tendrán conectividad sobre ese backbone.

Si todas las sedes en una RPV pertenecen a la misma corporación, la RPV es una 'intranet' corporativa.

Si varias sedes pertenecen a diferentes empresas, la RPV es una 'extranet'.

Una sede puede estar en más de una VPN; por ejemplo, en una intranet y en varias extranets.

En general, cuando empleamos el término RPV no distinguiremos entre intranets y extranets.

A continuación, vamos a hacer una descripción funcional del servicio VPN-IP, de forma general, con el objetivo de ver las características que ofrece este servicio, con un poco más de detalle.

Interfaces LAN de cliente

El servicio VPN IP soporta las siguientes interfaces de acceso LAN, que constituyen el Punto de Acceso al Servicio (PAS). Estas interfaces cubren la mayor parte de los escenarios de cliente existentes en el mercado:

–Ethernet.

–Fast Ethernet

–Token Ring.

Ethernet.

El servicio VPN IP ofrece la interfaz Ethernet CSMA/CD, con velocidad de transmisión de 10 Mbps.

Los puertos asociados a la interfaz Ethernet son conformes a los siguientes estándares y especificaciones:

–IEEE Carrier Sense Multiple Access with Collision Detection STD 802.3 (1992).

–IEEE 10BaseT supplement STD 802.3i (1990).

Los métodos de encapsulado soportados en este tipo de interfaz son:

–Encapsulado estándar de Ethernet versión 2.0.

–Encapsulado IEEE 802.3.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

–Encapsulado IEEE 802.2.
–Encapsulado SNAP, especificado en la RFC 1042.

Fast Ethernet.

El servicio VPN IP ofrece la interfaz Fast Ethernet, con velocidad de transmisión de 100 Mbps.
Los puertos asociados a la interfaz Fast Ethernet son conformes a los siguientes estándares y especificaciones:
–100BaseT es la especificación de IEEE para la implementación Ethernet de 100-Mbps sobre cables de pares UTP (Unshielded twisted-pair) y STP (Shielded twisted-pair). El nivel MAC (Media Access Control) es compatible con el nivel MAC IEEE 802.3.
100BaseT utiliza la ya existente especificación IEEE 802.3 CSMA/CD.
Los métodos de encapsulado soportados en este tipo de interfaz son:
–Encapsulado estándar de Ethernet versión 2.0.
–Encapsulado IEEE 802.3.
–Encapsulado IEEE 802.2.
–Encapsulado SNAP, especificado en la RFC 1042.

Token Ring.

El servicio VPN IP ofrece la interfaz Token Ring con velocidades de transmisión seleccionables de 4 ó 16 Mbps, tanto para cable apantallado como sin apantallar.
Los puertos asociados a la interfaz Token Ring son conformes a los siguientes estándares y especificaciones:
–ANSI/IEEE Token Ring Acces Method STD 802.5 (1989).
–IBM Token Ring Network Architecture Reference SC30-3374-02 (1989).
Los métodos de encapsulado soportados en este tipo de interfaz son:
–Encapsulado IEEE 802.2.
–Encapsulado SNAP, especificado en la RFC 1042.

4.2.2. Usos

Los distintos usos que las redes privadas virtuales tienen actualmente, está siempre ligada a la movilidad de los usuarios, ya que estos, no siempre están físicamente en sus respectivos puestos de trabajo.
Muchas personas trabajan desde casa durante toda la semana o parte de ella, flexibilizando así sus jornadas laborales.
Por ello, muchas redes están diseñadas para proporcionar esta conexión remota de los usuarios que están trabajando fuera de la oficina tradicional.
Tanto el personal de ventas, o representaciones, trabajadores a domicilio (que no puedan acceder temporalmente a la red, debido a viajes de negocios o de placer), e incluso usuarios que pagan por acceder a nuestra red, todos ellos, necesitan conectarse a ella, y usarla de la misma forma que si estuviesen conectado a ella de manera física.
Por ello, la alternativa más segura para los accesos remotos, ha surgido en los últimos años con el nombre de redes privadas virtuales o VPN.
La función principal de VPN es permitir que los usuarios separados por grandes distancias, puedan enviarse datos a través de un enlace WAN existente (generalmente internet) de modo seguro y transparente para el usuario.
La técnica, básicamente, proporciona una vía de transmisión segura conocida como “túnel “entre dos sistemas.
El túnel puede conectar dos computadoras individuales o dos redes enteras.
Actualmente, existen 4 tecnologías diferentes o tipos de VPN compitiendo entre ellas, con sus puntos fuertes y débiles.
Uno de los mayores quebraderos de cabeza de una empresa o de algún usuario avanzado a la hora de implantar y mantener una red local de ordenadores es la seguridad.
Dentro de la red local esta es una tarea relativamente sencilla, ya que el administrador posee control total sobre el tráfico que va a circular sobre dicha red.
Pero supongamos ahora que una empresa X abre una nueva oficina a 1500 kilómetros de distancia y desea que dicha oficina esté conectada con la principal, de la misma manera que están conectados todos los ordenadores de una misma oficina.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

En este caso la única salida posible es pasar a través de Internet, pero claro, ya no tenemos control sobre el tráfico una vez los datos salgan al exterior y antes de que lleguen a la otra oficina.
Nuestra información por un momento estará a la vista de todo aquel que sepa buscarla. Este es un riesgo que nadie debería estar dispuesto a correr.
Por suerte hay una solución sencilla y barata para esta situación, la VPN (Virtual Private Network o Red Privada Virtual).
Una VPN es una extensión de una red local que permite conectar dos o más puntos de manera segura.
Hablando en plata, es como si entre las dos oficinas X, distanciadas por 1500 kilómetros, se tendiera un inmenso cable de red, sólo que la VPN hace uso de la misma red de acceso a Internet, por lo que no hay que gastar tiempo y dinero en conectar físicamente en realizar la mencionada conexión entre oficinas.
Normalmente, VPN usa una tecnología denominada tunneling a la hora de establecer la comunicación entre dos puntos.
El tunneling simplemente hace uso de un protocolo especial (normalmente SSH) para crear un "túnel" (de ahí su nombre) por el que circulan todos los datos desde un extremo a otro.
Este "túnel" en realidad es la misma información que se manda pero encriptada por la acción del protocolo seguro de comunicación, lo cual hace que nuestros datos no puedan ser vistos por agentes externos.
Otro de los usos más extendidos de las VPN es facilitar el acceso remoto a una red local.
Un ejemplo clásico lo tenemos en los empleados que deben acceder a la red del trabajo desde su portátil cuando se encuentran desplazados.
En sus portátil, el empleado tiene instalado un programa cliente de VPN que, tras introducir siempre un usuario y un password, se conecta con un servidor VPN situado en las oficinas de la empresa y así tener acceso a toda la red de la misma.
Actualmente, por su efectividad y su nulo coste, VPN es prácticamente la tecnología más usada para permitir el acceso remoto y la conectividad entre distintos agentes y segmentos de una misma red local, cuya distancia entre si sea demasiado grande como para optar por una conexión física y real.

4.2.3. Tipos

En la actualidad, existen por lo menos 4 tecnologías VPN compitiendo entre sí, cada una con sus puntos fuertes y débiles.

IPSEC VPN.

Por la forma en que originariamente fue concebida, el protocolo TCP IP es débil en términos de seguridad.
IPSEC es un grupo de protocolo añadido a la pila de TCP IP para proporcionar la seguridad real y fuerte que necesita, es decir capacidad de cifrado para los datos que fluyen a través de internet.
IPSEC trabaja a nivel de red sobre el protocolo, por lo que no depende de programas o aplicaciones específicas.
Una de las mayoras ventajas, por lo tanto, es que no es necesario que se diseñen aplicaciones a propósito, para que puedan hacer uso de las ventajas que proporciona IPSEC.
Con el objetivo de crear una VPN, IPSec establece un túnel entre una máquina cliente ejecutando software IPSec y un servidor IPSec, situado en el otro extremo de la conexión, es decir modo túnel.
En el modo túnel, el cifrado de IPSec se realiza sólo sobre los datos que fluyen por internet, y no cifra nada en la red local o entre un equipo remoto y su conexión a internet.
Por lo tanto, si se tiene una oficina remota que se conecta a la red de la oficina local a menudo, IPSec se convierte en una buena solución VPN.
Puede colocarse un servidor VPN, en cualquiera de los dos extremos de la conexión para liberar a los equipos de la oficina de la necesidad de ejecutar software IPSec de cliente.
De esta manera, se puede usar una conexión de internet para compartir el túnel VPN con los usuarios de la oficina remota.
Los servidores IPSec, se suelen vender como hardware en lugar de software para instalar en los servidores que ya tenemos. Por ejemplo Cisco, dispone de un módulo tipo plugin para sus modelos Catalyst 6500 switch y 7500 internet router que, una vez añadido, nos proporciona servicios VPN. También existen otro fabricantes como SSi que añaden soporte para IPSec VPN a sus aplicaciones de seguridad, proporcionando servicios de cortafuego y proxy al mismo tiempos que VPN.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

IPSec, puede realizar cifrado en las comunicaciones de usuario a usuario cuando se ejecuta en modo transport.
De todas formas, para utilizar esta modalidad, debe tenerse controlada la longitud de la transmisión, algo imposible con redes VPN, que requieren a sus usuarios que se conecten a internet usando una ISP proporcionada por una organización externa.
IPSec, dispone de 2 protocolos.
El primero es la cabecera de autentificación, que se ocupa de verificar la identidad del remitente de un mensaje y se asegura de que el contenido no ha sido modificado durante la transmisión.
El segundo protocolo se llama, carga máxima de seguridad encapsulada y cifra el contenido del campo de datos del paquete IP.
Estos dos protocolos, pueden actuar de dos maneras diferentes:
1)El modo túnel
2)El modo transparente.
El modo transparente, proporciona seguridad a los accesos de cliente a cliente.
Ya que este modo transparente, sólo funciona entre dos usuarios individuales, se convierte en una molestia para la VPN, y soporta el tráfico de túnel de los demás usuarios.
IPSec, autentifica usuarios como equipos.
Para la autentificación de usuarios, se requiere simplemente un nombre de usuario y contraseña.
También existe la autentificación de dos niveles, que solicita al usuario que proporciones algún dato más que le identifique cómo puede ser alguna clave de usar y tirar.
IPSec, también puede autentificar hardware, en detrimento de algunas VPNs finalizan la autentificación en la de dos niveles de usuarios.
IPSec, también puede identificar hardware estableciendo una asociación de seguridad, en cuyo caso alguna agencia debe asignar un certificado indicando que ciertos computadores es un cliente conocido y seguro.
Una vez que el usuario y el equipo están autentificados, IPSec, establece una asociación segura.
En teoría, la autentificación de hardware parece una buena idea para evitar que algún cracker pueda insertar una máquina espía en la red, pero el problema es que la autentificación de hardware mediante agencias independientes no está muy extendida en la actualidad y no sólo añade un corte a la implementación de la VPN, sino que tampoco existe un acuerdo general sobre qué agencias independientes son más seguras y, además, no se puede autentificar hardware de usuarios cuando éste no está bajo nuestro control.
En una situación en la que se necesita conectar usuarios remotos muy distanciados, una IPSec VPN puede no ser la opción más segura.
Las razones son:
–IPSec permite que sus usuarios se conecten a la LAN de destino, como si estuvieran presentes físicamente. Esto puede no ser deseable para algunos usuarios remotos, como por ejemplo clientes, o compañeros de negocio que no pertenecen a la empresa.
–La mayoría de los usuarios remotos, deben conectarse a una ISP antes de acceder a internet, por lo que esos datos no quedan sujetos a la
protección de IPSec, ya que viajan de un usuario remoto a un ISP.
–Los túneles de IPSec, no son compatibles con la mayoría de cortafuegos y no pueden pasar por un router usando traducción de direcciones de red o NAT.
–Para garantizar la compatibilidad con cortafuegos y NAT, es necesario obtener hardware específico, que sea capaz de aportar dichas
funcionalidades.
–IPSec, necesita que en cada máquina cliente, esté instalado su propia versión de IPSec. Esto no supone un problema, cuando todos los usuarios, trabajan con computadores de la empresa, como pueden ser los ordenadores portátiles que usan los trabajadores durante sus viajes.
Sin embargo, hay casos en que los usuarios necesitan utilizar equipos de otra procedencia, como pueden ser los puestos de conexión a internet que se encuentran en hoteles o cibercafés, que harían imposible el acceso a la VPN de IPSec.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

PPTP VPN.

Una alternativa a IPSec para accesos remotos es usar un protocolo basado en el mismo que las conexiones telefónicas, como puede ser el protocolo de túnel punta a punta PPTP.
Esta solución VPN, evita algunos de los problemas que entraña el uso de IPSec, incluyendo el problema de la incompatibilidad con cortafuegos y NAT (aun así, el protocolo PPTP, necesita un editor de paquete PPTP).
Además, los sistemas operativos de Microsoft y apple soportan este protocolo, así que no es necesario adquirir software extra para los clientes.
Los sistemas operativos para redes de ambos fabricantes, también proporcionan software de servidor para PPTP.
PPTP, ha sido diseñado como un envoltorio para el protocolo de punta a punta, que es el que usa la mayoría de las conexiones telefónicas para comunicarse entre el módem del cliente y el del servidor ISP.
Funciona, tomando el paquete PPP, encapsulándolo por el método de encapsulamiento genérico en ruta GRE y encapsulándolo una vez más para convertirlo en un paquete IP.
PPTP, cifra los datos del paquete PPP, aunque este cifrado no empieza hasta que la conexión PPP se ha realizado.
Esto significa, que el intercambio de datos para la autentificación se envía como texto visible.
PPTP, tampoco autentifica el hardware, aunque como ya se ha mencionado, la autentificación de hardware no es una práctica tan extendida de todas formas.
Por otra parte, PPTP no necesita certificados de autor CA de ningún tipo, lo que simplifica su implementación.

L2TP / IPSEC.

Los sistemas de IPSec y PPTP funcionan únicamente en redes TCP IP.
Si la WAN sobre la que se va a realizar el tráfico remoto usa otro protocolo, como por ejemplo X.25, Frame Relay o ATM, entonces no es viable ni IPSEC ni PPTP.
El protocolo de tunelado a dos niveles L2TP, que soportan tanto Microsoft como Apple, es una alternativa a los protocolos WAN e IP.
Cuando se usa conjuntamente a IP, proporciona funcionalidad de tunelado a través de internet.
Al contrario de PPTP, que usa TCP, L2TP se basa en datagramas UDP para controlar el túnel creado.
Cada paquete PPP es primero encapsulado como L2TP, luego como UDP y finalmente como IP.
L2TP puede trabajar junto con IPSec para ofrecer seguridad de usuario a usuarios.
Esta combinación, conocida como L2tP / IPSEC, usa la capacidad de cifrado de IPSec para codificar el campo de datos del paquete PPP y ya que IPSec establece una asociación de seguridad antes del comienzo de cualquier envío de paquetes PPP, la codificación se realiza previamente a la autentificación de usuario de PPP.
Esto indica que nos garantiza que el nombre de usuario y contraseña, quedan protegidos, en vez de enviarse en texto claro, como se hacía con PPTP.
De todas formas, la autentificación de IPSec, requiere que los mecanismos de asociación de seguridad estén activos.
L2TP, ha demostrado tener problemas para desplazarse a través de routers con NAT, pero esto se puede solucionar, haciendo que tanto el cliente como el servidor VPN, ejecuten la utilidad IPSEC NAT transversal, es decir NAT-T.

SSL VPN.

La última alternativa VPN es SSL, capa de puertos seguros.
Comenzó siendo un protocolo para hacer más seguro el tráfico a través de navegadores web.
SSL, proporciona acceso VPN para las aplicaciones de una interfaz web a las que se puede acceder con cualquier navegador web, funcionando en cualquier máquina.
También evita problema de NAT al incorporar unos proxy que redirecciona una conexión VPN a aplicaciones específicas.
No se requiere de software cliente especial, aunque en realidad SSL VPN sólo puede prescindir de él cuando la aplicación que va a hacer uso de la VPN, tiene interfaz de navegador web.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Para acceder a aplicaciones no basadas en web, el servidor SSL VPN, debe ser capaz de manejar proxy para trasladar el tráfico web a las aplicaciones requeridas.
La mayoría de fabricantes disponen de soluciones cliente, para poder tener acceso de manera similar, a como se realizaría con IPSec VPN, que permite al cliente conseguir acceso completo a la red local.

4.2.4. Implementaciones

Los servicios VPN pueden ser ofrecidos basados en dos axiomas:
–Overlay VPN´s donde el proveedor de servicios proporciona enlaces virtuales punto a punto entre redes de clientes.
–Peer-to-Peer VPN´s donde el proveedor de servicios participa en el routing del cliente.

Beneficios de las diferentes implementaciones de vpn´s

OVERLAY VPN
·Muy conocidas y fáciles de implementar.
·El Proveedor de Servicios no participa en el routing del cliente.
·La implementación de un routing óptimo requiere full-mesh de VC´s.
·VC´s tienen que ser manualmente implementados.
PEER-TO-PEER VPN
·Garantiza un routing óptimo entre redes de clientes.
·Más fácil realizar la provisión de una nueva VPN.
·Sólo los sites son provisionados, no los enlaces entre ellos.
·El Proveedor de Servicios participa en el routing de los clientes.
·El Proveedor de servicios es responsable de la convergencia del cliente.
·Los PE´s llevan todas las rutas de todos los clientes.
En una primera aproximación, se puede implementar una VPN mediante mecanismos hardware.
Éstos se basan normalmente en routers con encriptación, que tienen la ventaja de ser lo más parecido a equipos “plug&play”.
Su única tarea es encriptar y desencriptar las tramas que pasan a través de ellos, por lo que tienen buenas prestaciones y no introducen demasiado retardo en la red.
Ahora bien, no tienen tanta flexibilidad como los sistemas basados en software. Otra aproximación son sistemas basados en Firewalls.
Estos sistemas aprovechan las ventajas del firewall como la restricción de acceso a la red o generación de registros de posibles amenazas, y ofrecen además otros como traducción de direcciones o facilidades de autentificación fuerte.
Ahora bien, el hecho de insertar el servicio de VPN dentro de un firewall puede afectar en mayor o menor medida al rendimiento del sistema, lo que puede o no ser un problema dependiendo de nuestras necesidades.
Si esto se convierte en un problema, algunos fabricantes de firewalls ofrecen procesadores dedicados a encriptación para minimizar el efecto del servicio VPN en el sistema.
Por último, los sistemas puramente software son ideales en los casos en los que los dos extremos de la comunicación no pertenecen a la misma organización, o cuando aun estando dentro de la misma organización, las tecnologías de routers y/o firewalls difieren.
Esta solución permite mayor flexibilidad en cuanto a la decisión de qué tráfico enviar o no por el túnel seguro, pudiendo decidir por protocolo o por dirección, a diferencia de los sistemas hardware, que normalmente sólo permiten decidir por dirección.
Puede ser conveniente en situaciones donde la VPN es útil en algunos casos (consultas a una base de datos) pero irrelevante en otros (navegación normal por la web).
También es útil en los casos en los que la conexión se realiza por líneas lentas.
Ahora bien, no todo son ventajas.
Los sistemas software son difíciles de administrar, ya que requieren estar familiarizados con el sistema operativo cliente, la aplicación VPN y los mecanismos de seguridad adecuados.
Y algunos paquetes VPN requieren cambios en las tablas de encaminamiento y los esquemas de traducción de direcciones.
Sin embargo, las fronteras entre estas tres aproximaciones se van diluyendo conforme pasa el tiempo.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Existen fabricantes que proporcionan soluciones basadas en hardware, pero que incluyen clientes software para VPN e incluso características que sólo se encontraban en los sistemas basados en firewalls.
Por otro lado, la introducción del protocolo IPSec está facilitando la mezcla de distintos productos VPN.
En cuanto a los algoritmos de encriptación, se puede utilizar prácticamente cualquiera: desde la encriptación de 40 bits que lleva W9x por defecto a algoritmos más elaborados como triple DES.
La autentificación de usuarios se realiza utilizando cualquier técnica, desde métodos software a passwords dinámicos tanto software como hardware.

