# Redes de Computadoras

**Clasificación:**
**Tipos de Conexión**

- Conexión Directa (Punto a Punto)
- Múltiples Conexiones (Multipunto)

**Distribucion geografica:**
- PAN Personal Área Network
- LAN Local Área Network
- MAN Metropolitan Área Network
- WAN Wide Área Network

**Topologia:**
- Topología o Red en Bus –> Ethernet
- Topología o Red en Estrella –> ATM
- Topología o Red en Anillo –>Token Ring/FDDI
- Topología o Red en Malla

## WAN Red de Área Amplia

- También se las denomina Redes de larga distancia y cubren extensa Área geográfica.
- Se diferencia de Una LAN no solo de la Distribución Geográfica (Tamaño de La red) sino por la capacidad de crecimiento (Escalabilidad).
    - Tipo de Equipos Teleinformáticas.
    - Ancho de Banda de canal.
    - Gran capacidad de Comunicación Simultánea.

**Redes Conmutadas**
Nodos de Conmutación con enlaces multiplexados (FDM -TDM).
- Conmutación de Circuitos
- Conmutación de paquetes

**Conmutación de Circuitos**
- Nodos
- Enlace Lógico
- Conmutación de canales sin retardos. Ej. : Red Telefónica
- Abonado
- Bucle Local
- Centrales
- Líneas Principales Multiplexadas
- División en el Espacio
    - Matriz de Conexiones Simple.
    - Varias Matrices en Etapa.
- División en el Tiempo
    - DM Sincronía

**Conmutación de Circuitos - Fases**
- Establecimiento del Circuito
- Transferencia de datos
- Desconexión del Circuito

**Conmutación de Paquetes**
- No es necesario reservar recursos (Circuito).
- Paquete de nodo de nodo siguiendo algún camino.
- Nodo Almacena y Retransmite.

Técnicas
- Datagramas.
- Circuitos Virtuales.

Independencia del fuente :
- Los paquetes se encaminan independientemente de la fuente de origen o la trayectoria tomada antes en particular.
- Aumenta la eficiencia porque todos los Switches utilizan el mismo principio.

Los Nodos están interconectados por Switches (Conmutadores de paquetes) que hacen almacenamiento(Buffer) y Reenvío.

Grupos de Conmutadores de Paquetes con varios conectores de Entrada/Salida

**Encaminamiento: Direccionamiento Físico Jerárquico**

Dirección {a,b}
a=Conmutador
b=Computadora

Tabla de Enrutamientos(Saltos)
- Estáticos : Las rutas son calculadas y quedan fijas.
- Dinámicos: Las rutas son calculadas y modificadas Dinámicamente.

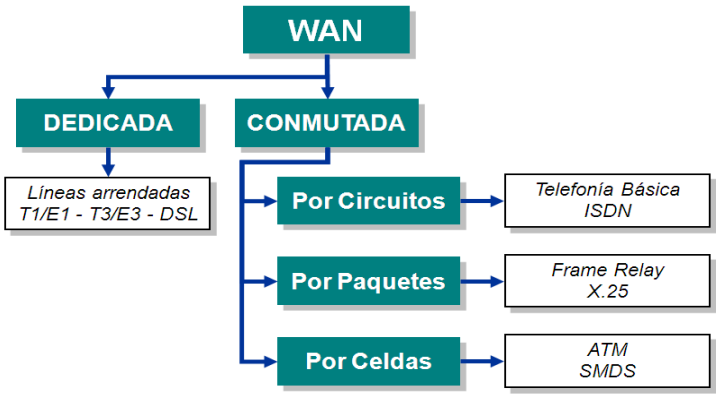
Algoritmo de Dijkstra
- (Trayectoria con menores enlaces=menor peso).
- Calculo Distribuido de Rutas (Informar calculo de rutas a vecinos=Adaptación permanente ante fallas)
- Enrutamiento Vector-distancia (distancia de destino =suma de los Pesos).
- Enrutamiento por Estado de enlace (SPF)

**ARPANET**

Red de la Agencia de Investigación avanzada de proyectos (ARPA)
Una de las primeras WAN de Conmutación de paquetes 1969 (30 Años).
Red de Conmutación de paquetes.
Dejo de funcionar en 1990 para convertirse en Internet .

**Abilene**
- Red de Servicios de conexión de alto rendimiento entre puntos de agregación regional de I2
- Proyecto UCAID complementario a I2.

- Backbone de Red Primario para I2.
- POS (Packet Over SONET)
- Comenzó a prestar servicios en Enero de 1999.
- IPv6 y QoS.
- OC 48 (2,5 Gbps) 1999– OC 192 (10 Gbps) 2004




**X25**

- Servicio Conmutador de Paquetes ofrecido por portadores públicos casado en la Norma CCITT X.25.
- Se utiliza para asistir a terminales remotos para conectar con sus Host.
- Comenzó con un ancho de banda de 64 KBPS y en 1992 paso a tener 2 MBPS.
- Argentina - Startel /Red Arpac.
- Protocolo Normalizado que correspondía a los primeros tres niveles del modelo OSI (Física, Enlace y Red).
- Trabaja bajo a una Topología que se la denomina Malla.
- Protocolo de Modo de transmisión Asincrónica.
- Aplica Detección y Corrección de Errores (Chequeo, Corrección, retransmisión)