4.2.5. Parámetros de configuración y gestión de interconexión de redes privadas virtuales

En la gestión de la interconexión de redes privadas virtuales, antes de proceder a los parámetros de configuración, existen unas tareas previas que deben de ser satisfechas para una correcta terminación del circuito y asignación de recursos de red necesarios.
En un entorno operador, los parámetros de configuración y gestión de interconexión de redes privadas virtuales, poseen particularidades ligeramente diferentes que a la hora de configurar entornos de VPNs bajo software o sistemas operativos.
La primera fase sería, la de tareas de asignación, que a continuación, se va a proceder a mencionar brevemente los pasos que se llevan a cabo.

Tareas de asignación.

Asignación de punto de acceso:
–En esta tarea se elige la central telemática más cercana para la terminación del circuito y se asignan los recursos necesarios para el acceso a la red.
–Esta tarea se realizará sea cual sea el tipo de circuito, lo único que cambia es el tipo de recursos asignados en función de la tecnología utilizada por el medio de transmisión.
Asignación de canales:
–En esta tarea se asignaran los parámetros que definen el origen y destino de un camino virtual, ya sea FR o ATM.
Asignación de recursos de gestión:
–Esta tarea es realizada automáticamente por el sistema en función de los requerimientos de servicio.
–Se asignarán direcciones IP de gestión y canales de gestión según sean necesarios.
Asignación de red:
–En esta tarea se asignan los recursos de nivel 3 necesarios para el acceso a la red y el funcionamiento del servicio. Parámetros como; direcciones IP WAN, Router e interfaz de acceso a la red de nivel IP a configurar….
La siguiente fase, consiste en las tareas de configuración de las asignaciones anteriormente indicadas.
Configuración de parámetros de red:
–Se configura el interfaz de red asignado, para que sea accesible desde toda la red y los canales virtuales asignados anteriormente.
Configuración de los parámetros de red en los routers de la red de acceso:
–Se configura en los router de la red de acceso los parámetros asignados anteriormente.
Configuración de recursos de red FR/ATM:
— Esta tarea aparecerá en servicios con accesos que utilizan tecnología ATM para el acceso a la red (ADSL).
Existen ciertos parámetros que deben de ser configurados en la red MPLS para preparar los routers en los bordes o fronterizos de dicha red MPLS, junto con las interfaces ethernet de los routers cliente que necesitan ser preparadas igualmente para trabajar con MPLS y las VRFs (tablas virtuales de routing and forwarding) en los routers fronterizos, además de establecer la configuración correspondiente de BGP entre los routers fronterizos y los de cliente para que se conozcan todas las rutas posibles a las distintas sedes de la compañía.
Con respecto a la configuración de las interfaces del router fronterizo contra la interfaz del router cliente, los parámetros de configuración serían:
ROUTER CISCO Fronterizo (PE) contra la interfaz del router de cliente.
<Id Interface WAN> Es el nombre del interface o subinterface de interconexión con el cliente (P.E.: Serial 0/1/0).

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

<Id router de Cliente>Nombre que describa el router de cliente con el que se establece la conexión (Este comando no es obligatorio pero ayuda a la hora de revisar la configuración).
<Id VRF>Nombre asignado a la VRF.
Son tablas de enrutamiento virtuales routing and forwarding, que son utilizadas para distinción de paquetes entre VPNs y la importación y exportación de rutas.
Cada VPN que se crea, debe tener una VRF diferente, pero en explotación, todas las VPNs del mismo cliente se les asigna el mismo nombre VRF para establecer una concordancia.
<Dirección IP WAN> Dirección IP Wan de la conexión a configurar (como norma general la primera dirección útil del rango asignado).
ROUTER CISCO de cliente.
<Id Interface WAN> Es el nombre del interface físico de conexión con el router fronterizo o PE. Este valor será: El interface serial disponible, normalmente Serial0/3/0
<Dirección IP WAN> Dirección IP Wan de la conexión a configurar (como norma general, en los routers será la segunda dirección útil del rango asignado).

4.3. Mecanismos de seguridad

Seguridad de redes.

Debemos tener en cuenta la seguridad de la red desde el mismo momento en que se plantea el diseño de la misma.
El punto de partida debe ser una planificación correcta que nos permita eliminar muchas de las vulnerabilidades que suelen afectar a las redes y limitar el efecto de los ataques que puedan afectarnos.
El término seguridad de redes es muy amplio.
En el mayor de los sentidos, significa proteger la información o los datos que están almacenados o que navegan por la red contra una modificación o
divulgación intencional o accidental no autorizada.
La parte de esta definición que se pasa por alto con más frecuencia, es la que incluye los incidentes ocasionales, como por ejemplo un programa de una aplicación al que no se le haya realizado una adecuada depuración o corrección de errores y que pueda llegar a dañar los datos.
Otras de las visiones de cómo entender la seguridad es considerando la confidencialidad o privacidad con la seguridad.
La confidencialidad es la necesidad de restringir el acceso a los datos, ya sean secretos comerciales o de carácter personal que por ley debe mantenerse de forma privada.
Dicho de otro modo, la seguridad es la acción que se lleva a cabo, para asegurar la confidencialidad o privacidad.
La seguridad, posee 3 objetivos:
1)Confidencialidad: Asegurar que los datos se mantengan y sean de carácter privado.
2)Integridad: Asegurar que los datos sean los adecuados. Para un profesional de la seguridad, esto significa que los datos deben estar protegidos contra modificaciones no autorizadas y / o su destrucción.
3)Disponibilidad: Asegurar que los datos sean accesibles en todo momento. Esto implica proteger la red de cualquier cosa que pueda provocar su indisponibilidad, incluida la indisponibilidad del suministro eléctrico.
Los mecanismos de seguridad son el tercer aspecto que se considera en la seguridad de la información.
Un mecanismo de seguridad es una técnica que se utiliza para implementar un servicio, es decir, es aquel mecanismo que está diseñado para detectar, prevenir o recobrarse de un ataque de seguridad.
Los servicios de seguridad especifican “qué” controles son requeridos y los mecanismos de seguridad especifican “cómo” deben ser ejecutados los
controles.
Los mecanismos básicos pueden agruparse de varias formas.
Conviene resaltar que los mecanismos poseen tres componentes principales:
a)Una información secreta, como claves y contraseñas, conocidas por las entidades autorizadas.
Las contraseñas resultan ser el fundamento y la mayor molestia en el campo de la seguridad de redes.
Hasta hace poco, un nombre de usuario y su contraseña correspondiente era la única manera de autentificar a un usuario frente a una red.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Sin embargo, y a pesar del creciente abaratamiento y la accesibilidad que suponen las unidades de reconocimiento por parámetros biométricos, las contraseñas siguen siendo el método más usado para garantizar un
acceso seguro.
Las contraseñas son almacenadas en alguna parte de los servidores en los que se autentifican los usuarios. Ya que los ficheros en los que se almacenan dichas claves, tienen la forma de un archivo igual que cualquier otro, suponen un botín de lo más apetecible para los crackers de sistemas.
Ejemplo:
Si un cracker consigue hacerse con el archivo de contraseñas, lo siguiente que hará es intentar descifrarlo para hacer uso de él y conseguir acceso a los recursos del servidor.
b)Un conjunto de algoritmos para llevar a cabo el cifrado, descifrado y generación de números aleatorios.
El cifrado es un método para cambiar la apariencia de un mensaje y evitar así que su contenido sea inteligible a ojos de cualquier usuario.
Se usa una clave que sólo conocen el emisor y el receptor para convertir el mensaje de texto legible en una cadena carente de sentido antes de enviarlo y para restablecerlo a texto legible cuando el receptor legítimo lo recibe.
El cifrado, también llamada encriptación, es el método de protección de mensajes más común para proteger el contenido de los mismos, mientras se mueven fuera del sistema en el que se originaron, y se puede usar también para proteger datos almacenados en un disco duro.
El cifrado y los métodos que lo acompañan son, aun así, la mejor manera de proteger los mensajes que se envían desde nuestra red y los datos almacenados en los discos duros.
Un conjunto de algoritmos que se usan para llevar a cabo el cifrado son:
·Esquemas de cifrado de clave única.
·Algoritmos de sustitución.
·Algoritmos de cifrado de clave única (estándar de cifrado de datos (DES), Triple DES, estándar de cifrado avanzado (AES), RC4.
·Esquemas de cifrado de doble clave.
c)Conjunto de procedimientos, que definen cómo se usarán los algoritmos, quién envía qué a quién y cuándo.
No existe un único mecanismo capaz de proveer todos los servicios, sin embargo, la mayoría de ellos hace uso de técnicas criptográficas basadas en el cifrado de la información.
Los mecanismos pueden ser clasificados como preventivos, detectables, y recuperables.
Los procedimientos que definen como se usan los algoritmos, son:
·Esquema de cifrado de clave única.
·Esquemas de cifrado de doble clave.
·Esquemas de combinación de clave única y clave doble.

4.3.1. Enmascaramiento y redirección

El enmascaramiento IP y el redireccionamiento de puertos permiten utilizar un determinado rango de direcciones privadas de una red local en concreto, para posteriormente ser utilizadas por un router, el cual actuará en nombre de la máquina que realiza la petición, y hará uso de la única dirección IP pública que posee junto con una traducción de direcciones IP y puertos.

La forma de operar que tiene el enmascaramiento es que cuando al router le llega un datagrama IP por parte de cualquier equipo de la red local, el router inspecciona el protocolo de nivel superior que encapsula dicho datagrama (UDP, TCP, ICMP), y posteriormente modifica el datagrama, para que parezca que ha sido generado por el propio router.

Posteriormente, el router reenvía el datagrama hacia internet, el cual aparece como dirección origen la dirección IP pública del router.

Una vez que la máquina de destino ha recibido el datagrama procedente del router con la dirección IP pública, y responde a esta última, la interfaz del router al cual está conectada internet, realiza un mapeo en su tabla de direcciones enmascaradas, para buscar la dirección privada a la cual le corresponde la respuesta del datagrama generado por el equipo destino.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Si se localiza la dirección privada de la LAN en dicha tabla, el router deshace el enmascaramiento y reenvía el datagrama al equipo local correspondiente.

4.3.2. Filtrado de paquetes

Introducción.

El filtrado de paquetes del protocolo IP es un mecanismo que principalmente se emplea en cortafuegos y en routers.
Este filtrado de paquetes son un conjunto de reglas que permiten o deniegan la entrada o salida de ciertos paquetes a una red determinada.
En este sentido, se utiliza los recursos necesarios para gestionar el filtrado de paquetes, con el fin de obtener políticas de reglas de acceso o salida de ciertos paquetes.
En los casos donde no se especifica exclusivamente dichas reglas, existen unas reglas de omisión para negar el acceso de paquetes y descartar el paquete.
Para filtrar paquetes, son necesarios ciertos datos para llevar a cabo tal operación.
–Dirección IP de origen
–Dirección IP de destino
–Protocolo (TCP, UDP e ICMP)
–Indicador de acuse de recibo (ACK)
–Puerto de origen
–Puerto de destino
–Dirección (de entrada, de salida o ambas)
–Interfaz de red (puerto seguro, puerto no seguro o ambos)
–Si el paquete es un fragmento
Por otro lado, todo el tráfico que se filtra puede ser marcado para su posterior análisis en un registro de anotaciones, incluso todo el tráfico de entrada, salida y además el que se deniega.

Cortafuegos de filtrado de paquetes.

Los cortafuegos de filtrado de paquetes funcionan en los niveles 3 y 4 del conjunto de protocolos TCP / IP, filtrando los paquetes TCP y UDP basados en cualquier combinación de direcciones IP origen, direcciones IP destino, puertos de origen o de destino.
El cortafuegos más sencillo de filtrado de paquetes filtra sólo paquetes de entrada y bloquea aquellos destinados a puertos que hayan sido cerrados.
Las modalidades más sofisticadas permiten a un administrador definir reglas, como combinación de los criterios disponibles.
Ejemplo:
Por ejemplo, una norma podría permitir el tráfico web puerto 80 en la red, sólo si los paquetes disponen como dirección IP de destino la del servidor web de la organización.
Cualquier otro tráfico web quedaría bloqueado.
Los cortafuegos de filtrado de paquetes y en especial aquellos que se ejecutan en encaminadores o en accesorios independientes, también aportan la traducción de direcciones de red NAT.
Un router externo muestra una única dirección IP a internet.
A medida que van llegando los paquetes, el cortafuego lo examina para determinar el puerto y mapearlo a la dirección IP interna del ordenador principal, donde el puerto está abierto.
Las direcciones Ip internas suelen ser direcciones no encaminables, que se ocultan a internet.
La mayoría de los cortafuegos personales, aquellos que están diseñados para que se ejecuten y protejan una estación de trabajo única, son cortafuegos de filtrado de paquetes.
Son ligeramente distintos de aquellos que se ejecutan en routers diseñados para redes domésticas.
Normalmente, los cortafuegos personales disponen de mejores capacidades de registro o control, que aquellos que se encuentran en los routers de las redes domésticas y por supuesto, no disponen de NAT.

Limitaciones de los cortafuegos en el filtrado de paquetes.

Existen 2 limitaciones importantes de los cortafuegos basados en el filtrado de paquetes.
La primera, no examinan la carga útil del paquete y la segunda, no mantienen un seguimiento o control de lo que le ocurre a un paquete una vez que pasa el cortafuegos

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Listas de acceso.

Introducción.
La utilización de listas de acceso en la configuración de un router se da por diferentes motivos:
–Denegar tráfico no deseado.
–Especificar los paquetes que pueden provocar una llamada en un entorno de marcación bajo demanda (DDR).
–Implementar procedimientos de seguridad/acceso.
–Actuar como un "firewall" de protocolo.
–Limitar conexiones VTY.
Las listas de acceso pueden ser de dos tipos:
1.Estándar: en ella se especifican direcciones más simples y generalmente permite y deniega un conjunto de protocolos completo.
2.Extendida: en este caso hay especificaciones de dirección más compleja y permiten y deniegan protocolos específicos.
Básicamente las listas de acceso, lo que hacen es permitir o denegar el paso de tráfico según unas condiciones especificadas.

Comando access list.

En primer lugar se seleccionan los parámetros para las condiciones de análisis de esta lista de acceso. Las condiciones pueden ser una o varias.
Access-list access-list-number {permit|deny} {test conditions}
En segundo lugar hay que habilitar el interface para que sea parte del grupo que utiliza la lista de acceso especificada. {protocol} access-group access-list-number

Identificación de listas de acceso.

Las listas de acceso se especifican en un rango numérico según el protocolo. Estos rangos son los siguientes:
IP Estándar 1-99
IP Extendida 100-199
IP Nombradas (las identifica un nombre)
IPX Estándar 800-899
IPX Extendida 900-999
IPX Filtros SAP 1000-1099
AppleTalk 600-699
Las listas de acceso IP, pueden ser nombradas a partir de Cisco IOS 11.2

4.3.2.1. Características

Listas de acceso ip estándares.
Se utilizan para filtrar tráfico del tipo IP. Se configuran de la siguiente manera:
Access-list número-lista-de acceso {permit|deny} {máscara-comodín|any}
Ip access-group número-lista-de acceso {in|out}
Ejemplo:

Access list 1 permit 192.168.0.0 0.0.255.255
Access list 1 deny any
interface receden 0
ip access-group 1

En este caso estamos permitiendo la red 192.168.0.0.
La segunda línea no sería necesaria, ya que implícitamente se deniega todo lo demás.
Después aplicamos la lista de acceso al interface ethernet.
Máscaras comodin.
Las máscaras comodín se ponen en orden inverso a la máscara de red. Un 0 en la máscara wildcard indica que el bit de la trama que llegue debe ser
idéntico al de la dirección de referencia.
Por el contrario, un 1 indica que el bit de la trama que llegue da igual el valor que tenga.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Si se omite la máscara se supone que es 0.0.0.0, o sea, la trama debe tener la misma dirección que el patrón, sino no pasa.

Ejemplos:

0.0.0.0 255.255.255.255 à Cualquier dirección
131.108.0. 0 0.0.255.255 à la red 131.18.0.0
131.111.8.0 0.0.7.255 à Sólo la subred 131.111.8.0
131.104.7.11 0.0.0.0 à El host 131.104.7.11
255.255.255.255 0.0.0.0 à Broadcast local

Cuando permitimos un rango, implícitamente queda negado todo lo demás.

Sería redundante poner:

Ejemplo:

access-list 1 deny any.

Restricción de acceso a terminales virtuales.

Para asignar una restricción a terminales virtuales se deben ejecutar los siguientes comandos:

Ejemplo:

Line {número-vty|rango-vty} (Access-class número-lista-acceso {in|out}

Ejemplo:

i
access-list 12 permit 192.168.95.0 0.0.0.255
!
line vty 0 4
access-class 12 in

En este caso permite conectarse a los puertos virtuales del router sólo a los ordenadores de la red 192.168.95.0.

Listas de acceso ip extendidas.

Permiten condiciones de filtrado más precisas. Con las listas de acceso extendidas se puede controlar la dirección IP origen y destino y especificar un número de puerto de protocolo IP para la dirección origen y para la de destino.

Configuración:

Ejemplo:

access-list número-lista-acceso {permit|deny}
{protocolo \ palabraclave-protocolo}{fuente-comodin-fuente|any}
{destino-comodin-destino|any}
[recedente precedencia] [tos tds]

Utilizan el rango del 100 al 199. Al igual que las listas de acceso estándares, las extendidas también se pueden asignar a una interfaz

Ejemplo:

ip access-group número-lista-acceso{in|out}

Alternativas a las listas de acceso.