**ATM Modo Asincrónico de Transmisión**

- Tecnología de Transmisión de datos de Alta velocidad desarrollada por AT&T y US Print.
- Los primeros productos que la soportan empezaron a aparecer partir del año 1994.
- Se pueden utilizar para Redes Privadas, Interconexiones de LANS o WANS.
- Su ancho de Banda permite la Transmisión de voz, vídeo y Datos.
- Conmutación de Circuitos –>Telefonía
- Conmutación de Paquetes –>Telegrafía
- Asincrónico se refiere a la discontinuidad entre celdas del mismo usuario.
- Routers que conectan a Redes ATM.
- Swiches ATM o con módulos opcionales.
- Swiches de Grupo de Trabajo para Introducir ATM a altas velocidades en computadoras de escritorio.
- Adaptadores ATM.
- Tecnología de Banda Ancha, de alta velocidad (1 Gbps).
- La conexión entre los Conmutadores se realiza con Medios de de Alta Velocidad.
- Todos los paquetes(Celdas) Transmitidos tienen el mismo tamaño (Longitud Fija) evitando retardos en la Comunicación. Examina cabecera de paquete e inmediatamente retransmite.

- Las redes de este Tipo contienen conmutadores ATM, Dispositivos multipuertos que realizan conmutación de Celdas.
- La conmutación se hace a Nivel de Hardware .
- Colocan Información a nivel de Celda y la envían (Paquete Rápido).
- En Nodo ATM se realiza verificaciones de errores, sin corrección para evitar evitan los atascos. Perdida / Errores originan retransmisión de la Celda.
- Opera dentro del Nivel de Enlace del Modelo OSI.
- Las Velocidades de Transferencia son escalables de acuerdo al medio físico utilizado.
- Los canales establecidos o conmutados se los denominan canales virtuales y el trayecto circuitos virtuales.

- Caminos Virtuales 4 Ventajas :
    - Arquitectura Simplificada
        - Canal Virtual _ Lógica Individual
        - Camino Virtual _ Grupo de Conexiones
    - Incremento de Eficiencia y Fiabilidad
    - Procesamiento/tiempo de conexión _ Pequeño
    - Servicios de red Mejorados
        - Grupos de usuarios fijos (Redes fijas de haces de canales virtuales)

**MPLS (Multiprotocol Label Switching)**

- Definido en el RFC 3031
- Opera en la capa de enlace de datos y de red.
- Proporciona circuitos virtuales en las redes IP.
- Es independiente del protocolo que se use en los extremos.
- El camino esta prefijado desde el origen (como en ATM – frame Relay)
- Solución al problema de procesamiento que presentan los routers externos IP (grandes tablas de enrutamiento: IP + interfaz).
- Introduce mejoras a IP:
  - Redes privadas virtuales
  - Ingeniería de tráfico
  - Mecanismos de protección frente a fallas
- Agrega etiquetas al paquete para enrutarlo.
- No utiliza la IP de origen y destino para enrutarlo.
- Sus Paquetes son de Log. Variable.
- Tabla de enrutamiento:
  - Interfaz de entrada
  - Etiqueta de entrada
  - Intefaz de salida
  - Etiqueta de salida
- LSP - Label Switch Pad: Camino designado entre routers MPLS.
- Si hay 2 rutas con igual cantidad de saltos, entonces se hace balanceo entre las 2 rutas.
-

**IP + MPLS**

- Label (20 bits): Es la identificación de la etiqueta.
- Exp (3 bits): uso en diffserv (servicios diferenciados).
- S (1 bit): stack, sirve para el apilado jerárquico de etiquetas. Cuando S=0 indica que hay mas etiquetas añadidas al paquete. Cuando S=1 estamos en el fondo de la jerarquía.
- TTL (8 bits): Time-to-Live, misma funcionalidad que en IP, se decrementa en cada enrutador y al llegar al valor de 0, el paquete es descartado.

**Etiquetas**

- Label 1: Etiqueta obligatoria MPLS
- Label 2: Etiqueta utilizada para establecer VPNs en MPLS. Solo es leida por los routers de los extremos.
- Label 3: Utilizado para el protocolo RSVP. Permite seleccionar un camino que no es el de menor saltos, sino que es más eficiente.
-

Un **SLA** es un protocolo plasmado normalmente en un documento de carácter legal por el que una compañía que presta un servicio a otra se compromete a prestar el mismo bajo unas determinadas condiciones y con unas prestaciones mínimas.

El nivel de servicio se basa en indicadores que permiten cuantificar de manera objetiva determinados aspectos del servicio prestado. Por ejemplo un indicador de nivel de servicio puede ser el tiempo de resolución de incidencias. Este indicador se mide a través de aplicaciones de gestión de incidencias que registran el momento que una incidencia es comunicada y cuándo es cerrada. La diferencia entre estos dos datos es el indicador en bruto desagregado que luego puede ser procesado mediante algoritmos para obtener promedios, desviaciones y otros indicadores normalizados.

En un SLA se pueden establecer tantos indicadores como se estime necesario y de su evaluación se obtienen por ejemplo penalizaciones a la empresa suministradora, identificación de puntos débiles del proceso e indicaciones para procesos de mejora contínua (CMM) en determinadas actividades.

El conjunto de indicadores de nivel de servicio suele formar un cuadro de mando donde se puede ver de manera global cómo se está desarrollando la prestación del servicio e identificar puntos críticos del proceso y establecer alarmas.