INTERFACE NULL.

Consiste en introducir una ruta a ninguna parte, con lo cual se ahorran valiosos ciclos de CPU.

Consiste en crear una ruta estática (no se debe asignar a ninguna interfaz) para filtrar el tráfico no deseado.

El nombre del interface al que se envía dicho tráfico es el Null 0.

El comando tiene la siguiente estructura:

Ip route red máscara null 0

Criterios.

Los criterios sobre los que se basa los mecanismos de Seguridad y donde poseen su verdadero fundamento son 2 esenciales:

1)Fuentes y orígenes de amenazas externas.

2)Fuentes y orígenes de amenazas internas.

4.3.2.2 .Criterios

Fuentes y orígenes de amenazas externas.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Con respecto a las amenazas externas, hacemos mención a internet, donde este fenómeno ha sido una completa bendición y en otros aspectos, una maldición en toda regla.
Una maldición, sobre todo para aquellos que se basan en las redes informáticas para mantener operativa una organización.
La red global ha hecho posible que los clientes potenciales o futuros, los clientes actuales y los empleados puedan acceder a una organización a través de su sitio web.
Pero con este nuevo acceso, han surgido numerosos problemas provocados por individuos y grupos que intentan entrar de forma ilegal en las redes de ordenadores y en los sistemas informáticas que los soportan.
Fuentes y orígenes de amenazas internas.
En la mayoría de los casos, los empleados saben más sobre una red y sobre los ordenadores que existen en ella que cualquier persona externa.
La mayoría de las amenazas internas provienen de dos fuentes: de los empleados y por accidente o causalidad.
También las amenazas provenientes de los empleados pueden ser intencionales o accidentales.
Por supuestos, el personal informático dispone de diferentes niveles de
acceso.
Los empleados pueden provocar grandes perjuicios de forma no intencionada, siendo tan peligrosos como los ocasionados por los empleados que amenazan la seguridad de manera intencionada.
Teóricamente, la mayoría de las amenazas no intencionadas provenientes de los empleados pueden gestionarse mediante la educación del empleado.
Los accidentes provocados por los empleados pueden dañar una red de forma no intencionada.
Además los accidentes ocurren sin más.
Una planificación de seguridad debe asegurar una protección contra las pérdidas y los daños sobre los datos causados por:
–Oscilaciones o fluctuaciones eléctricas.
–Fallos de hardware.
–Desastres naturales como por ejemplo, incendios o inundaciones.

4.3.2.3. Ventajas

Las ventajas de los mecanismos de seguridad se resumen ciertamente en la importancia de una buena política de seguridad, ya que esta, marcará las directrices que aportarían los beneficios y ventajas de las implementaciones de mecanismos de seguridad.
Una buena política de seguridad es un documento que expone la filosofía y estructura de las iniciativas de seguridad de una organización.
Cumple con los siguientes propósitos:
–Una política de seguridad es la documentación que ha diseñado la alta dirección para su cumplimiento.
Una política de seguridad escrita facilita la justificación de los gastos de seguridad al personal de informática.
–Una política de seguridad proporciona una guía para el personal de informática que estén planeando diseñar un sistema de seguridad en la red. Indica lo que tiene que estar protegido y quién es la persona responsable de esa protección.
–Una política de seguridad identifica una utilización aceptable de los recursos informáticos de la organización. Por ejemplo, puede indicar si los empleados pueden utilizar un sistema de correo electrónico corporativo para los correos privados y si es así, en qué medida.
–Una política de seguridad también identifica quién debe tener acceso y a qué.
Ésta puede ser una de las partes más difíciles de la política a desarrollar, porque el acceso a la información normalmente lleva implícito o connota los privilegios concretos dentro de una organización.
–Una política de seguridad actúa, como un contrato de seguridad con los empleados. Deben cumplir con la filosofía y los comportamientos reflejados en dicha política para poder seguir trabajando en la organización.
–Se puede proporcionar información sobre la política de seguridad a los nuevos empleados, antes de que empiecen a trabajar.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

De hecho, algunas organizaciones requieren que los nuevos empleados lean la política de seguridad y firmen una declaración, indicando que la entienden y que están de acuerdo con el cumplimiento de las disposiciones o requerimientos exigidos.
Conlleva mucho esfuerzo preparar y mantener una política de seguridad útil.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

5. Procedimientos de instalac. y prueba de dispositivos de interconexión de redes

5.1. Normativas de seguridad física y eléctrica aplicables a los dispositivos de interconexión de redes

Normativa de seguridad física en los dispositivos de interconexión de redes.

Concepto de seguridad física en los sistemas de información y comunicaciones.

La seguridad física en relación con los dispositivos de interconexión de redes, están clasificadas dentro de las sistemas de información y comunicaciones, cuyas zonas fijas o semipermanentes donde se ubiquen los dispositivos de interconexión de redes, deben de ser acreditados.
Esta acreditación como zonas de acceso restringido, pueden ser clasificadas como áreas de clase I o de clase II, según los criterios establecidos en la normativa NS/03 de la autoridad nacional sobre seguridad física.
Aparte del requisito de la clasificación de la zona de acceso restringido para aquellas instalaciones que alojan servidores o equipos críticos de red y de comunicaciones, donde almacenen, procesen o transmitan información clasificada, tendrán que ser acreditadas aparte de área de clase I, con medidas de seguridad adicionales especiales para proteger la posibilidad de acceso no autorizado a los equipos, clasificados como críticos.
Todas las medidas que se requieran como especiales, serán bajos los criterios que en todo momento establezca la AAS, mediante normativa específica o como un requisito de seguridad para la acreditación de un determinado sistema.
En las zonas, donde se alojan servidores o equipos de interconexión de redes críticos o de comunicaciones, donde se almacene, procese o transmita información clasificada con un grado de confidencialidad o superior, deberán ser acreditadas como Área de Clase I.
Cuando las zonas que albergan terminales de sistemas de información o equipos de interconexión de redes o de comunicaciones no críticos, deberán de acreditarse como Área de Clase II.
Para terminar con este apartado introductorio hay que destacar una serie de antecedentes ocurridos en EEUU y en España, que han dado paso a una serie de normativas, directivas y leyes, en materia de protección de las infraestructuras críticas.
La Unión Europea crea un programa de protección de infraestructuras críticas (PEPIC), estableciendo procedimientos que analicen las vulnerabilidades y la interdependencia, entre dichas infraestructuras, así como la presentación de soluciones que eliminen o mitiguen dichas vulnerabilidades.
Seguidamente, se aprueba la directiva 2008/114/CE, sobre la identificación y designación de cada una de las infraestructuras catalogadas como críticas.
En España se crea el catálogo nacional de infraestructuras y el plan nacional de infraestructuras críticas.
Más adelante, se aprueba la ley 8/2011 de 28 de Abril, en la que se diferencian las infraestructuras estratégicas, como pueden ser instalaciones, redes, sistemas y equipos de sistemas de información, sobre los que versan los servicios esenciales, y las infraestructuras críticas, que son ni más ni menos que infraestructuras estratégicas, cuyo funcionamiento no se permite soluciones alternativas.
Estas últimas infraestructuras críticas, cualquier distorsión o perturbación en el funcionamiento normal, o su destrucción total, causaría un grave impacto sobre los servicios esenciales que lleva a cabo.
Una infraestructura crítica es también una infraestructura estratégica, pero que no permite soluciones alternativas y que la perturbación o destrucción de la misma, causaría un grave impacto sobre los servicios que sustenta.

Seguridad en el personal.

La seguridad en el personal de acceso a zonas restringidas, donde se alberguen servidores y/o dispositivos de redes/comunicaciones, deben de estar habilitadas y en posesión de la acreditación Habilitación Personal de Seguridad (HPS), correspondiente al máximo grado de clasificación de la información, que puedan tener acceso a dicho sistema o zona de acceso restringido.
Esta habilitación es inherente a toda seguridad física de los dispositivos de interconexión de redes, servidores o cualquier dispositivo, donde se almacene, procese o transmita información clasificada, por lo que este criterio dentro de la seguridad física, resulta indispensable y necesario para una correcta implementación y gestión de normas de seguridad física para los dispositivos mencionados.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Esta acreditación resulta de aplicación para todo aquel personal, que no estén autorizadas a acceder a dicho equipamiento ni al tratamiento de los mismos, siempre y cuando hablemos de información clasificada.
El personal de mantenimiento, limpieza o administración, requerirá de dicha acreditación HPS, siempre y cuando la AOSTIC, determine ciertas medidas de actuación de aquel personal, cuando en el momento de acceso de dicho personal, no haya información clasificada a la vista o acceso fácil a los dispositivos de interconexión de redes o comunicaciones.
El personal que no tenga la acreditación HPS, independientemente de que exista información clasificada, irá acompañada del personal que esté en
posesión de dicha acreditación HPS, además de la formación técnica necesaria, para no comprometer la integridad, confidencialidad y disponibilidad de la información.
Este procedimiento de actuación del personal sin posesión de la acreditación HPS, deberá ir recogido en los procedimientos operativos de seguridad del sistema (POS).
Con respecto al personal dedicado a las tareas de administración, configuración y supervisión de los dispositivos de interconexión de redes, servidores y demás dispositivos de comunicaciones, donde se almacene, procese o transmita información clasificada, deberá estar en posesión de la acreditación HPS, con un grado superior a la máxima clasificación de la información manejada en el sistema, ya que el status del que goza este personal de administración de los dispositivos, que le permite el acceso total a la información clasificada es privilegiado.
Este grado superior de clasificación que se le concede al personal de administración de los sistemas y dispositivos, es con total independencia del criterio de necesidad de conocer, establecido en la norma NS/02 sobre seguridad en el personal de la Autoridad Nacional.
Esta habilitación del personal con acceso al equipamiento de comunicaciones y sistemas de información, se realizará, conforme al procedimiento establecido en la norma NS/02 sobre seguridad en el persona, con los criterios y medidas que se establezcan.
En relación al personal con acceso a los sistemas y dispositivos de interconexión de redes, podemos distinguir, diversas tareas, como por ejemplo, la administración de los mismos, la seguridad y la supervisión, pueden ser asignadas a personal diferente.
De hecho así se establece la asignación de tareas concretas y específicas en la operación con los sistemas y dispositivos de interconexión de redes.
Esta asignación de tareas concretas y específicas a cada personal, debe de estar recopilada y establecida de manera clara, tendrá que estar reflejada en los POS del sistema.
Por otro lado, en los POS del sistema, deberá reflejarse como anexos, la lista detallada de las personas que tienen acceso autorizado a los sistemas y dispositivos, así como los derechos de los que gozan y los permisos con los que cuentan para el cometido de sus diferentes tareas.
Importante
Identificar y autenticar a los individuos con acceso autorizado, deben de basarse en el principio de necesidad de conocer.

En búsqueda de una combinación de controles medioambientales, junto con el cumplimiento íntegro de los objetivos de disponibilidad, confidencialidad e integridad, en materia de seguridad física, deberán instalarse en las zonas catalogadas como de acceso restringido:
–Equipos de detección de incendios.
–Equipos de detección de temperatura y humedad.
–Sensores de agua.
–Sistemas de alimentación ininterrumpida.
Estos controles medioambientales, que se establecen en materia de seguridad física, deberán ser monitorizados permanentemente, por el centro de control de alarmas.
Seguridad física en los armarios de telecomunicaciones de dispositivos de interconexión de redes.
El armario de Telecomunicaciones, está dedicado exclusivamente al equipamiento de telecomunicaciones, ya sean, servidores, sistemas de información, dispositivos de interconexión de redes, etc.
Los equipos que no están destinados a tal fin, no deben de instalarse en el armario de telecomunicaciones, ni pasar a través de ellos, y mucho menos, entrar en ellos.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Mínimo de 1 armario por piso, y se deben de incorporar armarios adicionales por cada área por encima de los 1000 metros cuadrados, siempre que sea mayor de esa distancia y la distancia horizontal, pase de los 90 metros.

Dimensiones recomendadas basadas en 1 estación de trabajo por cada 10 metros:

Área atendida (m)	Dimensiones del armario(mm)
1000	3000*3400
800	3000*2800
500	3000*2200

Espacio de piso en la sala de equipos para edificios de utilizacion especial

N° de estaciones de trabajo	Area (m²)
0 a 100	14
101 a 400	36
401 a 800	74
801 a 1200	111

Espacio minimo en la pared para equipo y terminación

Área atendida (m)	Longitud de la pared(mm)
1000	990
2000	1060
4000	1725
5000	2295
6000	2400
8000	3015
10000	3630

Espacio minimo en el piso para equipo y terminación

Area atendida (m)	Dimensión de la sala (m²)
10000	3660*1930
20000	3660*2750
40000	3660*3970
50000	3660*4775
60000	3660*5588
80000	3660*6810
100000	3660*8440

Normativa de seguridad eléctrica en los dispositivos de interconexión de redes.

Las compañías eléctricas han convergido en la implantación de una arquitectura común de comunicaciones, sobre todo en las subestaciones, donde la automatización, es el factor clave de la tendencia que estas compañías eléctricas están experimentando.

El objetivo de todo esto es conseguir interoperabilidad entre los diferentes dispositivos inteligentes electrónicos (IEDs), que están ubicados en las subestaciones.

Esta iniciativa, fue impulsada bajo el auspicio de las compañías eléctricas norteamericanas EPRI (Electric Power Research Institute).

Esta nueva normativa internacional denominada IEC 61850 tiene como base la plataforma de comunicaciones basada en ethernet.

La subestación tradicional se llevaba a cabo mediante comunicaciones seriales de baja velocidad entre IEDs, donde este sistema era poco flexible y limitado a su control.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Esto daba lugar a un poco práctica implementación de este sistema, si requería un elevado número de interconexiones alambradas rígidas entre IEDs.
Las comunicaciones en tiempo real punto a punto son difíciles de realizar, debido a las comunicaciones seriales de baja velocidad, limitándose al arreglo de las comunicaciones maestro/esclavo.
–En la actualidad y bajo este nuevo estándar internacional, las ventajas de una red ethernet en las subestaciones eléctricas son:
–Comunicaciones de alta velocidad.
–Mínimo alambrado entre IEDs.
–Múltiples protocolo sobre la misma red física.
–Acceso fácil y confiable de datos sobre IP, mediante el uso de switches ethernet, conversores de medios, servidores seriales y routers, que están diseñados con los mismos estándares y normas que los dispositivos críticos de protección eléctrica.
El estándar IEC 61850 en una subestación eléctrica puede tener dos aplicaciones principales: Station Bus y Process Bus.
El "Station Bus" es una aplicación donde los relés y RTUs se conectan directamente a una LAN-Ethernet, mientras que el "Process Bus" se refiere a dispositivos como CT/VT, que proporcionan los valores de corriente y voltaje directamente sobre la LAN-Ethernet.
Para obtener un alto grado de confiabilidad en esta comunicación, es necesario utilizar dispositivos Ethernet de grado industrial que cumplan las exigencias del estándar IEC 61850.
Estos equipos deben garantizar la no pérdida de información bajo difíciles condiciones EMI (Electromagnetic Interference), ya que la información de la LAN será usada para medir y controlar la operación de la subestación.
Los encabezamientos principales en relación a la seguridad eléctrica aplicable a los dispositivos de interconexión de redes o de telecomunicaciones, se puede establecer en 3 ejes principales.
3)Protección de los usuarios de los equipos, frente a los riesgos generados por dicho equipos.
4)Protección del personal que trabaja en la red de telecomunicación, junto con otros usuarios, frente a riesgos peligrosos, generados por la conexión implícita del equipo en la red de telecomunicación.
5)Protección de todos los usuarios relacionados con los equipos de interconexión o de comunicaciones, frente a los riesgos derivados de las tensiones de la red de telecomunicación.

Separación con Relación a Fuentes de Energía y Electromagnética.

La instalación conjunta de cables de telecomunicaciones y cables de energía está gobernada por la norma de seguridad eléctrica aplicable.
Los requisitos mínimos para separación entre circuitos de alimentación (120/240V, 20 A) y cables de telecomunicación en EE.UU están dados por el artículo 800-52 de la ANSI/NFPA 70 que prevé: los cables de telecomunicaciones se deben separar físicamente de los conductores de energía; cuando pasan por la misma canaleta deben estar separados por barreras entre el cableado lógico y el eléctrico; incluso dentro de cajas o compartimentos de tomas, debe haber separación física total entre los cableados.
Para reducir el acoplamiento de ruido producido por cables eléctricos, fuentes de frecuencia de radio, motores y generadores de gran porte, calentadores por inducción y máquinas de soldadura, se deben considerar las siguientes precauciones:
Aumento de la separación física; los conductores línea, neutro y tierra de la instalación deben mantenerse juntos (trenzados, sujetos con cinta o atados juntos) para minimizar el acoplamiento inductivo en el cableado de telecomunicaciones; Uso de protectores contra irrupción en las instalaciones eléctricas para limitar la propagación de descargas; uso de canaletas o conductos metálicos, totalmente cerrados y puestos a tierra, o uso de cableado instalado próximo a superficies metálicas puestas a tierra; éstas son medidas que irán a limitar el acoplamiento de ruido inductivo.

5.1.1. Lista de las principales normas

Lista de normas relativas a la seguridad física.

Nivel nacional:
1)Autoridad nacional para la protección de la información clasificada.
2)NS/05 Seguridad en los sistemas de información y comunicaciones.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

3)NS/03 Seguridad física.
4)OR-ASIP Orientaciones para la constitución de zonas de acceso restringido.
5)Ley 8/2011 de 28 de Abril.
Nivel Europeo:
–Directiva 2008/114/CE, sobre la identificación y designación de cada una de las infraestructuras catalogadas como críticas.
Nivel Internacional:
–ANSI / TIA / EIA - 569 norma de construcción comercial EIA/TIA-569 para espacios y recorridos de telecomunicaciones.

Lista de normas relativas a la seguridad eléctrica.

Nivel Internacional:
–IEC 61850 Estándar de comunicación para subestaciones eléctricas.
–ANSI / TIA / EIA - 569 norma de construcción comercial EIA/TIA-569 para espacios y recorridos de telecomunicaciones.
Nivel Europeo:
–Normas técnicas armonizadas de material eléctrico para equipos de tecnologías de la información y para equipos y componentes para telecomunicaciones y radiocomunicaciones.
–EN 60950; 2000
UNE EN 60950; 2002.
Seguridad de los equipos de tratamiento de la información.
–EN 60950-1; 2001
UNE EN 60950-1; 2003
Equipos de tecnología de la información. seguridad. parte 1: requisitos generales.
–EN 60950-21; 2003
UNE EN 60950-21; 2004
Equipos de tecnología de la información. seguridad. parte 2: alimentación remota.
–EN 41003; 1998
UNE EN 41003; 2000
Reglas particulares de seguridad, destinados para equipos que se conectan a las redes de telecomunicaciones.
–EN 50065-1; 2001
UNE EN 50065-1; 2002.
Aplicable a los equipos eléctricos que utilizan señales de frecuencias situadas entre 3 KHz y148,5 KHz, para la transmisión de información, por las redes eléctricas de baja tensión, ya sea por las redes públicas o por las redes de los consumidores.

5.1.2. Características destacadas de cada una

Normativa de seguridad física

NS/05 seguridad en los sistemas de información y comunicaciones.

En esta normativa se pueden extraer las características más destacadas de dicha normativa, en relación con la seguridad en los sistemas de información y comunicaciones, como son:
a)Seguridad de la información (documental)
Se expone los órganos encargadas de la custodia de la información clasificada como CONFIDENCIAL, a efectos de protección de dicha
información.
Por otro lado también se refleja la custodia y responsabilidad de la
información catalogada con un grado de DIFUSIÓN LIMITADA y que no estén jerárquicamente dependientes de ningún órgano de control, dichas tareas serán designadas a un responsable de seguridad.
La clasificación de la información, deberán estar en sistemas autorizados, según el grado de clasificación de la documentación.
Con respecto a los dispositivos removibles, los usuarios son los últimos responsables de ellos, y además deben de estar debidamente etiquetados, manteniendo el grado de clasificación que se les haya

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

encomendado, según la información que contenga, salvo en casos en que hayan sido desclasificados por un procedimiento aprobado.
La información grabada en soportes reutilizables, solo podrán borrarse por procedimientos aprobados por la AAS.
b)Seguridad en el personal
Todas aquellas personas que tengan acceso a los sistemas o dispositivos, donde se almacene, procesen o transmita información clasificada con un grado CONFIDENCIAL o superior, además de acceder a lugares o zonas de acceso donde estén ubicados este equipamiento crítico, deberán estar en posesión de la acreditación de personal de seguridad HPS.
Otro tipo de personal podrá prescindir de dicha acreditación HPS, siempre y cuando la AOSTIC haya establecido un procedimiento que asegure que no hay información clasificada a la vista y que este escoltado por personal con la acreditación HPS y la formación técnica para no comprometer la disponibilidad, integridad ni confidencialidad de la información.
c)Seguridad física
Aquellas instalaciones fijas o semipermanentes donde se ubiquen los distintos componentes de los sistemas que manejen información clasificada "CONFIDENCIAL o equivalente" o superior, deberán estar acreditadas como zonas de acceso restringido, que podrán estar configuradas como área clase I o área clase II, según los criterios que se marcan.
Aquellas instalaciones fijas o semipermanentes donde se ubiquen sistemas que manejen información clasificada de grado "DIFUSIÓN LIMITADA o equivalente", deberán estar constituidas como zonas administrativas de protección, salvo que sean ZAR.
d)Seguridad en los sistemas de información y comunicaciones.
Proporciona confidencialidad, integridad, disponibilidad, además de requerir la autenticación de personas y el no repudio, para determinar que una acción concreta ha sido llevada a cabo, sin que exista la posibilidad de rechazar tal acción.
e)Organización de la seguridad.
Cuenta con estructuras STIC de la organización, estructura de operación STIC del sistema y estructura de control de material de cifrado de la
organización.
f)Gestión de los riesgos de seguridad.
Lleva a cabo, un exhaustivo proceso de gestión de los riesgos de la seguridad, así como de las zonas física donde se ubican los sistemas y equipos de interconexión de redes críticos.
g)Interconexión de sistemas.
La interconexión de sistemas, requiere su debida acreditación de la interconexión al mayor grado de clasificación de la información, que se maneje dentro de estos sistemas.
Debido a una gran variedad de razones que nos llevan a esta debida acreditación, es la única forma de poder asegurar la disponibilidad, integridad y confidencialidad de la información clasificada entre sistemas.
h)Servicios Criptológicos.

NS/03 seguridad física

La característica más destacada con respecto a esta norma estaría vinculada, a la ubicación de equipos de sistemas de información y comunicación, cuya seguridad física de dichas instalaciones, resultan prioritarias para cumplir los objetivos de disponibilidad e integridad.
Junto a los objetivos de integridad y disponibilidad, se añaden ciertas controles medioambientales, que son necesarios, como puede ser la instalación de sistemas contra incendios, equipos de detección de temperatura y humedad, sensores de agua y sistemas de alimentación ininterrumpida.

OR-ASIP orientaciones para la constitución de zonas de acceso restringido.

Una de las características más notables y actuales de esta norma, en relación a los dispositivos de interconexión de redes y sistemas de información, es su seguridad física.
En esta norma, además de contemplar la seguridad física en zonas de acceso restringido, tiene una característica especial que está en plena sintonía con el equipamiento de interconexión de redes y sistemas de información, y es que las instalaciones en las que los CIS (Sistema de Información y Comunicaciones) son utilizados para visualizar, almacenar, procesar o transmitir Información Clasificada de grado CONFIDENCIAL

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

o superior, deberán ser acreditadas como Zonas de Acceso Restringido, configurada como Área Clase I o Área Clase II según el procedimiento de explotación de la Información Clasificada que se siga en dicha zona. Las instalaciones que alojan Servidores o Equipos Críticos de Red, de Comunicaciones o de Cifra, que almacenan, procesan o transmiten Información Clasificada, deberán ser acreditadas como Área Clase I. Cuando el Entorno Local de Seguridad protege Terminales de Sistemas de Información y Comunicaciones o Equipos No Críticos de Red, de Comunicaciones o de Cifra que almacenan, procesan o transmiten Información Clasificada, deberá acreditarse como Área Clase II.

Ley 8/2011 de 28 de abril:

Preámbulo

Los Estados modernos se enfrentan actualmente a diferentes desafíos que confieren a la seguridad nacional un carácter cada vez más complejo.

Estos nuevos riesgos generados en gran medida por la globalización, y entre los que se cuentan el terrorismo internacional, la proliferación de armas de destrucción masiva o el crimen organizado, se suman a los ya existentes, de los cuales el terrorismo tradicional venía siendo un exponente.

–Para su protección se hace imprescindible, por un lado, catalogar el conjunto de aquellas que prestan servicios esenciales a nuestra sociedad y, por otro, diseñar un planeamiento que contenga medidas de prevención y protección eficaces contra las posibles amenazas hacia tales infraestructuras, tanto en el plano de la seguridad física como en el de la seguridad de las tecnologías de la información y las comunicaciones.

–Sin embargo, la seguridad de las infraestructuras críticas exige contemplar actuaciones que vayan más allá de la mera protección material contra posibles agresiones o ataques, razón por la cual resulta inevitable implicar a otros órganos de la Administración General del Estado, de las demás Administraciones Públicas, de otros organismos públicos y del sector

privado.

Estas infraestructuras críticas dependen cada vez más de las tecnologías de la información, tanto para su gestión como para su vinculación con otros sistemas.

Artículo 1. Objeto.

1)Esta Ley tiene por objeto establecer las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, para mejorar la prevención, preparación y respuesta de nuestro Estado frente a atentados terroristas u otras amenazas que afecten a infraestructuras críticas.

Artículo 2. Definiciones.

a)Servicio esencial

b)Sector estratégico

c)Subsector estratégico

d)Infraestructuras estratégicas

e)Infraestructuras críticas

f)Infraestructuras críticas europeas

g)Zona crítica

h)Criterios horizontales de criticidad

i)Análisis de riesgos

j)Interdependencias

k)Protección de infraestructuras críticas

l)Información sensible sobre protección de infraestructuras estratégicas

m)Operadores críticos

n)Nivel de Seguridad

o)Catálogo Nacional de Infraestructuras Estratégicas

Artículo 7. El Centro Nacional para la Protección de las Infraestructuras Críticas.

–Se crea el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) como órgano ministerial encargado del impulso, la coordinación y supervisión de todas las actividades que tiene

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

encomendadas la Secretaría de Estado de Seguridad en relación con la protección de las Infraestructuras Críticas en el territorio nacional.
Artículo 13. Operadores críticos.

–Los operadores considerados críticos en virtud de esta Ley deberán colaborar con las autoridades competentes del Sistema, con el fin de optimizar la protección de las infraestructuras críticas y de las infraestructuras críticas europeas por ellos gestionados.
ANSI / TIA / EIA - 569 norma de construcción comercial EIA/TIA-569 para espacios y recorridos de telecomunicaciones.
–Las características más destacadas por esta norma destinada para espacios y recorridos de telecomunicaciones, van desde los recorridos horizontales, pasando por armarios de telecomunicaciones, recorridos para backbones, salas de equipos, estación de trabajo y sala de entrada de servicios.
En recorridos horizontales, las características más destacadas son:
·Implican en infraestructuras para instalación de cable de telecomunicaciones proveniente del armario de las mismas y destinado a una toma/conector de telecomunicaciones.
·Los recorridos horizontales pueden ser de dos tipos: canaleta debajo del piso, piso de acceso, conducto eléctrico, bandejas y tuberías de cableado, cielo raso y perímetro.
·Las directrices y los procedimientos de proyecto se especifican directamente para estos tipos de recorridos
·Consisten en los recorridos internos (dentro de un edificio) y entre edificios (externos).
·Consisten en los recorridos internos (dentro de un edificio) y entre edificios (externos).
·Dan los medios para la colocación de cables backbones a partir de:
›La sala o espacio de acceso para armarios de telecomunicaciones.
›La sala de equipo para la sala o espacio de acceso, los armarios de telecomunicaciones.
·Están compuestos de conducto eléctrico, manga de conexión, aberturas y bandejas.
En recorridos entre edificios, las características más destacadas son:
›Están compuestos de recorridos de cables subterráneos, enterrados, aéreos o en túneles.
–En estaciones de trabajo, las características más destacadas son:
·Espacio interno de un edificio donde un ocupante actúa entre sí con dispositivos de telecomunicaciones.
–En tomas de telecomunicaciones, las características más destacadas son:
·Localización del punto de conexión entre el cable horizontal y los dispositivos de conexión del cable en el área de trabajo.
·Se refiere a la caja (alojamiento) o faceplate en general, al contrario de las tomas incluyendo los conectores de telecomunicaciones individuales.
·Es necesaria una toma por estación de trabajo como mínimo (dos por área de trabajo).
·La destinación de espacio de trabajo es una por cada 10 m2.
·Por lo menos se debe instalar una toma de energía cerca de cada toma de telecomunicaciones.
–En armarios de telecomunicaciones, las características más destacadas son:
·Dedicado exclusivamente a la infraestructura de las telecomunicaciones.
·Equipos e instalaciones extraños a las telecomunicaciones no se deben instalar en estos armarios, ni pasar a través o entrar en los mismos.
·Mínimo de un armario por piso.
·Se deben conseguir armarios adicionales para cada área por encima de 1.000 m2 siempre que:
›El área atendida del piso sea mayor que 1.000 m2
›La distancia horizontal pase de los 90 m.
–En salas de equipo, las características más destacadas son:
·Espacio destinado para equipos de telecomunicaciones.
·Acomoda solamente equipos directamente relacionados con el sistema de telecomunicaciones y los sistemas de apoyo ambiental correspondientes.
·Determinación del tamaño:
›Para satisfacer los requisitos conocidos del equipo específico.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

›Si el equipo es desconocido planifique un área de 0,07 m2 de espacio para cada 10 m2 de área de trabajo.
›Deberá tener un área mínima de 14 m2.

Normativa de seguridad eléctrica.

IEC 61850 Estándar de comunicación para subestaciones eléctricas.
Las características más destacadas de este estándar de comunicaciones para subestaciones eléctricas son:
–Mejora de la calidad del suministro.
–Integración de la generación renovable en la red eléctrica.
–Necesidad de monitorización de los consumos.
–Nuevos modelos de negocio en el sector eléctrico.
–Requiere menor cableado.
–Mayor flexibilidad.
–Ampliación o modificación más simple.
–Configuración y puesta en marcha.
–Diagnósticos.
–Funcionalidad ampliada.
–Mantenimiento.
Otras características también muy destacadas son:
–El desarrollo de un estándar internacional para las comunicaciones en el interior de una subestación automatizada.
–Conseguir interoperabilidad entre equipos de diferentes proveedores.
–Comunicaciones cerca de los equipos de potencia, con capacidades para adquisición de datos y control, incluidas directamente en los equipos primarios.
–Reducción del cableado convencional.
–Los servicios que se desplieguen serán duraderos a pesar de los rápidos cambios tecnológicos.
–Está diseñado para seguir la evolución como el progreso de los sistemas de comunicación.
EN 41003; 1998 / UNE EN 41003; 2000
Reglas particulares de seguridad, destinados para equipos que se conectan a las redes de telecomunicaciones.
Esta norma relativa a los equipos que se conectan a las redes de telecomunicaciones, tiene unas características destacadas que son:
–Protección de los usuarios y operarios frente a los potenciales peligros de los equipos generados por ellos.
–El cumplimiento de las normas de seguridad, darán la protección adecuada al usuario de los peligros generados por el equipo, como por ejemplo, una de las normas listadas en el Anexo A.
–Protección del personal de administración que trabajan en la propia red de telecomunicación, junto con otros usuarios con acceso a dichos equipos, frente a potenciales condiciones peligrosas que la red de telecomunicación generan, debido a la conexión del equipo.
–Protección de todos los usuarios implicados en la red de telecomunicación que tengan acceso a los mismos, frente a las tensiones de generan la red de telecomunicaciones.
EN 50065-1; 2001 / UNE EN 50065-1; 2002.
En esta norma relativa a la transmisión de señales por la red eléctrica por los equipos de telecomunicaciones, se presenta las características siguientes:
–Aplicable a los equipos eléctricos que utilizan señales de frecuencias situadas entre 3 KHz y 148,5 KHz, para la transmisión de información, por las redes eléctricas de baja tensión, ya sea por las redes públicas o por las redes de los consumidores.
–Se especifica las bandas de frecuencias, asignadas a las distintas aplicaciones, los límites de tensión en la banda utilizada, además de los límites de las perturbaciones. Igualmente, se determina los métodos de medida.
ANSI / TIA / EIA - 569 norma de construcción comercial EIA/TIA-569 para espacios y recorridos de telecomunicaciones.
Las características más destacadas de esta norma, en relación con las norma en materia eléctrica, aplicable a los dispositivos de interconexión de redes o de telecomunicación son:

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

–La instalación conjunta de cables de telecomunicaciones y cables de energía está gobernada por la norma de seguridad eléctrica aplicable.
–Los requisitos mínimos para separación entre circuitos de alimentación (120/240V, 20 A) y cables de telecomunicación en EE.UU. están dados por el artículo 800-52 de la ANSI/NFPA 70 que prevee:
·Los cables de telecomunicaciones se deben separar físicamente de los conductores de energía;
·Cuando pasan por la misma canaleta deben estar separados por barreras entre el cableado lógico y el eléctrico;
·Incluso dentro de cajas o compartimentos de tomas, debe haber separación física total entre los cableados.
–Para reducir el acoplamiento de ruido producido por cables eléctricos, fuentes de frecuencia de radio, motores y generadores de gran porte, calentadores por inducción y máquinas de soldadura, se deben considerar las siguientes precauciones:
·Aumento de la separación física; los conductores línea, neutro y tierra de la instalación deben mantenerse juntos (trenzados, sujetos con cinta o atados juntos) para minimizar el acoplamiento inductivo en el cableado de telecomunicaciones; Uso de protectores contra irrupción en las instalaciones eléctricas para limitar la propagación de descargas; uso de canaletas o conductos metálicos, totalmente cerrados y puestos a tierra, o uso de cableado instalado próximo a superficies metálicas puestas a tierra; éstas son medidas que irán a limitar el acoplamiento de ruido inductivo.

5.2. Procedimientos de carga de configuración en dispositivos de interconexión de redes

Formas de conexión para la carga de la configuración en dispositivos de interconexión de redes.
Existen cinco formas de acceder al router desde dispositivos externos
–Puerto de consola: Este puerto está configurado por defecto con el valor 9,600-N-8-1 (null parity, 8 data bits, 1 stop bit).
Sin embargo se puede configurar a con las siguientes velocidades: 1200, 2400, 4800 y 9600.
Por diseño, este puerto es el más recomendado para configuraciones y modificaciones.
Cuando se configura el router por primera vez se suele usar este puerto para conectar un PC dotado de un programa de emulación VT como la aplicación hyper-term.
–Puerto auxiliar: Este puerto está configurado por defecto con el valor 9,600-N-8-1. Sin embargo, con la excepción de las series 3600, la máxima velocidad soportada es de 38400bps.
Los routers de la serie 3600 soportan velocidades máximas de 115200bps. Este puerto está diseñado para la conectividad y mantenimiento fuera de banda.
Esto no significa que no pueda usurase para la transmisión de datos ya que si se configura correctamente, puede conectarse a un módem.
–VTY 0 4: Los virtual terminals permiten la conexión al router a través de una Red. 0 4 indica el número de conexiones simultáneas que se pueden establecer. Todas ellas pueden modificar la configuración al mismo tiempo.
–TFTP: (Trivial file Transfer Protocol) Es otra opción para conectividad en banda. Requiere que previamente el router esté configurado para trabajar en Red. El servidor TFTP puede almacenar los ficheros de IOS y/o configuración que se cargan en el router
–Network Management: Son programas que permiten gestionar el router remotamente como Cisco Works.
Estas 5 formas de conexión al router, sirven igualmente para establecer los diferentes procedimientos de carga de la configuración al equipo de interconexión de redes.
Cada una de las formas de conexión, tienen una particularidad singular dependiendo del entorno, que van desde la configuración y el establecimiento previo de una plantilla de configuración personalizada del servicio, hasta la carga de un fichero de configuración, mediante TFTP o con un programa de gestión remota de routers, como por ejemplo Cisco Works.
A continuación, se va a exponer debido a su gran importancia en la configuración del archivo principal de configuración del router, los distintos niveles dentro de un router Cisco Systems, para proceder a la carga del archivo de configuración.
Cada nivel que a continuación se va a exponer, tiene sus restricciones y límites, dependiendo del nivel de privilegio que tenga el usuario y el objetivo de la tarea a desarrollar.
Existen 6 niveles de conexión:

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

–Usuario: Este es el modo inicial en que los usuarios acceden al router para autentificarse cuando el router está funcionando de forma correcta con una configuración.
En este modo no es posible realizar ninguna modificación en la configuración aunque sí se pueden realizar un diagnóstico básico.
Este modo requiere una password de acceso y se identifica por el símbolo ">" en el promt después del nombre de usuario (router>)
–Privilegiado: Desde este modo es posible entrar en modo configuración y realizar cambios sobre la misma, realizar análisis más detallados, aplicar debugs y realizar diagnósticos más específicos.
Este modo tiene una password de acceso visible y otra encriptada.
Se identifica por el símbolo "#" en el promt (router #).
–Configuración: Este es el modo empleado en la configuración de un router. Permite al administrador modificar el fichero de configuración actual (running-config).
La única forma de acceder a este modo es estando en modo privilegiado. Se identifica con la palabra "config" en el promt. (router (config)#).
–Setup: Este modo se utiliza en la configuración inicial del router.
Es recomendable que sólo se use para este fin y que las sucesivas modificaciones se realicen en modo configuración.
Existen dos formas de entrar en este modo:
·Si el router no encuentra un archivo de configuración válido, muestra un mensaje al administrados preguntando si desea entrar en este modo.
·La otra forma es accediendo desde el modo privilegiado, tecleando la palabra 'setup'.
–ROM: Este modo es el que aparece cuando el router no encuentra una imagen de IOS válida o si se interrumpe la secuencia de arranque antes de que el router pueda cargar la IOS.
Se identifica porque sólo aparece en el promt el símbolo ">". Muchos routers, como los de las series 1000, 4500, 7200 y 7500 podrán tener su propio promt "rommon>".
Tecleando la palabra 'continue' devolverá al administrador al modo
usuario.
–RX-Boot: Este modo se utiliza cuando el router no puede encontrar una imagen de IOS válida.
El RX-boot es un subconjunto de la IOS que es capaz de realizar funciones básicas configurar un interfaz o cargar una IOS desde un servidor TFTP.
Sin embargo, no tiene capacidad de enrutamiento. Se identifica con la palabra "boot" en el promt (router (boot)>).