SLA también es una referencia a la hora de establecer parámetros de calidad del servicio (nivel de satisfacción) (QoS) basados en indicadores objetivos que obvian impresiones y percepciones más subjetivas y personales.

**Jitter** es un efecto de las redes de datos no orientadas a conexión y basadas en conmutación de paquetes. Como la información se discretiza en paquetes cada uno de los paquetes puede seguir una ruta distinta para llegar al destino.Se define técnicamente como **la variación en el tiempo en la llegada de los paquetes, causada por congestión de red, perdida de sincronización o por las diferentes rutas seguidas por los paquetes para llegar al destino**.

Las comunicaciones en tiempo real (como VoIP) son especialmente sensibles a este efecto. En general, es un problema frecuente en enlaces lentos o congestionados. Se espera que el aumento de mecanismos de QoS (calidad del servicio) como prioridad en las colas, reserva de ancho de banda o enlaces de mayor velocidad (100Mb Ethernet, E3/T3, SDH) puedan reducir los problemas del Jitter en el futuro aunque seguirá siendo un problema por bastante tiempo.

El Jitter entre el punto inicial y final de la comunicación **debiera ser ser inferior a 100 ms**. Si el valor es menor a 100 ms .Puede ser compensado de manera apropiada. En caso contrario debiera ser minimizado.

La disponibilidad de cada enlace deberá ser del *(ej.: 99,7% horas)* medida en términos anuales y del *(ej.: 99,2%)* en términos mensuales <*opcionalmente se podrán indicar bandas horarias, ej.: "...del 99,4% mensual durante los días hábiles entre las 8:00 y las 20:00 hs y del 99,2% para otros horarios..."*>, con una tasa de error de 1 bit errado cada 107 bit transmitidos.

El Tiempo Mínimo Medio entre Fallas (***MTmBF***) por mes será de *(ej.: 30 horas)*.
El Tiempo Mínimo entre Fallas (***TmBF***) por mes será de *(ej.: 15 horas)*.
El Tiempo Máximo de Restauración del Servicio (***TMRS***) será menor a *(ej.: 3 horas)*.

Las **redes convergentes** o **redes** de multiservicio hacen referencia a la integración de los servicios de voz, datos y video sobre una sola **red** basada en IP como protocolo de nivel de **red**. Este sistema ha fomentado la creación de soluciones en comunicaciones unificadas.

**Red tradicional**
**Caracteristicas:**
- Red de datos con múltiples protocolos.
- Complejas Interacciones entre ellos.
- Inteligencia Distribuida en elementos activos/dispositivos intermedios.
- El Plano de control de Rutas se realiza a Través de Capa 2 o Capa 3 – OSI.
- Rutas Definidas – Tráfico de Red con trayectorias programadas.
- Elementos Activos-Dispositivos intermedios: Routers/Switches
- Sistemas Abiertos y Estándares.
- Componentes Monolíticos.
- Soluciones Propietarias.

**Redes definidas por software (SDN)**
**Caracteristicas:**
- Conjunto de técnicas relacionadas con el área de redes computacionales.
- Su objetivo es facilitar la implementación de servicios de red de una manera determinista, dinámica y escalable.
- Libera al administrador de red gestionar dichos servicios a bajo nivel.
- Paradigma que posibilita servicios de computación a través de red, usualmente es internet.
- Una nueva forma de organizar y programar las redes de computadoras; configurar y administrar el comportamiento de la red de forma dinámica y escalable.
- Permite, centralizar y automatizar la administración de la red.
- Aplica virtualización en la red, optimizando un gran control de la ingeniería de tráfico.

**Arquitectura:**
**Capa de Infraestructura**
En esta capa, los switches se encargarán de procesar los paquetes de datos basados en las reglas instauradas por el controlador de SDN. La red pasa a ser completamente programable con la posibilidad de realizar cambios de comportamiento en tiempo real y con un comando centralizado en un único punto lógico, el controlador. Los switches que están conectados a la capa de control mediante un canal seguro (Southbound API), son un simple dispositivo que reenvía flujos de datos desde un cliente a un servidor y viceversa.

**Capa de Control**
Aquí se encuentra el controlador a cargo de coordinar los cambios de configuración en los switches de la capa de datos, basado en las VNF programadas por los operadores de la red. Como el sistema operativo de una computadora normal ofrece servicios para el manejo de recursos y el acceso a sistema de archivos, un controlador de SDN provee funciones similares para las VNF. Existen diferentes tipos de controladores opensource que soportan diferentes versiones del protocolo Openflow, con diversas interfaces de programación y que ofrecen distintos servicios para las funciones de red virtualizadas (VNF).

**Capa de aplicación y compilación**
En esta capa se encuentran las funciones de red programadas en los lenguajes de alto nivel con el correspondiente compilador asociado, para traducir el código de las aplicaciones que emulan las VNF a las llamadas a la API (Northbound API) específica del sistema operativo del controlador de SDN que se esté implementando

**+ Caracteriticas:**

Programable: El control de la red se puede programar directamente porque está desacoplado de las funciones de reenvío.

Ágil: La abstracción del control del reenvío permite a los administradores ajustar dinámicamente el flujo de tráfico en toda la red para satisfacer las necesidades cambiantes.

Gestionada Centralmente: La inteligencia de la red está (lógicamente) centralizada en controladores SDN basados en software que mantienen una visión global de la red, que para las aplicaciones y los motores de políticas aparece como un único conmutador lógico.

Configurada Pragmáticamente: SDN permite a los administradores de red configurar, administrar, proteger y optimizar los recursos de red muy rápidamente a través de programas SDN dinámicos y automatizados, que pueden escribir ellos mismos porque los programas no dependen de software propietario.

Abierto: Basado en estándares e independiente del hardware: Cuando se implementa a través de estándares abiertos, SDN simplifica el diseño y la operación de la red porque los controladores SDN proporcionan las instrucciones en lugar de múltiples dispositivos y protocolos específicos del proveedor.

**Componentes - Controlador:**

**Interfaz Sur :**

A través de esta interface el controlador gestiona las tablas de instrucciones de los elementos de red mediante envío de registros de flujos.

Dispositivos :

- Switch SDN.
- Routers SDN.

Los Elementos de red luego procesaran los paquetes en el plano de datos de acuerdo a la información e las tablas.

**Interfaz Norte:**

Mediante esta interfaz el controlador permite que aplicaciones externas pueden utilizar el controlador para modelar algunos tipos de elementos físicos o lógicos (como firewalls, balanceadores de trafico, modeladores de Qos, orquestadores de datacenter, etc.), puedan implementarse de forma virtual.

**API**: Es un conjunto de subrutinas, funciones y procedimientos (o métodos, en la programación orientada a objetos) que ofrece cierta biblioteca para ser utilizada por otro software como una capa de abstracción.

La interfaz norte, permite que aplicaciones SDN puedan modificar comportamientos del controlador, a través de APIs.

A través de las API las aplicaciones pueden:

• Configurar flujos para alterar rutas entre dos equipos de red.
• Balancear el trafico a través de múltiples caminos de red.
• Reaccionar en forma tempranas a cambio en la topologías de la red, mediante la detección de fallas de enlaces, inserción de nuevos dispositivos y enlaces de red.
• Redirigir trafico con la finalidad de inspeccionar, autenticar, segregar y realizar algunas otras tareas relacionadas con la seguridad. La interfaz norte carece actualmente de estándar y podría complicar la interoperabilidad entre aplicaciones y controladores.

**Protocolo Openflow – Interfaz Sur**

**Establece la comunicación entre el controlador SDN y los conmutadores o enrutadores de red (switches o routers), es decir, entre la capa de control y la capa de infraestructura.**

**Protocolo Openflow:**
**Surgido en la Universidad de Standford.**
**Control Centralizado, los elementos de red SOLO reenvían paquetes.**

OpenFlow: Se define como un protocolo emergente y abierto de comunicaciones que permite a un servidor de software determinar el camino de reenvío de paquetes que debería seguir en una red de switches.

**OpenFlow : Es un protocolo empleado entre la interfaz sur del controlador y los switches SDN, para la trasmisión de políticas, efectuar consultas al controlador sobre inexistencia de alguna política para procesar algún tipo de paquete , efectuar intercambio de información para la gestión de la topología de red y obtención de información estadística.**

Los flujos almacenados en los elementos de red tienen dos campos, los datos que identifican ese flujo (origen, destino) y una acción. Existen dos modos de funcionamiento de OpenFlow: proactivo y reactivo

• **En el modo proactivo**, el controlador carga todas las tablas en forma previa al comienzo del procesamiento de paquetes en el plano de datos.
• **En el modo reactivo**, los dispositivos de red tienen sus tablas vacías cuando comienzan a procesar paquetes. Cuando llegan los paquetes, el dispositivo de red revisa si existen entradas en las tablas para procesarlos. Si no existe una entrada para procesar un paquete, el elemento de red informa al controlador de esta situación, el controlador determina la acción correcta y envía al elemento de red la entrada de flujo correcta. Con este método se van poblando las tablas con todas las acciones necesarias.

**El controlador SDN s**e encarga de traducir las necesidades o requisitos de la capa Aplicación a los elementos de red, y de proporcionar información relevante a las aplicaciones SDN, pudiendo incluir estadísticas y eventos

Rol de los Controladores, estos son los encargados principales de tomar el responsabilidad del Panel de Control de la red. También son los encargados de segmentar la red global y unificarla en redes regionales. A raíz de ello, se obtiene una reducción en la complejidad de la red ya que

se disminuye el tamaño de las tablas de enrutamiento, como así también, se disminuye la cantidad de actualizaciones en los protocolos de comunicación que utilizan los Controladores entre sí cuando se generan cambios en la red.
Además, el rol del Controlador permite la comunicación entre los distintos tipos de enlaces que puedan existir en la red. Por ejemplo, si hay más de un proveedor de MPLS, necesitamos de los controladores para hacer de puente entre ellos. Sucede de la misma manera, si tenemos enlaces de Internet, MPLS, LTE, etc.