Configuración básica de un router.

Introducción.
Los routers proporcionan el hardware y software necesarios para encaminar paquetes entre redes locales y de área extensa.
Existen muchos modelos de routers Cisco, cada uno de ellos diseñado para satisfacer las necesidades de una determinada conexión en red.
La gama media y alta es modulable, o sea puede ampliarse y/o modificarse el hardware existente (la IOS puede ser modificada en todos los routers).
El hardware de un router consta principalmente de una CPU –normalmente RISC, memoria RAM, Flash RAM, NVRAM y ROM; interfaces de consola, LAN y WAN.
Tanto del hardware como del software de un router podemos ver el estado –y por supuesto configurar- mediante una serie de comandos implementados en la IOS
Establecer la configuración básica de un router no es más que activar las distintas interfaces del router y configurar los parámetros de software para los protocolos encaminados (IP, IPX, AppleTAlk, etc.) y de encaminamiento (RIP, EIGRP, NLSP, etc.).
Así mismo en cada interfaz WAN se debe configurar el correspondiente protocolo de nivel de enlace (Frame Relay, PPP, etc.) y su sincronización.
Toda la configuración del router se guarda en un archivo almacenado en la memoria RAM (running-config), el cual debe almacenarse en la memoria no volátil NVRAM (startup-config) para poder restaurarla en caso de apagado del equipo.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

El archivo de configuración también puede extraerse de un servidor de TFTP dentro de la red.
A continuación, vamos a realizar un estudio de las distintas fases a tener en cuenta en el procedimiento de carga de ficheros de configuración de equipos de interconexión de redes, ya que es de vital importancia, su conocimiento como su estudio.
Los ficheros de configuración, junto con la IOS, son elementos a conocer muy importantes a la hora de configurar equipos de interconexión de redes, además de que hay que tener muy en cuenta, una multitud de cuestiones precedentes, que harán una gestión y configuración responsable y eficiente de dichos equipos de interconexión de redes.

Arquitecturas run from flash y run from ram.

Introducción.
Run-from flash
Los routers CISCO que utilizan arquitectura "run-from-Flash" incluyen a los Cisco 1601-Cisco 1604 y los Cisco 2500 series.
Debido a que la IOS se está ejecutando desde la flash no se puede cargar una versión de IOS a la flash donde está corriendo. Además no puede estar comprimida.
run-from RAM
Cisco routers tales como 1000, 3600, 4x00, y7x00 series utilizan la arquitectura run from RAM.
Si nos bajamos la IOS desde un servidor de red, cualquier Cisco router,
(incluyendo Cisco 1601-Cisco 1604 y Cisco 2r500 series) correrán desde la RAM.
En una arquitectura run-from-RAM, la imagen IOS puede estar comprimida en la flash.
Esto reduce la cantidad de memoria flash requerida para almacenar el software. El router descomprimirá la imagen Cisco IOS y la copiará a la memoria RAM para poder ejecutarla.
Durante el proceso de upgrade el router continúa conmutando paquetes.

Interpretación del nombre de una iOS.

Introducción.
Cisco tiene una nomenclatura para el nombre de la imagen con el que se identifica la plataforma, las funcionalidades que soporta y el área de memoria en la que la imagen corre en tiempo de ejecución.
Se puede clasificar en tres partes:
–PPPPP= Plataforma.
–FFFF= Características, funcionalidades.
–MM= Memoria en tiempo de ejecución y formato de compresión.
Ejemplo de nombre de IOS C7200-ajs40-mz
PPPPP-FFFF/MM
Identificadores de plataforma:
–PPPP La plataforma indica que es un Cisco 7200 Series Router.
–Funcionalidades contenidos en la imagen IOS.
–FFFF
En el ejemplo, la "a" indica que posee la característica (APPN) , "j" es para características enterprise (desktop plus all routing protocols), "s" es para características plis como el NAT, Inter-Switch Link (ISL), L2F, and VPDN, y el número "56" indica una encriptación de 56 bits.
Memoria en tiempo de ejecución y formato de compresión.
(En el anexo del documento se incluye una tabla con el significado de las letras)
MM está compuesta por 2 letras. La primera identifica el área de memoria conde la IOS se ejecuta en tiempo de ejecución. La segunda letra indica el método utilizado para comprimir la imagen.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Área en tiempo de ejecución

F	La imagen arranca desde la flash
m	La imagen arranca desde la RAM
R	La imagen arranca desde la ROM
L	La imagen se ejecuta en la flash "run-from-flash"

Identificadores de compresión

Z	La imagen es comprimida en formato ZIP
x	La imagen es comprimida en formato MZIP
w	La imagen es comprimida en formato "Stac"

Tipos de release

Cisco puede describir la release con dos letras:
Release Software: construye versiones basadas en major release ya consolidadas.
ED: Early deployment release: normalmente se identifica con letras mayúsculas, ejemplo 12.0(7)T.
La early deployment aparece porque hay que añadir ciertas funcionalidades al aparecer una nueva tecnología.
A su vez tiene 2 ciclos de vida; LD (limited deployment) que es un paso intermedio entre ED y GD.
GD: release que se ha consolidado y extendido por la mayoría de las plataformas y es estable.
Ejemplo de early deployment release:
Ejemplo:
S= Service Provider, ejemplo 12.0S
T= tecnología consolidada 12.0T

Interpretación del registro de la configuración.

Introducción.
El router guarda el registro de configuración en la NVRAM y se compone de 16 bits.
Se puede utilizar el registro de configuración para las siguientes tareas:
–Forzar a que el router entre en ROM Monitor (bootstrap program).
–Seleccionar un fichero de arranque o utilizar un fichero por defecto.
–Habilitar y deshabilitar la tecla de Break.
–Controlar el formato de las direcciones de broadcast.
–Cargar la subconjunto de la IOS (Rxboot).
Significado de los bits del registro de configuración:

Campo de arranque	Hexadecimal
00	Permanece en modo ROM monitor tras un reseteo o apagado del equipo
01	Arranca de la Rxboot o subconjunto de la IOS
02-F	Con el comando boot system arranca una IOS situada en el dispositivo indicado. Si no existe este comando en la configuración, el sistema arranca de la primera imagen que haya en la flash

Bit Number	Hexadecimal	Significado
00-03	0x0000-0x000F	Campo de arranque
06	0x0040	Ignora el contenido de la NVRAM
07	0x0080	OEM bit habilitado
08	0x0100	Tecla break deshabilitada
09	0x0200	Causa que el sistema utiliza la imagen de bootstrap secundaria Normalmente esta opción no se utiliza (se pone a 0).
10	0x0400	IP broadcast con todo a ceros
5, 11, 12	0x0020, 0x0800, 0x1000	Velocidad de la línea de consola
13	0x2000	Arranca del software de la ROM si el arranque desde un servidor falla.
15	0x8000	Habilita mensajes de diagnóstico e ignora el contenido de la NVRAM.

Cambiando el registro de configuración

Se puede querer modificar los valores del registro de configuración para desarrollar las siguientes tareas:

–Recuperación de una password perdida.

–Cambiar la velocidad de acceso a la consola.

–Habilitar o deshabilitar la tecla de Break.

–Manualmente arrancar una imagen con el comando b en modo ROMmonitor.

–Forzar al router para que automáticamente arranque desde la Rxboot, o arrancar en función del comando boot system almacenado en el fichero de configuración en la NVRAM.

Configurando el campo de arranque

Los cuatro últimos bits del registro de configuración (bits 3, 2, 1, y 0) forman el campo de arranque.

Campo de arranque	Descripción
00	Permanece en modo ROM monitor tras un reseteo o apagado del equipo
01	Arranca de la Rxboot o subconjunto de la IOS
02-F	Con el comando boot system arranca una IOS situada en el dispositivo indicado. Si no existe este comando en la configuración, el sistema arranca de la primera imagen que haya en la flash

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Action/File Name	Bit 3	Bit 2	Bit 1	Bit 0
Bootstrap mode	0	0	0	0
Default software	0	0	0	1
cisco2-RSP	0	0	1	0
cisco3-RSP	0	0	1	1
cisco4-RSP	0	1	0	0
cisco5-RSP	0	1	0	1
cisco6-RSP	0	1	1	0
cisco7-RSP	0	1	1	1
cisco10-RSP	1	0	0	0
cisco11-RSP	1	0	0	1
cisco12-RSP	1	0	1	0
cisco13-RSP	1	0	1	1
cisco14-RSP	1	1	0	0
cisco15-RSP	1	1	0	1
cisco16-RSP	1	1	1	0
cisco17-RSP	1	1	1	1

Interpretación del bit 8

Bit 8 controla la tecla de Break. Poniendo a uno el bit 8 (valor por defecto de fábrica) causa que el procesador ignore la tecla Break desde consola.

Poniendo a cero el bit 8 fuerza al router a entrar en modo ROM Monitor. Break se puede enviar antes de los primeros 60 segundos durante el proceso de arranque.

Interpretación de los bits 10 y 11

Bit 10 controla las direcciones IP broadcast.

Poniendo a uno el bit 10 causa que el procesador ponga las direcciones de broadcast todo a ceros; poniendo a cero el bit 10 (valor por defecto) causa que el procesador los ponga todo a unos. El bit 10 interactúa con el bit 14 para fijar los números de red y subred a unos o a ceros.

Bit 10	Bit 14	Address (<net> <host>)
Off	Off	<ones> <ones>
On	Off	<zeros> <zeros>
On	On	<net> <zeros>
Off	On	<net> <ones>

Interpretación del bit 13

El bit 13 determina la respuesta del router ante fallos en el proceso de arranque. Poniendo a uno el bit 13 causa que el router intente durante 6 veces cargar la IOS antes de cargar la Rxboot.

Poniendo a cero el bit 13 causa que el router continúe indefinidamente intentando cargar un fichero de boot, por defecto va a cero.

Interpretación de los bits 5,11 y 12

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Bits 5, 11, y 12 indicar la velocidad de acceso al puerto de consola (por defecto son 9600 bps).

Velocidad de acceso mediante consola	Bit 5	Bit 12	Bit 11
115200	1	1	1
57600	1	1	0
38400	1	0	1
19200	1	0	0
9600	0	0	0
4800	0	0	1
2400	0	1	1
1200	0	1	0

A continuación se va a proceder a explicar, la secuencia de arranque de la IOS de un router Cisco, una vez se haya ejecutado el procedimiento de carga del archivo IOS, en este caso, para su posterior arranque.
Esto es importante ya que dentro del procedimiento de carga del archivo de configuración o de la IOS en equipos de interconexión de redes, poseen sus propias fases y elementos, además de compartir otras fases y elementos que son comunes entre ellos.

Secuencia de arranque de un router

Introducción.
Hay que tener en cuenta que no todos los productos del Cisco tienen los mismos componentes o mecanismos para el arranque.
Este apartado describe la secuencia de arranque típica.
La ROM del router es memoria inalterable que contiene dos programas:
–El monitor o ROMmon de la ROM - el ROMmon es una imagen de diagnóstico que provee al usuario de un subconjunto limitado de comandos. Este modo de diagnóstico se utiliza normalmente durante procedimientos de recuperación (para recuperación de password o cuando la imagen de la IOS se corrompe o no existe). Es posible modificar el registro de configuración para acceder a este modo.
–La imagen (RxBoot) o boot helper image- subconjunto de la IOS que es llamado también System Bootstrap Image que permite realizar la mayoría de las funciones que posee la IOS como configuración de interfaces, visualizar la configuración pero no posee funciones de routing. En los equipos de gama baja se guarda en esta memoria pero en los de gama alta se guarda en una memoria independiente llamada bootflash.
La imagen IOS del sistema se almacena en la memoria flash en placa o en una tarjeta PCMCIA.
ROMmon toma el control del procesador principal y realiza lo siguiente:
–Si el campo de boot del registro de configuración es 0x0, el sistema no arranca la IOS y espera la intervención manual del usuario mediante la herramienta ROM Monitor.
–Si el campo de boot del registro de configuración es 0x1, el ROM monitor arranca la boot helper image.
RxBoot analiza el hardware.
Dependiendo de los bits de arranque del registro de configuración, el router se queda en RxBoot, o busca la imagen del sistema IOS del Cisco la que existe por defecto (la primera que se encuentre en la flash) o la definida en la configuración del equipo mediante el comando boot system.
Esta imagen principal del software del IOS del Cisco vuelve a chequear el hardware.
En el fichero de configuración (startup-config) almacenado en la NVRAM puede que tenga el siguiente comando:
Boot system flash slot0:c1600-sy-l.122-1a.bin
Esto fuerza el RxBoot a buscar el archivo “c1600-sy-l.122-1a.bin” el dispositivo de la flash llamado “slot 0:”.
Si no hay file system configurado, y si el registro de la configuración está en su valor por defecto, la RxBoot intenta cargar el primer fichero que se encuentra en su flash.
Si eso falla, intenta entrar en ROM Monitor.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

El software del IOS del Cisco crea ciertas estructuras como bloques descriptores de interfaz (IDBs) en la memoria principal del procesador según el nº de interfaces y subinterfaces que detecte, reserva memoria para los buffers de datos y los coloca en la memoria de entrada-salida (I/O), por último carga la configuración startup-config.
RxBoot también realiza estas funciones, pero no vuelve a chequear el hardware a menos que se ejecute el software completo del IOS del Cisco.

5.2.1. Carga mediante ficheros

Carga mediante ficheros de configuraciones e ios.

Introducción.
A continuación se comentan las operaciones básicas para el almacenamiento de configuraciones e IOS, principalmente como sistema de backup antes posibles degradaciones en los routers.
Las configuraciones se deben almacenar en archivos de texto planos, sin ningún tipo de carácter especial.
Las versiones de IOS son sistemas operativos, con una filosofía bastante parecida al UNIX, con varios procesos ejecutándose simultáneamente.
El proceso de almacenaje de la configuración en un servidor TFTP deben darse los siguientes requisitos.
–Debe de haber alguna máquina, en la cual se pueda instalar un servidor TFTP.
–Una vez activado el servicio tftp, se crea un fichero con permisos de lectura y escritura en el que salvar la configuración. Este archivo se creará en el directorio /tftpboot que se crea al activar el servidor tftp.
Se recomienda nombrar al fichero con un nombre específico que identifique al router, por ejemplo, que aparezca en el nombre del fichero el hostname del router, IP de la LAN, NRI, etc.
–El último requisito fundamental es que exista conectividad UDP / IP, entre el router y el servidor TFTP.
A continuación se muestran los pasos a seguir una vez comprobado los requisitos anteriores.
3.Accedemos al router que queramos guardar la configuración vía telnet.
4.Mediante tftp, transferimos al servidor la configuración almacenada en el router, ya sea la de la RAM (configuración que realmente está corriendo en el router), o la de la NVRAM (configuración que se carga en la RAM al arrancar el equipo).
Habitualmente estas dos configuraciones coinciden. Los comandos respectivos a utilizar son:
›copy running-configuration tftp
›copy startup-configuration tftp
Una vez ejecutado uno de estos comandos, el router va solicitando datos necesarios para realizar la transferencia, concretamente, la dirección IP del servidor tftp, y el nombre del fichero en el que almacenar la configuración.
Remote host []? 172.24.96.177
Name of configuration file to write [router-confg]? configuration.cfg
Write file router on host 172.24.96.177? [confirm]
Building configuration...
Writing router
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Como último paso puede ser conveniente cambiar el fichero de directorio, y realizar copias de backup periódicamente de estos ficheros.
Al igual que se puede copiar a un servidor tftp, se pueden realizar múltiples combinaciones, de la RAM a la NVRAM, de tftp a la NVRAM, etc.
Por ejemplo en un modelo 3620 se pueden hacer las siguientes combinaciones.
router1#copy ?
/erase Erase destination file system.
flash: Copy from flash: file system
ftp: Copy from ftp: file system
null: Copy from null: file system
nvram: Copy from nvram: file system
rcp: Copy from rcp: file system
running-config Copy from current system configuration
slot0: Copy from slot0: file system

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

slot1: Copy from slot1: file system
startup-config Copy from startup configuration
system: Copy from system: file system
tftp: Copy from tftp: file system
xmodem: Copy from xmodem: file system
ymodem: Copy from ymodem: file system
router1#copy running-config ?
flash: Copy to flash: file system
ftp: Copy to ftp: file system
lex: Copy to lex: file system
null: Copy to null: file system
nvram: Copy to nvram: file system
rcp: Copy to rcp: file system
running-config Update (merge with) current system configuration
startup-config Copy to startup configuration
system: Copy to system: file system
tftp: Copy to tftp: file system

Carga del fichero iOS

Para el cambio de IOS en un router hay dos posibilidades, una primera y simple, insertar un módulo nuevo de memoria FLASH en el router con la nueva versión de IOS, y una segunda, telecargársela, si es que dispone de la suficiente memoria FLASH libre para acogerla.

A partir de la diferenciación anterior, y centrándose en la opción de la telecarga, también aquí hay que hacer una diferenciación, que es si el router es de gama baja (series 1600 y 2500) o superior.

Esta diferencia es debido a que los routers de la serie 1600 y 2500 trabaja directamente la IOS en la FLASH, y los demás, en la FLASH almacenan una IOS en un fichero comprimido, que al arrancar el router, se descomprime en la memoria RAM, ejecutándose desde la RAM.

Telecarga serie 1600 y 2500.

Al trabajar la IOS directamente sobre la FLASH, y al tener que poner la FLASH en modo lectura-escritura, no se puede utilizar esta IOS, y se recurre a la versión resumida, llamada RXBOOT, contenida en ROM.