Por un lado, se encuentra el rol de Director o Administrador de la solución, el cual es el encargado de la Orquestación de la arquitectura. Es decir, es el cerebro de la red y, por ende, el encargado del aprovisionamiento de los equipos, el despliegue o instalación de los mismos en la red y su posterior administración. A su vez, es el administrador de todos los servicios que se brindan en la red (Enrutamiento, seguridad, aceleración, balanceo, etc.).
Cabe señalar que el Director, además, es el encargado de establecer la topología de la arquitectura de la red (ya sea una red mallada completa, redes malladas conexas, redes punto a punto, punto-multipunto, etc.), como así también, de todas las configuraciones de los equipos remotos.
Dentro de este mismo rol, también se definirán las plantillas de configuración, que son las que poseen la configuración general de los sitios a implementar (tema que se tratará en más detalle en el capítulo X. Despliegue y automatización). De esa manera, si varios sitios poseen características similares, permite que puedan agruparse en una misma plantilla de configuración y estandarizarse el despliegue de la red. En otras palabras, esto implica que una misma configuración, pueda ser utilizada para varias oficinas o sitios de manera que se agilice la implementación de los equipos a raíz de su automatización.
En el rol de Director, además, se puede definir una cantidad muy granular de configuraciones, como puede ser la calidad de servicio para cada tipo de enlace, las configuraciones de los dispositivos finales, configuraciones hacia la LAN y configuraciones hacia los circuitos Wan, las especificaciones tanto Underlay como Overlay de los sitios, configuraciones de BGP, etc.
El Director termina haciendo las veces de un único panel o interfaz de administración de toda la red, en virtud de que desde una única ubicación de red se puede administrar toda la infraestructura WAN por más grande que sea. De esa manera, resulta posible ver todos los equipos a través de distintos tableros predefinidos y/o configurables desde los cuales se obtiene el control absoluto de lo que sucede en cada sitio particular y, a su vez, en la red en general. Asimismo, permite monitorear cualquier enlace, ejecutar cualquier tipo de operación a nivel de equipo o grupo de equipos, como desplegar nuevos dispositivos finales o controladores, agregarlos a la red, ejecutar actualizaciones a nivel global en todos los equipos, etc.
Por otro lado, también existe el rol de los dispositivos finales, que son los encargados de conectar los distintos sitios remotos a la red. Son los enrutadores de cada sitio, los cuales también pueden brindar los servicios agregados que se necesiten, como podría ser la aceleración WAN, seguridad, balanceo, etc.
Justamente, estos dispositivos finales reciben la configuración desde el Director o Manager y son quienes brindan la conectividad a los usuarios finales a la red WAN. Asimismo, pueden brindar múltiples servicios a los usuarios finales, los cuales pueden ser propios (ya sea desarrollados por el proveedor de la solución) o de un proveedor externo (un desarrollo de una empresa tercerizada) como puede ser las funciones de seguridad, aceleración WAN, perímetro de seguridad, balanceo de carga, etc.
El agregado de servicios en los enrutadores se da gracias al uso de servicios virtuales en los dispositivos finales (los cuales son físicos). Para ello, se les agregan imágenes de servicios virtuales a los equipos finales -los cuales constan de un módulo principal- que ofrece la funcionalidad de Enrutador (a estos, a su vez, se les pueden adicionar más servicios a través

de otras imágenes a medida que las necesidades lo requieran). Estas funcionalidades virtuales que se agregan a los dispositivos finales son llamadas Virtualización de Funciones de red (del inglés Virtual Network Function – VNF).
Esto hace que los dispositivos finales puedan brindar servicios desde la capa 2 hasta la capa 7 dentro del modelo TCP/IP, gracias a los distintos servicios que pueden ejecutar dentro de los mismos.
Como ya se ha mencionado anteriormente, los dispositivos finales son quienes tendrán bajo su responsabilidad (junto con los controladores), establecer los túneles dinámicos (lógicos) a los fines de conectar los distintos sitios entre sí, o conectar ellos mismos contra los controladores

**La “Nube”**, como bien le dicen, es el nombre corto que coloquialmente se utiliza para referirse a las tecnologías de Cloud Computing.

Más allá de ser una tecnología, involucra un ecosistema de herramientas, aplicaciones e infraestructura que soporta una genial y moderna forma de trabajo. La nube es un espacio que, de forma sencilla, **permite sincronizar nuestro trabajo, contenido o archivos, en cualquier dispositivo que esté enlazado a esta**. Es más, si lo ponemos un poco más sencillo, es la forma de:

- Tener todos nuestros archivos **sincronizados** en todos nuestros equipos.
- **Respaldar** toda la información en un lugar externo a nuestro equipo
- **Consumir recursos** de “otra computadora compartida” en lugar de la nuestra.
- **Trabajar con contenidos** que no tenemos físicamente en nuestro equipo.
- Trabajar de forma **colaborativa, simultánea e incluso remota**.

**Un centro de datos** es una instalación utilizada para alojar sistemas de computación y componentes relacionados, entre los que se incluyen los siguientes:

- Conexiones de comunicaciones de datos redundantes
- Servidores virtuales de alta velocidad (en ocasiones, denominados “granjas de servidores” o “clústeres de servidores”)
- Sistemas de almacenamiento redundante (generalmente utilizan tecnología SAN)
- Fuentes de alimentación redundantes o de respaldo
- Controles ambientales (p. ej., aire acondicionado, extinción de incendios)
- Dispositivos de seguridad

**Servicios de Internet**

Se identifican con :

- Dirección IP.
- Nombre de Dominio Único.
- Puerto Asociado a cada Servicio Solicitado.
- Cada Servicio (Server).
- Escucha permanentemente cada Puerto.
- Puerto : identificador único del servicio Deseado.
- Lo utiliza TCP para identificar los Servicios.
- El protocolo usa el identificador para dirigir las solicitudes de entrada al servidor adecuado .
- Numero Entero de 32 Bits (IPv4).
- Numero Hexadecimal de 128 Bits (IPv6).
- WWW Web Internet
- WWW2 Web Internet 2

**DNS - Sistema de Nombres de Dominio**

Conjunto de protocolos y servicios sobre una red TCP/IP, permite a los usuarios de red utilizar nombres jerárquicos sencillos para comunicarse con otros equipos, en vez de memorizar y usar sus direcciones IP.
Usado en Internet y en Redes Privadas Actuales.
Servicios como: browsers, servidores de Web, FTP y Telnet; utilizan DNS.

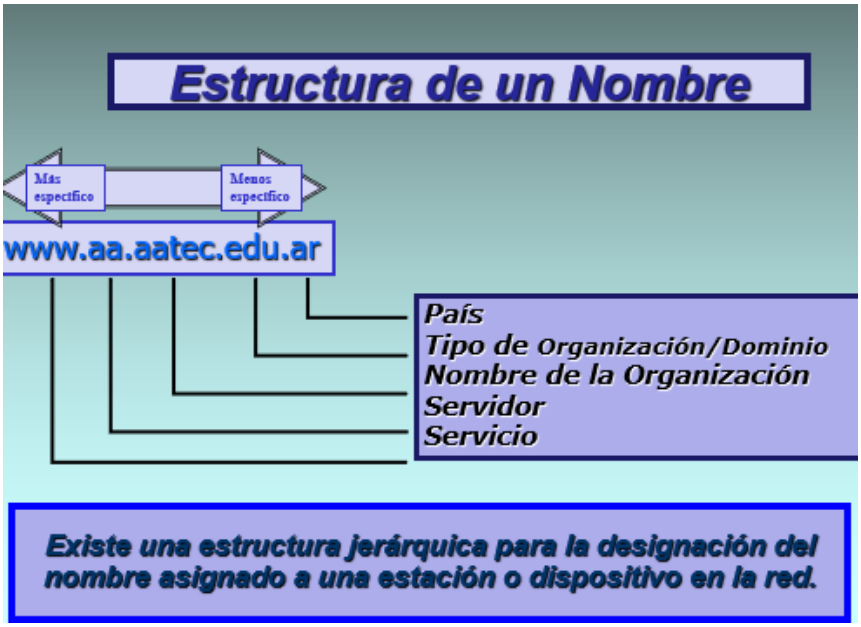
**DNS define:**

Un modelo de base de datos para almacenar información sobre direcciones.
Un mecanismo para preguntar y actualizar información sobre direcciones en la base de datos.

Un mecanismo para replicar replicar información entre servidores.

Una zona DNS es una porción del espacio de nombres DNS sobre la que un servidor DNS tiene autoridad. Dentro de una zona DNS, hay registros de recurso (RR), que definen los hosts y otro tipo de información que completan la base de datos de la zona.
Hay varios tipos de zona:
- Zonas primarias: Contienen la copia principal de los RR de la zona. Los cambios y actualizaciones de la zona se producen en la zona primaria. Si queremos crear un nuevo dominio DNS tendremos que crear una zona primaria. La zona DNS primaria se almacena en un archivo local (en Windows tiene extensión .dns) del servidor.
- Zonas secundarias: Las zonas secundarias son copias no editables de las zonas primarias. Se usan para balanceo de carga y tolerancia a fallos. Períodicamente, según la configuración, la DNS primaria realiza una "transferencia de zona" a la secundara. Si la DNS primaria cae, durante un tiempo, la DNS secundaria asumirá las respuestas, aunque pasado un periodo de tiempo especificado por el administrador (TTL o Time To Live), la zona secundaria caducará. Antes de que esto ocurra, la DNS primaria debe ser rearmada.
- Zonas integradas con Active Directory

- El Nombre consta de una Secuencia de segmentos alfanuméricos separados por puntos.
- Sistema de Nombres Jerárquicos siendo la parte mas significativa a la Derecha.
- La parte de la izquierda corresponde al nombre de una computadora.
- Los otros segmentos del nombre corresponden al Grupo al cual pertenecen.
  -




| Domain Name | Assigned To |
|---|---|
| com | Commercial organization |
| edu | Educational institution |
| gov | Government organization |
| mil | Military group |
| net | Major network support center |
| org | Organization other than those above |
| arpa | Temporary ARPA domain (still used) |
| int | International organization |
| *country code* | A country |

- Estructura Geográfica de Registro identificando al País.
- Las Organizaciones Propietarias del Domino Registrado con Direcciones IP ante NIC local/InterNIC pueden decidir si agregan alguna estructura jerárquica adicional.
- No existen Normas ni patrones informes para las Estructuras Jerárquicas Adicionales.
- Cada Servidor sabe como llegar a la raíz y los mismos son autoridades de los nombres de inferior Jerarquía.

**Un resolutor** es un proceso que gestiona el proceso de consulta y recepción de respuesta de datos DNS. Los resolutores están presentes en los clientes, y en los servidores que intentan responder a consultas de clientes, que a priori no saben consultar.
Una consulta es una petición de información enviada a un servidor DNS. Hay tres tipos de consulta: recursiva, inversa o interativa.