Esta versión básica no dispone de ciertas funcionalidades, algunas de ellas necesarias para el funcionamiento normal del router, como por ejemplo, no entiende de routing, algunos comandos de frame-relay como el lmi-type q933a, que nos va a hacer configurar el router de manera especial antes de la telecarga.

También hay que tener en cuenta que el proceso de la telecarga de estos routers es muy crítico, ya que podemos perder la gestión remota de los equipos.

También recordar que la transferencia de estos archivos debe ser en modo binario, y una forma fácil de comprobar que se ha realizado con éxito es que el tamaño del archivo en origen y destino es idéntico.

Los pasos a seguir para la telecarga se indican a continuación.

–Situar en el servidor tftp la IOS a cargar con todos los permisos de lectura y escritura.

Si el servidor está alojado en una máquina UNIX, se debe alojar el fichero en el directorio /tftpboot.

–Cargar en la NVRAM una configuración especialmente preparada para realizar esta carga, una configuración que soluciona los problemas inicialmente descritos de pérdidas de funcionalidades con la RXBOOT.

Para solucionar el problema de la carencia de routing hay que mapear la dirección IP del servidor tftp, otra solución para este problema de carencia de routing es usar el comando ip default-gateway; sin embargo, algunas versiones de RXBOOT no admiten este comando, por lo que en la configuración básica para la NVRAM se incluyen ambas opciones.

Para solucionar el problema del lmi hay que usar el comando frame-relay lmi-type ccitt en vez del comando frame-relay lmi-type q933a.

Un ejemplo de esta configuración básica está guardado en el router de gestión interlan1 en /tftpboot y su nombre es remoto.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Un ejemplo de configuración para la telecarga de un router, podría ser:

```
no service udp-small-servers
no service tcp-small-servers
!
hostname remoto
!
enable secret cisco
enable password cisco
!
interface Serial0
no shutdown
ip address x.x.x.x z.z.z.z
encapsulation frame-relay IETF
frame-relay lmi-type ccitt
frame-relay map ip 172.24.96.177 1006 broadcast
frame-relay map ip y.y.y.y 1006 broadcast
ip default-gateway y.y.y.y
!
ip route 172.24.96.0 255.255.255.0 y.y.y.y
!
line con 0
password cisco
login
!
line aux 0
password cisco
login
!
line vty 0 4
password cisco
login
```

La dirección IP 172.24.96.177 es la del servidor tftp remoto, x.x.x.x z.z.z.z es la IP y máscara del subinterface que se conecta con el Nodo de Concentración de Red.

La dirección IP y.y.y.y es la del router directamente enfrentado.

Resumiendo, con el mapeo, también con el ip default-gateway, indicamos como llegar desde el router remoto al servidor tftp y al gateway por defecto.

–Cambiar el registro de configuración por el 0x2101, que indica que arranque desde la RXBOOT.

config-register 0x2101

–Reiniciar el router.

–Entrar en el router arrancado en modo boot y ejecutar el comando copy tftp flash y seguir las instrucciones del router; en caso de que no haya suficiente espacio en la FLASH habrá que borrar la anterior versión de IOS (erase flash).

–Una vez terminado el proceso, verificar que el tamaño de fichero origen es igual al destino almacenado en flash.

–Cambiar el registro de configuración a 0x2102.

config-register 0x2102

–Copiar en NVRAM la configuración original del router.

–Reiniciar el router.

Como última nota, indicar que como servidor tftp puede actuar otro router, simplemente habría que indicarle que actúe la FLASH como servidor, y seguir el procedimiento anteriormente descrito.

El comando necesario para indicar a un router que actúe como servidor tftp se indica a continuación.

tftp-server flash <nombre del fichero a enviar>

Telecarga modelos superiores.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Este proceso es mucho más simple, solo hay que ejecutar el comando copy tftp flash, y seguir las instrucciones que indica el router.
El diálogo con el router se muestra a continuación.
ROUTER#copy tftp flash
System flash directory:
File Length Name/status
1 2596832 c3640-i-mz.112-16.P
[2596896 bytes used, 5791712 available, 8388608 total]
Address or name of remote host [255.255.255.255]? <IP servidor tftp>
Source file name? <fichero origen>
Destination file name [<fichero origen>]?]
Accessing file '<fichero origen>' on 172.24.96.177...
Loading >fichero origen>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Carga de ficheros desde diferentes dispositivos.

A continuación, se va a presentar la carga de ficheros desde diferentes dispositivos, con el objetivo de tener un conocimiento más profundo sobre la carga ficheros o imágenes IOS, desde otros dispositivos, como por ejemplo PCMCIA.
Utilizando el comando Show flash-filesystem, obtenemos el sistema de ficheros que se encuentra en el slot correspondiente, siempre y cuando la PCMCIA, se encuentre en el slot correspondiente.
Si la PCMCIA está en formato ATA, la nomenclatura a utilizar cambia de slot a disk.
show flash-file system: [partition number] [all | chips | detailed | err | summary]
Siendo el flash-file system el dispositivo flash, slot0 o slot1 si la PCMCIA se encuentra en el slot correspondiente o disk0, disk1 si la PCMCIA es de formato ATA con mayor capacidad que las estándar.
También se puede utilizar el comando dir para conocer el número de ficheros en ese dispositivo.
Ejemplos:
Router# show slot1:
PCMCIA Slot1 flash directory, partition 1:
File Length Name/status
1 1933052 c3640-i-mz.111-6.3.AA
[1933116 bytes used, 6455492 available, 8388608 total]
8192K bytes of processor board PCMCIA Slot1 flash (Read/Write)
PCMCIA Slot1 flash directory, partition 2:
File Length Name/status
1 3399444 c3640-j-mz.111-7.AA
[3399508 bytes used, 794796 available, 4194304 total]
4096K bytes of processor board PCMCIA Slot1 flash (Read/Write)
PCMCIA Slot1 flash directory, partition 3:
File Length Name/status
1 2359 running-config
[2424 bytes used, 4191880 available, 4194304 total]
4096K bytes of processor board PCMCIA Slot1 flash (Read/Write)
show flash:
De forma similar puedes ver el contenido de la flash que se encuentra en placa con el comando:
copy flash:[filename] {slot0: | slot1:}[filename]
Copiando un fichero desde la memoria flash en placa a una PCMCIA
–Paso 1
Entra en modo enable
Router> enable
Password: <password>
Router#
–Paso 2

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

copy flash:[filename] {slot0: | slot1:}[filename]
Router# copy flash:TESTFILE slot0:TESTFILE
PCMCIA Slot0 flash directory,
No files in PCMCIA Slot0 flash
[0 bytes used, 4194304 available, 4194304 total]
Verifying checksum for 'TESTFILE' (file # 1)... OK
Erase flash device before writing? [confirm] n
–Paso 3
Presiona Return o teclea y para borrar el contenido de la flash.
Copy 'TESTFILE' from flash: device
as 'TESTFILE' into slot0: device WITHOUT erase? [yes/no] y
!
[OK - 68/4194304 bytes]
Flash device copy took 00:00:05 [hh:mm:ss]
Verifying checksum... OK (0x4ACD)
Copiar una Running Configuration File a una Flash Memory Card
Paso 1 Entra en modo enable
Paso 2 Teclea
copy running-config {slot0: | slot1:}[partition:filename]
Router# copy running-config slot 0: miconfiguración
PCMCIA Slot0 flash directory, partition 3:
File Length Name/status
1 68 TESTFILE
[132 bytes used, 4194172 available, 4194304 total]
Building configuration...
Erase flash device before writing? [confirm] n
–Paso 4:
Presiona Return o teclea y para borrar el contenido de la flash o n para no hacerlo
Copy 'running-config'
as 'myconfig' into flash device WITHOUT erase? [yes/no] y
!
[OK - 922/4194172 bytes]
Verifying checksum... OK (0xC4D4)
Flash device copy took 00:00:00 [hh:mm:ss]
Router#

Copiando un fichero entre slots

–Paso 1 entra en modo enable.
–Paso 2 Inserte la PCMCIA con el fichero que desea copiar en el slot etiquetado con 0.
–Paso 3 Inserte una segunda PCMCIA en el slot 1.
–Paso 4 Teclee copy {slot 0: | slot1:}[partition:filename]{slot 0: | slot 1:} [partition:filename]
Nomenclatura de simbolos que aparecen mientras una copia entre
dispositivos
Durante una copia se pueden obtener los siguientes caracteres:
(#) significa que la flash está siendo transmitida.
Una exclamación (!) significa que 10 paquetes han sido transferidos correctamente.
Un conjunto de caracteres "V" significa se está realizando la verificación del checksum del fichero copiado.
Una "O" significa un paquete fuera de orden.
Un periodo de (.) significa un timeout.
La última línea indica si el fichero se ha copiado de forma satisfactoria.
Para interrumpir la copia pulsa Ctrl-^ or Ctrl-Shift-6.
La operación termina pero parte del fichero que se ha copiado continúa en la memoria flash hasta que sea
borrado.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

5.2.2. Modificación de parámetros

La modificación de parámetros, son uno de los procedimientos, donde se requiere mayor conocimiento por parte del operador o técnico que realice dichos cambios.
El conocimiento profundo sobre las posibilidades que ofrece las modificaciones de parámetros de registro de configuración, es esencial, para evitar un arranque fallido del router o mayor aún, perder la conectividad en remoto de dicho equipo. Cuando se está modificando parámetros de los ficheros de configuración, de la IOS, o del propio registro, normalmente lo básico se realiza localmente por consola.
A veces, ciertas configuraciones complejas en redes en entorno operador, y bajo petición del cliente, requiere de modificaciones en remoto, carga del archivo de configuración y salvado del mismo.
Este proceso, se debe de extremar las precauciones, ya que se incurriría en un desastre de gran magnitud, para el servicio en sí, y para el soporte en remoto que se está ofreciendo.
Por ello, a continuación, se expondrán ciertas modificaciones de parámetros, que serán necesarios conocer para su operación.
Con el comando show flash podemos ver el nombre del archivo de configuración, su tamaño y la capacidad de la memoria.
Para hacer un backup de la imagen o copiar el archivo desde un servidor sólo tendremos que usar el comando copy, en el primer caso copy flash tftp y en el segundo copy tftp flash.

Registro de configuración.

```
Router# configure terminal
Router(confiig)#config-register 0x10F
[Ctrl-Z]
```

- **Los bits 3, 2, 1 y 0 del registro de configuración selecciona la opción de arranque (boot)**

Valor del registro	Significado
0x0	Utiliza el modo monitor ROM (manualmente arranca utilizando el comando b)
0x1	Automáticamente arranca desde ROM (defecto si el router no tiene flash)
0x2 a 0xF	Examina NVRAM por comandos *boot system* (0x2 es el defecto si el router tiene flash

- **Control del registro de configuración con el comando *show version***

Sirve para indicar al router de donde debo cargar la IOS.
Aconsejable dejarlo en Valor 0x2 a 0xF puesto que en la ROM los routers suelen traer una versión de IOS de fábrica y antigua.
En cualquier caso podemos consultar su valor con el comando show recede y fijándonos en la línea Configuration register is…
Si su valor es inadecuado puede que al rebotar el router sea incapaz de encontrar una ubicación con la IOS y no arranque, no pudiendo entonces acceder al router de manera remota –telnet- y teniendo pues que enviar a un técnico para solucionar la avería.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

```
Router# configure terminal
Router(config)# boot system flash nombre-fichero_IOS
Router(config)# boot system tftp nombre-fichero_IOS dirección_tftp
Router(config)# boot system rom
Router(config)# exit
Router# copy running-config startup-config
```

Comandos "boot system" no encontrados en NVRAM

Obtiene el software IOS por defecto de la flash

Memoria flash vacía

Obtiene el IOS por defecto desde el servidor TFTP

El comando show versión nos dice también la versión de IOS y describe el hardware instalado en el router.

Configuración del password.

Password de consola

```
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password cisco
```

Password de terminal virtual

```
Router(config)#line vty 0-4
Router(config-line)#login
Router(config-line)#password cisco
```

Password de enable

```
Router(config)#enable password cisco
```

Encriptación de password

```
Router(config)#service password-encryption

Router(config)#service password-encryption
```

La validación del usuario puede realizarse también contra un servidor de TACACS – Terminal Access Controller Access Control System-, en cuyo caso cada usuario tendrá un nombre de usuario y contraseña para validarse en el router.

Para activar la utilización de tacacs en el modo enable se utiliza el comando enable use-tacacs –cuidado con poner este comando sin haber introducido con anterioridad toda la configuración correspondiente al servicio de tacacs, ya que sin ella después no podremos entrar en el router.

Con el comando enable last-resort password hacemos posible que si el interfaz por el que debiera buscar el servidor de tacacs está caído o simplemente el servidor de tacacs no responde, puede utilizar la última contraseña válida introducida, la cual tendremos configurada.

Asimismo también se puede configurar la línea vty, la consola y el puerto

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

auxiliar para que utilicen tacacs para entrar en el modo usuario.
El comando es login tacacs y debe introducirse desde el modo de configuración de línea (dentro de Router(config-line)).

Configuración de la identificación del router.

–El nombre del router se configura de la siguiente forma:
Router(config)#hostname Málaga
Málaga(config)#
–El texto que se muestra al conectarse al router se configura de la siguiente manera:
Málaga(config)#banner motd #
Bienvenido al router Málaga
#
–El texto descriptivo para una interfaz se configura de la siguiente manera:
Málaga(config)#interface ethernet 0
Router(config-if)#description Red local

Configuración horaria del router.

La forma más sencilla de configurar la hora en un router cisco es con el comando “clock set HH:MM:SS Dia Mes Año”.
Igualmente para visualizarla debemos teclear el comando show clock.
Es esencial para los debugs y el archivo de log una correcta configuración horaria.
Otro método es utilizar servidores de SNTP –Simple Network Time Protocol-, con los cuales se centraliza la gestión horaria de todos los routers de una red.
El comando es tan sencillo como “sntp server Dir IP”; si hacemos un ping desde el router hasta el servidor SNTP y responde la configuración de hora y fecha se pondrá a hora automáticamente.
–Clock timezone MET 1
Utilizado para especificar la zona horaria con respecto a la hora universal.
Únicamente tiene sentido cuando la configuración del reloj es manual.
–clock summer-time DST recurring last Sun Mar 2:00 last Sun Oct 2:00
Configura la hora para que cambie automáticamente con el horario de verano.

Configuración del archivo de log.

Los routers Cisco guardan un registro, por defecto, de eventos.
En él se registran por ejemplo las caídas de interfaz o cuando se ha configurado el router.
También podemos activar ‘debugs’ de parámetros concretos para monitorizar o analizar alguna incidencia de forma que queden reflejados en el fichero de log.
Los debugs son las líneas que se guardan en el fichero log.
Además los debugs pueden ser visualizados en el instante en que ocurren si se activa en el router.
Los siguientes comandos son de uso habitual:
–service timestamps debug datetime localtime show-timezone
Consigue que en cada debug veamos la fecha y hora acorde con la configuración horaria del router.
–service timestamps log datetime localtime show-timezone
Consigue que en cada línea del log veamos la fecha y hora acorde con la configuración horaria del router.
–logging buffered 4096 debugging
Establece el tamaño máximo del archivo de log.
Preceden para activar un debug concreto podemos teclear “debug” y nos aparecerá toda la lista de debugs posibles.
Para desactivar todos los debugs –es conveniente hacerlo puesto que consumen tiempo de procesador y recursos del router-, se utiliza el comando “undebug all”.
Para visualizar el contenido del archivo de log se utiliza el comando show logging.

5.2.3. Actualización de firmware

Procedimiento de upgrade del firmware (ios) de un router cisco.
Introducción.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Instala un servidor TFTP en la máquina donde vayas a instalar el software y cópiala al directorio "C:\tftp" para Windows o al /tftpboot para Unix o Linux.
NOTA: (Antes debes verificar si para esa nueva IOS cumples los requisitos de memoria y flash).
Ejemplo:
Router#copy flash tftp
Source filename []? C7200-js-mz.120-4.bin --à Nombre de la imagen a cargar
Address or name of remote host []?164.100.9.31 --à Ip servidor TFTP
Destination filename [C7200-js-mz.120-4.bin]?
!!
!!
!!
!!!!!!!!!!!!!!!!!!!!!!!!!
3802992 bytes copied in 27.276 secs (140851 bytes/sec)
Copia el fichero de imagen desde el servidor tftp a la memoria flash utilizando:
Ejemplo:
Router# copy tftp flash
When prompted, enter the IP address of the TFTP server as
Address or name of remote host [255.255.255.255]? 164.100.21.131
Source file name? c2600-io3s56i-mz.121-6
Destination file name? c2600-io3s56i-mz.121-6
Erase flash device before writing? [confirm] yes/no
Router#reload
*Mar 1 00:30:49.972: %SYS-5-CONFIG_I:
Configured from console by console
System configuration has been modified. Save?
[yes/no]: no Proceed with reload? [confirm] yes

5.2.4. Conexiones locales y remotas para configuración

Se pueden recordar las 5 formas de acceder al router desde dispositivos externos en esta misma unidad didáctica, en el epígrafe 5.2. Procedimientos de carga de configuración en dispositivos de interconexión de redes.

5.3. Procedimientos de verificación de los servicios de comunicación

En este apartado, se va a establecer las diferentes herramientas disponibles de troubleshooting para verificación de los diferentes servicios de comunicación en equipos de interconexión de redes.
A través de los comandos show, se establece una serie de procedimientos que podemos verificar todos los servicios de comunicación establecidos en los equipos de interconexión de redes, desde interfaces ethernet, pasando por líneas seriales, BRI, frame Relay, ISDN y PPP.
Show version
router# sh ver
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-Y-M), Version 12.2(4)YB, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
Synched to technology version 12.2(6.8)T2
TAC Support: http://www.cisco.com/tac
System type (Nombre de la imagen) Versión major.minor(relase.interim)[who]Desc
–Nombre de la imagen (C1700-Y-M): El nombre de la imagen es diferente para equipos run from flash y run from ram.
–Versión: El texto que hay detrás de esta palabra cambia cada vez que se modifica la IOS en el router.
·Major: Número de versión Major. Cambia (en teoría) cuando se han añadido al software nuevas características.
·Minor: minor versión number. Menor número de cambios pero significativos, (en realidad Cisco no está muy seguro de la diferencia entre major y minor, pero un incremento indica que se han añadido nuevas características.
–Release: incrementa (1, 2,3...) por cada revisión de la release o por cada nueva compilación.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

–Interim: incrementa por cada construcción del “release tree”, que ocurre semanalmente aunque generalmente es cada 7 u 8 semanas.
–[who]: Indica quién la construyó. Tiene el valor de “fc1” o similar para software release y para los software test aparece algo como [billw 101].
–Desc: Descripción adicional. En este caso indica la compatibilidad con versiones de IOS y el contacto del soporte técnico.
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Fri 15-Mar-02 20:32 by ealyon
Image text-base: 0x80008124, data-base: 0x807D8744
–Copyright, fecha de compilación (y quién la hizo), además de la dirección de comienzo de la imagen.
·ROM: System Bootstrap, Version 12.2(4r)XL, RELEASE
SOFTWARE (fc1)
·ROM: C1700 Software (C1700-Y-M)
·ROM: C1700 Software (C1700-Y-M), Version 12.2(4)YB, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
–Versión de ROM bootstrap y la imagen Rxboot que en este caso está almacenada en memoria ROM.
·R17O1141 uptime is 1 week, 6 days, 19 hours, 24 minutes
·System returned to ROM by power-on
–Cuánto tiempo lleva activo el router desde que se reseteó.
·System image file is “flash:c1700-y-mz.122-4.YB.bin”
–Desde qué dispositivo se arrancó la imagen de sistema.
·cisco 1760 (MPC860P) processor (revision 0x200) with 29492K/3276K bytes of memory.
·Processor board ID FOC06330HE1 (4055339560), with hardware revision BB67
·MPC860P processor: part number 5, mask 2
–Tipo de procesador y tamaño de la memoria DRAM.
·Bridging software.
·X.25 software, Version 3.0.0.
·Basic Rate ISDN software, Version 1.1.
–Diferentes opciones de software que han sido compiladas.
·1 FastEthernet/IEEE 802.3 interface(s)
·1 Serial(sync/async) network interface(s)
·1 ISDN Basic Rate interface(s)
–Configuración de hardware.
·32K bytes of non-volatile configuration memory.
·16384K bytes of processor board System flash (Read/Write)
–Tamaño de las memorias NVRAM y Flash.
·Configuration register is 0x2102
–El ultimo valor del registro de configuración tras resetear el router.
·Show flash
·router#show flash
·System flash directory:
·File Length Name/status
· 1 4253624 c1700-y-mz.122-4.YB.bin
·[4253688 bytes used, 12523528 available, 16777216 total]
·16384K bytes of processor board System flash (Read/Write)
–Muestra información sobre el tamaño de la memoria Flash y cada uno de los archivos que contiene. Para cada archivo indica el tipo (1 significa que es un archivo de configuración) el tamaño en bytes que ocupa (length) y el nombre del archivo.
Show diag
router# show diag
Slot 0:
C1760 1FE VE 4SLOT DV Mainboard Port adapter, 3 ports
Port adapter is analyzed
Port adapter insertion time unknown

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

EEPROM contents at hardware discovery:
Hardware Revision : 2.0
PCB Serial Number : FOC06330HE1
Part Number : 73-7167-02
Board Revision : C0
Deviation Number : 0-47975
Fab Version : 04
EEPROM format version 4
EEPROM contents (hex):
0x00: 04 FF 40 03 16 41 02 00 C1 8B 46 4F 43 30 36 33
0x10: 33 30 48 45 31 82 49 1B FF 02 42 43 30 80 00 00
0x20: BB 67 02 04 FF FF FF FF FF FF FF FF FF FF FF FF
0x30: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x40: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
–WIC Slot 0:
Serial 1T
Hardware revision 1.0 Board revision M0
Serial number 0028872490 Part number 800-01514-01
Test history 0x00 RMA number 00-00-00
Connector type WAN Module
EEPROM format version 1
EEPROM contents (hex):
0x20: 01 02 01 00 01 B8 8F 2A 50 05 EA 01 00 00 00 00
0x30: B0 00 00 00 02 08 13 01 FF FF FF FF FF FF FF FF
–WIC Slot 1:
BRI S/T – 2186
Hardware revision 1.3 Board revision B0
Serial number 0028777053 Part number 800-01833-04
Test history 0x00 RMA number 00-00-00
Connector type WAN Module
EEPROM format version 1
EEPROM contents (hex):
0x20: 01 07 01 03 01 B7 1A 5D 50 07 29 04 00 00 00 00
0x30: 58 00 00 00 02 08 20 01 FF FF FF FF FF FF FF FF

Este comando sirve para determinar el tipo de hardware instalado en el router.

Muestra el número de serie y el part-number de cada módulo hardware (estos números identifican de forma exclusiva cada componente hardware), el tipo de módulo (wan, para tarjetas Wic) y la información que se almacena en la memoria EEPROM respectivamente.

–Show arp

router# show arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.202.24.220 6 0000.e229.afaa ARPA FastEthernet0/0
Internet 10.202.24.221 10 0004.759f.362d ARPA FastEthernet0/0
Internet 10.202.24.253 59 000a.8a13.6a40 ARPA FastEthernet0/0
Internet 10.202.24.254 - 0007.8580.997c ARPA FastEthernet0/0
Internet 10.202.24.240 9 0002.b3b4.7780 ARPA FastEthernet0/0

Este comando muestra la tabla ARP del router y es útil para determinar los dispositivos vecinos en la LAN a la que está conectado.

La tabla refleja la relación entre las direcciones IP y las direcciones MAC así como el tiempo transcurrido (en minutos) desde que se eliminó la correspondiente entrada en la tabla.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Para actualizar la tabla Arp, se usa el comando clear arp.
–Show ip interface brief
router#show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 10.202.24.254 YES TFTP up up
Serial0/0 unassigned YES TFTP up up
Serial0/0.16 10.202.254.24 YES TFTP up up
Serial0/0.17 10.200.2.24 YES TFTP up up
BRI1/0 unassigned YES TFTP up up
BRI1/0:1 unassigned YES unset down down
BRI1/0:2 unassigned YES unset down down
Dialer1 10.202.124.254 YES unset up up
Loopback0 10.202.124.254 YES TFTP up up
Este comando muestra la información resumida sobre los interfaces configurados, indicando para cada uno la dirección ip asignada (en caso de que la tenga) ,el estado ('up' significa que el interfaz a nivel hardware está operativo) y la actividad a nivel de protocolo, es decir si el interfaz está en condiciones de poder ofrecer comunicación en ambos sentidos.
–Show interface fastethernet
router#show interface FastEthernet0/0
FastEthernet0/0 is up, line protocol is up
Hardware is PQUICC_FEC, address is 0007.8580.997c (bia 0007.8580.997c)
Description: LETO1141
Internet address is 10.202.24.254/24
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:01, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 4000 bits/sec, 2 packets/sec
5 minute output rate 7000 bits/sec, 3 packets/sec
1100783 packets input, 175541666 bytes
Received 108500 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog
0 input packets with dribble condition detected
1196899 packets output, 484531457 bytes, 0 underruns
11 output errors, 0 collisions, 7 interface resets
0 babbles, 0 late collision, 0 deferred
11 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Entrada	Descripción
Fast Ethernet0 is ... is up ...is administratively down	Indica si el interface a nivel hardware está operativo o si ha sido bloqueado por un administrador
line protocol is	Indica si el proceso software que maneja el protocolo de la línea considera si ésta en condiciones de ser usada.
Hardware	Tipo de hardware y dirección MAC.
Internet address	Dirección ip de Internet y mascara.
MTU	Tamaño de MTU (Maximum Transmission Unit of the interface)
BW	Ancho de banda del interfaz en Kbps.
DLY	Retraso del interfaz en microsegundos.
rely	Fiabilidad del interfaz expresada como fracción de 255 (255/255 significa un 100% de fiabilidad)
load	Carga del interfaz expresada como fracción de 255 (255/255 significa que el interfaz está totalmente saturado)
Encapsulation	Método de encapsulación asignado al interfaz.
ARP type:	Tipo de protocolo de resolución de dirección asignado.
loopback	Indica si hay o no loopback.
keepalive	Indica si se envían o no keepalives (en caso afirmativo se indica el tiempo)
Full/Half duplex	Indica el modo de transmisión, velocidad y tecnología
Last input	Número de horas, minutos y segundos transcurridos desde la recepción del último paquete en el interfaz y procesado localmente en el router. Este comando es útil para saber cuándo un interfaz ha fallado. NOTA: Este campo no se actualiza para el tráfico conmutado en fast switching.
output	Número de horas, minutos y segundos transcurridos desde el envío del último paquete a través del interfaz
output hang	Número de horas, minutos y segundos (o nada) desde que el interfaz ha sido finalmente reseteado debido a una transmisión demasiado larga. Cuando el número de horas en los campos anteriores excede las 24, se muestra el número de días y horas.
Last clearing	Tiempo transcurrido desde el último reseteo de contadores 0:00:00 indica que los contadores han sido reseteados hace más de 2^{31} ms y menos de 2^{32} ms
Output queue, input queue, drops	Número de paquetes en las colas de entrada y salida, seguido (y separados mediante barras) del tamaño máximo de la cola, el número de paquetes descartados debido a que la cola está llena y el número de veces que se ha limpiado la cola.
5 minute input rate, 5 minute output rate	Número medio de bits y paquetes recibidos y transmitidos por segundo
packets input	Número total de paquetes recibidos sin errores
bytes	Número total de bytes recibidos sin error (incluyendo datos y encapsulación MAC) Total number of bytes, including data and MAC encapsulation, in the error free packets received by the system.
Received ... broadcasts	Número total de paquetes broadcast recibidos

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

runts	Número de paquetes que han sido descartados debido a que su tamaño es inferior al tamaño mínimo medio. Por ejemplo, cualquier paquete ethernet cuyo tamaño sea inferior a 64 bytes es considerado como runt
giants	Número de paquetes que han sido descartados debido a que su tamaño es superior al tamaño máximo medio. Por ejemplo, un cualquier paquete ethernet cuyo tamaño sea superior a 1518 bytes es considerado como runt.
input errors	Incluye además los errores registrados en los contadores de runts, giants, no buffer, CRC, frame, overrun e ignored otros tipos no especificados. Además, hay que tener en cuenta que un paquete pude producir más de un error por lo que el valor de este contador no es un sumatorio del valor de los contadores anteriores
CRC	Código de redundancia cíclica, generado por la estación LAN origen y recalculado por la estación destino. Si ambos valores no coinciden, es señal de que existe ruido en la LAN o de que hay problemas de transmisión en el interfaz. Un número elevado de errores de CRC, pueden ser resultado de colisiones o de que una estación este enviando datos de forma errónea...
frame	Número de paquetes recibidos de forma incorrecta (errores de CRC o porque contienen un número no entero de octetos). Normalmente es el resultado de colisiones o de un funcionamiento incorrecto del dispositivo Ethernet.
overrun	Número de veces que el dispositivo hardware es incapaz de manejar los datos del buffer de entrada debido a que la velocidad de entrada excede la capacidad del dispositivo para manejar los datos.
ignored	Número de paquetes ignorados por el interfaz. Tormentas de broadcast y picos de ruido pueden provocar que este contador aumente.
watchdog	Número de veces que se recibe un paquete con longitud superior a 2048.
multicast	Número de paquetes multicast recibidos.
input packets with dribble condition detected	Indica que se ha recibido una trama que es sensiblemente larga. Este contador tiene un propósito informativo ya que la trama es aceptada.
packets output	Número total de mensajes transmitidos por el sistema.
bytes	Número total de bytes, incluidos datos y encapsulación MAC, transmitidos por el sistema.
underruns	Número de veces que el emisor ha transmitido más deprisa que la velocidad que puede manejar el router. En algunos interfaces esto nunca sucede.
output errors	Sumatorio de todos los errores que impiden la transmisión final de un datagrama a través del interfaz que está siendo contemplado. Hay que tener en cuenta que un mismo datagrama puede tener más de un error y que pueden existir errores fuera de los que se contemplan en los contadores estándar.
collisions	Número de mensajes retransmitidos debido a una colisión en la Ethernet. Generalmente es consecuencia de una lan sobredimensionada (cable demasiado largo, más de dos repetidores entre estaciones
interface resets	Número de veces que un interfaz ha sido completamente reseteado. Esto puede ocurrir cuando los paquetes que están encolados para ser transmitidos no son enviados transcurridos bastantes segundos. En una línea serie, esto puede estar causado por un funcionamiento incorrecto del módem que no está proporcionando correctamente la señal de reloj o por un problema de cable. Si el sistema detecta que la línea de detección de portadora está up, pero el protocolo está down, periódicamente resetea el interfaz en un intento de restablecerlo. Los reseteos del interfaz, también se producen cuando éste pasa a estar en shut down.
late collision	Número de late collisions. Se llaman late collisions a las colisiones que se producen después de haberse transmitido el preámbulo de la trama
deferred	Número de deferred collisions. Cuenta el número de veces que el interfaz ha intentado enviar una trama, pero se encuentra con la portadora ocupada. Esto no supone un problema y es algo normal en el comportamiento ethernet.
lost carrier	Número de veces que se ha perdido la portadora durante una transmisión
no carrier	Número de veces que la portadora no está presente durante una transmisión
output buffer failures	Número de fallos en los buffers de salida y veces que se ha realizado un swap out de los buffers.

–Show interface serial0/0

router# sh int ser0/0

Serial0/0 is up, line protocol is up

Hardware is PowerQUICC Serial

Description: LFRO1141

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation FRAME-RELAY IETF, loopback not set
Keepalive set (10 sec)
LMI enq sent 119296, LMI stat recvd 119297, LMI upd recvd 0, DTE LMI up
LMI enq recvd 0, LMI stat sent 0, LMI upd sent 0
LMI DLCI 0 LMI type is CCITT frame relay DTE
Broadcast queue 0/64, broadcasts sent/dropped 148840/0, interface broadcasts 128963
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters 1w6d
Input queue: 1/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/9/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1158 kilobits/sec
5 minute input rate 7000 bits/sec, 5 packets/sec
5 minute output rate 5000 bits/sec, 5 packets/sec
1323997 packets input, 474880503 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
3 input errors, 2 CRC, 1 frame, 0 overrun, 0 ignored, 0 abort
1360356 packets output, 185368155 bytes, 0 underruns
0 output errors, 0 collisions, 4 interface resets
0 output buffer failures, 0 output buffers swapped out
2 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
Serial0/0.16 is up, line protocol is up
Hardware is PowerQUICC Serial
Internet address is 10.202.254.24/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation FRAME-RELAY IETF
Serial0/0.17 is up, line protocol is up
Hardware is PowerQUICC Serial
Internet address is 10.200.2.24/22
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation FRAME-RELAY IETF

–La mayoría de las entradas para el interfaz serie son similares a las del interfaz Fastethernet por lo que no se van a volver a describir.
Pueden aparecer entradas diferentes pero son de fácil deducción.
En el ejemplo expuesto, también se facilita información para cada uno de los dlci's configurados sobre el interfaz.
DCD-Data Carrier Detect
DSR-Data Send Ready
DTR-Data Terminal Ready
RTSàRequest To Send
CTS- Clear To Send:
Show interface BRI1/0
router# sh int BRI1/0
BRI1/0 is up (spoofing), line protocol is up (spoofing)
Hardware is PQUICC BRI

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Description: RDSO1141
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set
Last input 1w6d, output never, output hang never
Last clearing of “show interface” counters 1w6d
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/1/16 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 48 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
59 packets input, 285 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
59 packets output, 279 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 output buffer failures, 0 output buffers swapped out
2 carrier transitions
BRI1/0:1 is down, line protocol is down
Hardware is PQUICC BRI
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set
LCP Closed
Closed: BRIDGECP, IPCP, CCP, CDPCP, LLC2, BACP
Last input 1w6d, output 1w6d, output hang never
Last clearing of “show interface” counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/0/16 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 48 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
335 packets input, 15014 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
161 packets output, 12051 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
2 carrier transitions
BRI1/0:2 is down, line protocol is down
Hardware is PQUICC BRI
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set
LCP Closed
Closed: BRIDGECP, IPCP, CCP, CDPCP, LLC2, BACP
Last input never, output never, output hang never

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Last clearing of “show interface” counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/0/16 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 48 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
Dialer1 is up (spoofing), line protocol is up (spoofing)
Hardware is Unknown
Interface is unnumbered. Using address of Loopback0 (10.202.124.254)
MTU 1500 bytes, BW 56 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set
DTR is pulsed for 1 seconds on reset
Last input never, output never, output hang never
Last clearing of “show interface” counters 1w6d
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/1/16 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 42 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
327 packets input, 14844 bytes
153 packets output, 11887 bytes
–Como sucede con el comando anterior, los valores de los campos son similares.
En este caso se muestra además la información relativa a cada uno de los canales B y si existen, también sobre los interfaces Dialer configurados.
Show frame-relay pvc
router# sh fr pvc
PVC Statistics for interface Serial0/0 (Frame Relay DTE)
Active Inactive Deleted Static
Local 2 0 0 0
Switched 0 0 0 0
Unused 0 0 0 0
DLCI = 16, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0.16
input pkts 59914 output pkts 64511 in bytes 3347218
out bytes 4904232 dropped pkts 0 in FECN pkts 0
in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
in DE pkts 0 out DE pkts 0
out bcast pkts 64511 out bcast bytes 4904232
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

pvc create time 1w6d, last time pvc status changed 1w6d
DLCI = 17, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0.17
input pkts 1146754 output pkts 1178400 in bytes 470297027
out bytes 179303970 dropped pkts 0 in FECN pkts 0
in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
in DE pkts 19831 out DE pkts 0
out bcast pkts 84412 out bcast bytes 12703545
5 minute input rate 7000 bits/sec, 4 packets/sec
5 minute output rate 6000 bits/sec, 4 packets/sec
pvc create time 1w6d, last time pvc status changed 1w6d

Campo	Descripción
DLCI	Uno de los dlci (data-link connection identifier) del PVC.
DLCI USAGE	Muestra el valor SWITCHED cuando el router o el servidor de acceso se usa como un switch, o el valor LOCAL cuando el router o el servidor de acceso es utilizado como DTE
PVC STATUS	Los diferentes estados del CVP son: ACTIVE, INACTIVE, o DELETED.
INTERFACE	Especifica el subinterface asociado al DLCI
input pkts	Número de paquetes recibidos sobre el PVC.
output pkts	Número de paquetes enviados sobre el PVC
in bytes	Número de bytes recibidos sobre el PVC
out bytes	Número de bytes enviados sobre el PVC
dropped pkts	Número de paquetes (entrantes y salientes) descartados por el router
in FECN pkts	Número de paquetes recibidos con el bit FECN activado FECN (Forward Explicit Congestion Notification): Notificación de congestión en el sentido de la transmisión
in BECN pkts	Número de paquetes recibidos con el bit BECN activado BECN (Backward Explicit Congestion Notification): Notificación de congestión en el sentido contrario a la transmisión
out FECN pkts	Número de paquetes enviados con el bit FECN activado
out BECN pkts	Número de paquetes enviados con el bit BECN activado
in DE pkts	Número de paquetes recibidos con el bit DE activado DE (Discard Eligibility): Las tramas que tienen este bit a "1" son susceptibles de descarte en situaciones de congestión en la Red.
out DE pkts	Numero de paquetes enviados con el bit DE activado
out bcast pkts	Número de paquetes broadcast de salida
out bcast bytes	Número de bytes de broadcast de salida
5 minute input rate	Velocidad de entrada de datos en los últimos 5 minutos.
5 minute output rate	Velocidad de salida de datos en los últimos 5 minutos
pvc create time	Tiempo transcurrido desde que se creó el interface
last time pvc status changed	Tiempo transcurrido desde que el PVC cambió de estado por última vez (de activo a inactivo)