El resolutor de DNS es un componente del sistema que realiza solicitudes de DNS a otro u otros servidores de DNS. La pila de TCP/IP se configura, normalmente, con la dirección de IP de al menos un servidor de DNS al que el resolutor envía una o más solicitudes de información de DNS. el resolutor forma parte del servicio Cliente de DNS. Este servicio se instala automáticamente cuando se instala TCP/IP y se ejecuta como parte del proceso. En Windows , el resolutor de DNS es un componente del sistema que realiza solicitudes de DNS a otro u otros servidores de DNS. La pila de TCP/IP de Windows se configura, normalmente, con la dirección de IP de al menos un servidor de DNS al que el resolutor envía una o más solicitudes de información de DNS.
El resolutor forma parte del servicio Cliente de DNS. Este servicio se instala automáticamente cuando se instala TCP/IP y se ejecuta como parte del proceso Services.Exe. Como la mayoría de los servicios de Windows , el servicio Cliente de DNS se activa en el dominio System de Windows.
La resolución de nombres de DNS se produce cuando un resolutor, en un host, envía a un servidor de DNS un mensaje de solicitud con un nombre de dominio. El mensaje de solicitud indica al DNS que busque el nombre y devuelva ciertos RR. El mensaje de solicitud contiene el nombre de dominio a buscar y un código que indica los registros que se deben devolver.
Un cliente envía una solicitud de DNS pidiendo al servidor de DNS todos los registros A de kona.midominio.com. La respuesta a la solicitud contiene la entrada de solicitud y los RR de respuesta.
Resolución de alias: Si el resolutor intenta realizar resolución de nombres de un nombre que indique el usuario, no sabe a priori si el nombre se refiere a un RR (A) de host o a un CNAME. Si se refiere a un CNAME, el servidor puede devolver el CNAME. Sin embargo, en este caso, el CNAME debe resolverse todavía. Para evitar tráfico extra de DNS, cuando un servidor de DNS devuelve un CNAME en respuesta a una búsqueda de registro de host, el servidor de DNS también devuelve el registro A relativo al CNAME.
El cliente de DNS envía una solicitud de DNS al servidor de DNS solicitando el registro Host de nsl.midominio.com, que en realidad es un alias de kona.midominio.com. En la respuesta de DNS existen dos RR de respuesta. El primero es el RR CNAME de nsl.midominio.com, que contiene el nombre canónico. El segundo RR de respuesta es el registro Host de kona.midominio.com, que contiene la dirección de IP de este equipo.

**InterNIC Servicio de Base de Datos y de Directorio**
- Servicio Internacional y fuente de información de documentos de Internet.
- Administración de elementos técnicos del DNS.
- Servicio de Registro de Red –> Registro de Direcciones IP y Nombres de dominio. –> IANA
- InterNIC : delega sus funciones en los NIC de cada País.
- NIC Argentina :Secretaria  Legal  y Técnica de la PN.

**Un servidor DNS** (Servidor de nombre de dominio, del inglés, Domain Name Server) es la tecnología encargada de enlazar los dominios que colocamos en la barra de navegadores a las direcciones IP de los servidores. En estos servidores es donde se encuentra realmente nuestro contenido, actuando como si fuera un enlace.

Cuando adquirimos un dominio, el registrador nos adjudica sus servidores DNS por defecto. Gracias a ello podemos establecer los registros que necesitemos para apuntar a nuestra página web, crear subdominios o configurar el servidor de correo. En definitiva, conectar el dominio con la red.

En algunas ocasiones, podemos preferir modificar estos DNS para gestionarlos con otro proveedor. Esto no implica que el dominio se cambie de registrador, simplemente que tendremos que introducir los registros en este nuevo proveedor.

También nos encontramos con que el router tiene su propio DNS asignado para realizar esta conversión dominio-ip, aunque ese caso es diferente del que trata este artículo.

**Un registro es la manera de establecer la relación entre el dominio y la dirección IP.** Por ejemplo, para unir nuestro dominio con un servidor podemos usar los de tipo A(en los que se coloca una dirección IP) o CNAME(en los que se coloca un dominio) y, en el caso de que queramos configurar un servidor de correo, serán imprescindibles los registros MX.
También existirán otros problemas que pueden estar ocasionados por el cambio de servidor.
Cómo configurar un servidor DNS
En esta ocasión vamos a realizar un ejemplo en el que tenemos un dominio que está comprado en Namecheap y vamos a cambiar los servidores DNS, que actualmente son los de Namecheap, a DNSimple.
**DNSimple** es una aplicación especializada únicamente en la administración de DNS. Destacamos que, entre sus caracterísitcas, cuentan con una API REST para proyectos más complejos.
Para ello, debemos de acceder al panel de configuración del dominio en Namecheap. En él, navegamos hasta la opción Nameservers y con la opción Custom DNS establecida, colocaremos las direcciones DNS.
En el caso de DNSimple tendremos que establecer los siguientes
DNS: ns1.dnsimple.com, ns2.dnsimple.com, ns3.dnsimple.com y ns4.dnsimple.com.
Cuando se hagan efectivos los cambios de servidores se aplicarán los registros que hayamos añadido en nuestro nuevo servidor de DNS. En el caso de que no hayamos añadido registros, debemos de comenzar a hacerlo en DNSimple para que nuestro dominio actúe acorde con los que introduzcamos.
Generalmente, cuando se realiza un cambio de estas características, nos suelen proveer de dos direcciones de servidor DNS y es más que suficiente para hacer el cambio. Se pueden añadir más si en nuestro caso es requerido, como en el ejemplo de la imagen.