–Show ip route
router# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
–Gateway of last resort is 10.200.0.1 to network 0.0.0.0
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

C 10.202.254.0/24 is directly connected, Serial0/0.16
C 10.202.124.0/24 is directly connected, Loopback0
C 10.200.0.0/22 is directly connected, Serial0/0.17
C 10.202.24.0/24 is directly connected, FastEthernet0/0
R* 0.0.0.0/0 [120/1] via 10.200.0.1, 00:00:11, Serial0/0.17
Este comando muestra la tabla de routing IP. Cada entrada es una ruta aprendida.

code	Indica la forma en que se ha aprendido la ruta (los distintos valores y su código se muestran cada vez que se ejecuta el comando)
N.N.N.N/nn	Dirección y máscara destino
directly connected	Indica que la red está directamente conectada a un interfaz local
via N.N.N.N	Indica la dirección del router remoto del que se aprende la ruta

La ruta marcada con un * es la ruta por defecto.
También podemos realizar consultas más específicas.
Así podemos preguntar por una ruta en particular (pej: show ip route 0.0.0.0) o por las rutas aprendidas de una determinada forma.
A través de los comandos show, se establece una serie de procedimientos que podemos verificar todos los servicios de comunicación establecidos en los equipos de interconexión de redes, desde interfaces ethernet, pasando por líneas seriales, BRI, frame Relay, ISDN y PPP.
–Show version
router# sh ver
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-Y-M), Version 12.2(4)YB, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
Synched to technology version 12.2(6.8)T2
TAC Support: http://www.cisco.com/tac
System type (Nombre de la imagen) Versión major.minor(relase.interim)[who]Desc
·Nombre de la imagen (C1700-Y-M): El nombre de la imagen es diferente para equipos run from flash y run from ram.
·Versión: El texto que hay detrás de esta palabra cambia cada vez que se modifica la IOS en el router.
›Major: Número de versión Major. Cambia (en teoría) cuando se han añadido al software nuevas características.
›Minor: minor versión number. Menor número de cambios pero significativos, (en realidad Cisco no está muy seguro de la diferencia entre major y minor, pero un incremento indica que se han añadido nuevas características.
·Release: incrementa (1, 2, 3...) por cada revisión de la release o por cada nueva compilación.
·Interim: incrementa por cada construcción del “release tree”, que ocurre semanalmente aunque generalmente es cada 7 u 8 semanas.
·[who]: Indica quién la construyó. Tiene el valor de “fc1” o similar para software release y para los software test aparece algo como [billw 101]
·Desc: Descripción adicional. En este caso indica la compatibilidad con versiones de IOS y el contacto del soporte técnico.
(show ip route rip). Puede dares el caso de que una misma ruta se pueda aprender de varias formas, es decir que el router conoce varios caminos para llegar a un mismo destino.
En este caso puede que una ruta sea prioritaria sobre la otra (se marcaría con un * la ruta preferente) o simplemente tengan la misma prioridad en cuyo caso el router tomará una u otra sin distinción.

Show isdn active y show isdn history

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Campo	Descripción
History Table MaxLength	Número máximo de entradas que pueden ser almacenadas en la tabla
History Retain Timer	Número máximo de segundos que puede permanecer una llamada en la tabla
Call Type	Tipo de llamada (entrante o saliente)
Calling Number	Para las llamadas entrantes, el número llamante
Called Number	Para las llamadas salientes, el número llamado
Duration Seconds	Duración de la llamada hasta el momento
Remote Name	Nombre el host llamante (entrantes) o llamado (salientes)
Time until Disconnect	Número de segundos que quedan antes de que la llamada finalice (en el caso de que haya especificado un dialer idle-timeout)
Recorded Charges Units/Currency	Para llamadas salientes indica el costo de la llamada si la información se proporciona durante la llamada o al final de la llamada (esta última sólo para history) AOC (Advice Of Charge)

Router# show isdn active

ISDN ACTIVE CALLS					
History Table Max Length = 320 entries History Retain Timer = 15 Minutes					
Call Calling	Called	Duration	Remote	Time until	Recorded Charges
Type Number	Number	Seconds	Name	Disconnect	Units/Currency
Out	9876543210	Active(34)	idacom	115	5 u(D)

Este comando muestra la información relativa las llamadas en curso (para el caso de history muestra además las realizadas).

–Show isdn status

router# show isdn status
The current ISDN Switch type = basic-ni1
ISDN BRI0 interface
Layer 1 Status:
ACTIVE
Layer 2 Status:
TEI = 109, State = MULTIPLE_FRAME_ESTABLISHED
TEI = 110, State = MULTIPLE_FRAME_ESTABLISHED
Spid Status:
TEI 109, ces = 1, state = 8(established)
spid1 configured, spid1 sent, spid1 valid
Endpoint ID Info: epsf = 0, usid = 1, tid = 1
TEI 110, ces = 2, state = 8(established)
spid2 configured, spid2 sent, spid2 valid
Endpoint ID Info: epsf = 0, usid = 3, tid = 1
Layer 3 Status:
0 Active Layer 3 Call(s)
Activated dsl 0 CCBs = 0
Total Allocated ISDN CCBs = 0

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Campo	Descripción
Switchtype	
The current ISDN Switch type = basic-ni1	Tipo de acceso. El switch type ha de ser suministrado por el proveedor (en este caso se configura basic-ni1)
Layer 1 Status	
ACTIVE	Estado del livel1: Comprueba la conectividad del nivel físico. Los estados más comunes con ACTIVE o DEACTIVE. Otros estados son: GOINGDOWN INIT TESTING RESET DELEATED (sic) SHUTDOWN ACTIVATING ACTIVE_ErrorInd La mayoría de estos estados son temporales. Se puede utilizar el comando clear interface bri para resetearlos. Si estos estados se mantienen durante un tiempo prolongado, son indicadores de problemas de conexión con el proveedor del servicio
Layer 2 Status	
TEI = 109,state = MULTIPLE_FRAME_ESTABLISHED TEI = 110, state = MULTIPLE_FRAME_ESTABLISHED	Estado del nivel 2. Muestra el número de TEI (Terminal Endpoint Identifier) este número está comprendido entre 64 y 126. Los estados más comunes son MULTIPLE_FRAME_ESTABLISHED y TEI_ASSIGNED MULTIPLE_FRAME_ESTABLISHED indica que existe nivel de enlace con el proveedor. Este es el estado que aparece en condiciones normales. Cualquier otro indica que existe un problema en el circuito TEI_ASSIGNED indica que el router ha perdido la conectividad... Esto es normal cuando el proveedor desactiva los niveles 1 y 2 si no existen llamadas en curso (DDR) Otros valores posibles: TEI_UNASSIGNED ASSIGN_AWAITING_TEI ESTABLISH_AWAITING_TEI AWAITING_ESTABLISHMENT AWAITING_RELEASE TIMER_RECOVERY La mayoría de estos estados son temporales. Por lo que si se mantienen, pueden ser indicativos de problemas. Utilizar el debug isdn q921 para troubleshooting.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Spid Status	
TEI 109, ces = 1, state = 8(established)	Número de TEI y estado Los valores más comunes son: state = 1(terminal down) state = 3(await establishment) state = 5(init) state = 6(not initialized) state = 8(established) Sólo los estados 5 y 8 indican actividad sobre el circuito. El resto indican que el circuito no se ha establecido correctamente.
spid1 configured, spid1 sent, spid1 valid	Configuración de spid para un interface activo. En este caso el spid es válido. Otros estados posibles son: spid1 configured, no LDN, spid1 sent, spid1 valid spid1 NOT configured, spid1 NOT sent, spid1 NOT valid spid1 configured, spid1 NOT sent, spid1 NOT valid spid1 configured, spid1 sent, spid1 NOT valid Los últimos tres estados indican que el spid no está configurado o es incorrecto
Endpoint ID Info: epsf = 0, usid = 1, tid = 1 Endpoint ID Info: epsf = 0, usid = 3, tid = 1	(Endpoint identifier information) Se usa para determinar qué canal responderá a la llamada.
Layer 3 Status:	
0 Active Layer 3 Call(s)	Número de llamadas activas.
Activated dsl 0 CCBs = 0	(Digital Signal Link activated) (Number of call control blocks in use)
CCB:callid=27, callref=0, sapi=0, ces=1, B-chan=1	Información sobre la llamada activa. Esta línea no aparece hasta que la llamada está establecida.
Number of active calls =	Número de llamadas activas. Para un interfaz BRI puede haber como máximo 2. Esta línea no aparece hasta que la llamada está establecida
Number of available B-channels =	Número de canales B que no están siendo usados. Esta línea no aparece hasta que la llamada está establecida
Total Allocated ISDN CCBs =	ISDN call control blocks

Este Esquema, explica adecuadamente todos los parámetros del ISDN status, que pueden verificar los diferentes estados en las 3 capas en las que opera, layer 1, 2 y 3.

Tras haber observado diferentes procedimientos para verificar algunos servicios de comunicación, y como en este último caso, nos hemos ocupado de RDSI, que como he dicho, está en fase de decrecimiento.

No obstante, debido a un alto porcentaje de implantación de RDSI actualmente, vamos a ilustrar un proceso para verificar un backup RDSI sobre un servicio ADSL, con el objetivo de introducir al alumno en este proceso y poder aprender a solventar problemas actuales en este sentido, en las actuales implantaciones de este tipo de servicios de comunicaciones, con respaldo basado en tecnología RDSI.

Prueba de la rdsi de backup

Se puede forzar la llamada por RDSI sin tirar el ADSL, por ejemplo configurando una ruta en el equipo que vaya por el Dialer 1:

Málaga (config)#ip route 1.1.1.1 255.255.255.255 Dialer 1

Quitamos el backup del ADSL con:

Málaga (config)#interface ATM0.1 point-to-point

Málaga (config-subif)#no backup delay 3 180

Málaga (config-subif)#no backup interface Dialer1

Podemos activar un debug para comprobar que no hay problemas con el password y el usuario:

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Málaga #debug ppp authentication
Málaga #term mon
Lanzamos un ping a la 1.1.1.1 para forzar que haya tráfico por la RDSI y ver en el debug que levanta el interfaz BRI0:1:
Málaga #ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
.
Apr 18 11:31:26.900 METDST: %DIALER-6-BIND: Interface BR0:1 bound to profile Di1
Apr 18 11:31:26.900 METDST: BR0:1 PPP: Using dialer call direction
Apr 18 11:31:26.900 METDST: BR0:1 PPP: Treating connection as a callout
Apr 18 11:31:26.904 METDST: BR0:1 PPP: Session handle[4B00000A] Session id[8]
Apr 18 11:31:26.904 METDST: BR0:1 PPP: Authorization NOT required
Apr 18 11:31:26.904 METDST: BR0:1 PPP: No remote authentication for call-out
Apr 18 11:31:26.968 METDST: BR0:1 CHAP: I CHALLENGE id 1 len 28 from “ITAVAS1”
Apr 18 11:31:26.972 METDST: BR0:1 CHAP: Using hostname from interface CHAP
Apr 18 11:31:26.972 METDST: BR0:1 CHAP: Using password from interface CHAP
Apr 18 11:31:26.972 METDST: BR0:1 CHAP: O RESPONSE id 1 len 43 from “Málaga@vpn_Málaga-01”
Apr 18 11:31:27.264 METDST: BR0:1 PPP: Authorization NOT required
Apr 18 11:31:27.264 METDST: BR0:1 PPP: No remote authentication for call-out
Apr 18 11:31:27.316 METDST: BR0:1 PPP: Authorization NOT required
Apr 18 11:31:27.316 METDST: BR0:1 PPP: No remote authentication for call-out
Apr 18 11:31:27.372 METDST: BR0:1 CHAP: I CHALLENGE id 1 len 28 from “shbest1”
Apr 18 11:31:27.372 METDST: BR0:1 CHAP: Using hostname from interface CHAP
Apr 18 11:31:27.372 METDST: BR0:1 CHAP: Using password from interface CHAP
Apr 18 11:31:27.372 METDST: BR0:1 CHAP: O RESPONSE id 1 len 43 from “Málaga@vpn_Málaga-01”.
Apr 18 11:31:27.376 METDST: BR0:1 CHAP: I CHALLENGE id 2 len 28 from “shbest1”
Apr 18 11:31:27.376 METDST: BR0:1 CHAP: Using hostname from interface CHAP
Apr 18 11:31:27.376 METDST: BR0:1 CHAP: Using password from interface CHAP
Apr 18 11:31:27.376 METDST: BR0:1 CHAP: O RESPONSE id 2 len 43 from “Málaga@vpn_Málaga-01”
Apr 18 11:31:27.448 METDST: BR0:1 CHAP: I SUCCESS id 2 len 4
Apr 18 11:31:28.448 METDST: %LINEPROTO-5-UPDOWN: Line protocol o
Apr 18 11:31:28.448 METDST: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1, changed state to up...
Success rate is 0 percent (0/5)
Podemos comprobar que la llamada ha levantado y el destino con el siguiente comando:
Málaga# show isdn active

ISDN ACTIVE CALLS							
Call Type	Calling Number	Called number	Remote name	Second used	Second left	Second Iddle	Charges Uds/currency
Out	N/A	909 210 709	avas-MP	15	0	0	0

También podemos ver problemas de Nivel 1 y 2 en caso de que no se establezca la llamada con el siguiente comando:
Málaga # show isdn status
Global ISDN Switchtype = basic-net3

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

ISDN BRI0 interface
dsl 0, interface ISDN Switchtype = basic-net3
Layer 1 Status:
ACTIVE
Layer 2 Status:
TEI = 97, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
Layer 3 Status:
1 Active Layer 3 Call(s)
CCB:callid=8003, sapi=0, ces=1, B-chan=1, calltype=DATA, hdlctype=HDLC-TRUNK
Active dsl 0 CCBs = 1
The Free Channel Mask: 0x80000002
Total Allocated ISDN CCBs = 1
Una vez terminado este escenario de pruebas, debemos volver al estado original con el backup RDSI en Stand by, y el ADSL funcionando.
No olvidemos igualmente, eliminar la ruta estática creada para generar el tráfico que necesitábamos, para levantar la interfaz BRI de RDSI.
Málaga (config)# undebug all
Málaga (config)# term no mon
Málaga (config)# no ip route 1.1.1.1 255.255.255.255 Dialer1
Málaga (config)#interface ATM0.1 point-to-point
Málaga (config-subif)# backup delay 3 180
Málaga (config-subif)# backup interface Dialer1
Una vez hemos analizado los procedimientos de verificación del ISDN, se va a proceder a hacer una breve introducción del Interfaz ISDN BRI para un mejor conocimiento de esta interfaz, hoy día en decrecimiento.
El interfaz ISDN BRI de los Routers permite manejar un acceso básico de RDSI que incluye un canal D y dos canales B. Generalmente el canal D se utiliza para enviar mensajes de señalización de establecimiento y liberación de llamadas.
Los canales B se usan para la transmisión de datos de otros protocolos.
Los routers, soportan RDSI conmutada o semipermanente y se adaptan a muchos de los distintos estándares de RDSI que existen.
Además, se pueden configurar una serie de parámetros que determinan el comportamiento del interfaz y que permiten que estos routers puedan ser utilizados en la mayoría de los escenarios y lugares del mundo.
El interfaz ISDN BRI asegura el acceso a la RDSI para la transmisión de datos sobre los canales B, soportándose en ellos distintos protocolos.
Se puede considerar este interfaz como un intermediario entre la RDSI y otros interfaces usuarios que solicitan sus servicios.
Sobre el interfaz ISDN BRI se pueden configurar tantos interfaces usuario como se quiera (de tipo FR Generic o PPP Generic).
Al arrancar el equipo, cada interfaz usuario se registra sobre el interfaz base ISDN BRI.
En la información de registro se le indica al ISDN BRI qué canal B se quiere utilizar y se le proporciona un nombre de perfil de llamada.

El ISDN BRI utiliza ese perfil cuando realiza llamadas salientes por encargo del interfaz usuario y también para filtrar las llamadas entrantes y poder así asignarlas al interfaz que corresponda.
Cuando un interfaz usuario quiere establecer un enlace, se lo solicita al interfaz base ISDN BRI mediante un comando interno.
El ISDN BRI, cuando tenga disponible el enlace (por ejemplo, cuando haya conseguido establecer una llamada), informará al interfaz usuario mediante el correspondiente evento.
Una vez establecido el enlace, comienza el intercambio de datos.
Naturalmente, si varios interfaces usuario, ya sean FR Generic o PPP Generic, compiten por el mismo canal B, el interfaz ISDN BRI asignará el enlace al primer usuario que se lo haya pedido, teniendo que esperar el otro a que se libere el recurso.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

Cuando se trabaja con una RDSI donde los dos canales B son semipermanentes, no es necesario el establecimiento de llamada y tampoco que el interfaz usuario solicite la activación del enlace mediante comando.
Ésta se produce de manera automática en el momento del registro y, en consecuencia, sólo dos interfaces usuario podrán conseguir la activación de sus enlaces.
En los apartados que siguen a esta introducción se explica la configuración específica del interfaz ISDN BRI.
No obstante, un operador que desee configurar un router para que maneje enlaces Frame Relay o PPP por RDSI deberá también dominar la configuración de los perfiles de llamada y de los interfaces usuario FR Generic y PPP Generic.
El interfaz ISDN BRI asegura el acceso a la RDSI para la transmisión de datos sobre los canales B, soportándose en ellos distintos protocolos.
Se puede considerar este interfaz como un intermediario entre la RDSI y otros interfaces usuarios que solicitan sus servicios.
Sobre el interfaz ISDN BRI se pueden configurar tantos interfaces usuario como se quiera (de tipo FR Generic o PPP Generic).
Al arrancar el equipo, cada interfaz usuario se registra sobre el interfaz base ISDN BRI.
En la información de registro se le indica al ISDN BRI qué canal B se quiere utilizar y se le proporciona un nombre de perfil de llamada.
El ISDN BRI utiliza ese perfil cuando realiza llamadas salientes por encargo del interfaz usuario y también para filtrar las llamadas entrantes y poder así asignarlas al interfaz que corresponda.
Cuando un interfaz usuario quiere establecer un enlace, se lo solicita al interfaz base ISDN BRI mediante un comando interno.
El ISDN BRI, cuando tenga disponible el enlace (por ejemplo, cuando haya conseguido establecer una llamada), informará al interfaz usuario mediante el correspondiente evento.
Una vez establecido el enlace, comienza el intercambio de datos.

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.