**¿Qué tipo de registros DNS existen y para qué sirven?**

El lugar donde se configuran las entradas DNS para cada dominio son los servidores de nombres. Los diferentes tipos de entradas de registro son:
**Registro A:** Este registro se utiliza para convertir nombres de host en direcciones IP.
**Registro CNAME:** Se utiliza para crear nombres de host adicionales (alias), y para crear diferentes servicios bajo una misma dirección IP.
**Registro NS:** indica los servidores de DNS autorizados para el dominio, es decir, a quién hay que preguntar para saber acerca de los registros de midominio.info.

**Registro MX:** Se utiliza para asociar un nombre de dominio a una lista de servidores de correo para la recepción de emails. Nos interesa si queremos realizar redirecciones de nuestro correo o utilizar nuestro correo electrónico con otro proveedor.
**Registro SPF:** define qué servidores están autorizados para enviar correo electrónico con nuestro dominio.

**Servicios de Internet - Wais : Servidores de Información de Largo Alcance**

- Son Bases de datos de documentos indexados.
- Basado en el Protocolo ANSI Z39.50.
- Pueden accederse a través de Telnet.
- Pueden accederse a través de WWW.
- Busca un tópico en todas las bases de datos disponibles en la red.
- El Servidor mantiene un índice global de todo el mundo lo que permite una búsqueda de alto detalle.

**Servicios de Internet - Gopher: Servicio de Distribución de Información**

- Gopher permite visualizar Directorios y bajar información.
- Posee una interfaz basada en menú y trabaja con los siguientes componentes.
    - Items :Directorios, Archivos de Texto, Una Imagen o Búsqueda.
    - Documento : Información incluida en un Item.
    - Bookmark: Señalador o entrada de menú asociada.
    - Server: Servidor de Documentos.

**Servicios de Internet - Archie: Servicio de Distribución de Información**
- Permite la localización de información y transferirlos utilizando FTP.
- También las búsquedas pueden encararse a través de Telnet o Correo Electrónico.
- Trabaja con Arquitectura Cliente-Servidor, necesita de la interfaz de cliente para el usuario.
- Descendiente del servicio Gopher.
- Protocolo que interpreta ficheros de una maquina remota.
- Puede interpretar Texto, , imágenes, sonidos y Secuencias de video.
- Para ello utiliza el HTML (Hypertext Markup Language) Mucha información en archivos pequeños.

**Servicios de Internet - WWW: WORLD WIDE WEB**
- Colección de Ficheros o Páginas WEB que incluyen información en forma de textos, gráficos, sonidos y video además de Links o Vínculos con otros ficheros.
- Los ficheros son identificados por un Localizador Universal de Ficheros (URL) que especifica el Protocolo de Transferencia, la dirección de Internet de la máquina y el Nombre del fichero .
- El visualizador (Navegador) es un programa interactivo que permite al usuario ver la información de la WWW. La información tiene objetos seleccionables para que el usuario vea otra información.
- La mayoría tiene una interfaz para apuntar y seleccionar elementos de Hipertexto/Hipermedia.

**Servicios de Internet FTP :Protocolo de Transferencia de Archivos**
- Aplicación que opera sobre TCP. (RFC 959).
- Se utiliza para Operaciones Básicas sobre Archivos y Transferencias en Redes de Área Extensa.

- Normalmente, para acceso a un Host solicita Nombre de Usuario y Contraseña.
- Las contraseñas las envía encriptadas: garantiza su privacidad (No Hay Encriptación de Datos) .
- Establece un canal Lógico entre ambos Host.
- Conexión de control :  Puerto 21
- Transferencia de los datos:Puerto 20 o superior a 1023

**Servicios de Internet TFTP :Protocolo de Trivial de Transferencia de Archivos**
- Diseñado para realizar transporte de archivos en forma sencilla: Variante del protocolo FTP.
- Prescinde de la conexión de control.
- Sin autenticaciones de seguridad.
- Se utiliza para anular la carga de trabajo de FTP. Es muy eficiente.
- Es usado normalmente dentro de una LAN.
- Es arriesgado su Uso en WAN.

**Servicios de Internet:**
**SFTP :Protocolo de Transferencia de Archivos Seguro**
**FTPS : Protocolo Seguro de Transferencia de Archivos**

- Protocolo de Transferencia de Archivos Seguro para conexiones remotas.
- Puede utilizar para la encripción de datos en el transporte:
- SSH en el Puerto 22 : SFTP
- SSL /TLS Puerto 990: FTPS
- Servicios que sincronizan Usuarios habilitados en AD/LDAP.
- Puede Trabajar con:
- Certificados SSL /X509
- Claves Publicas/Privadas SSH

**Servicios de Internet: SMTP :Protocolo Simple de Transferencia de Correo**
- Protocolo Simple de Transferencia de Correo.
- Protocolo orientado a la conexión.
- Basado en RFC 2821 y 822 (Formato de Mensajes).
- Utiliza los Puertos 25 y 587  para conectividad entre cliente y el servicio de transporte.
- Los Puertos 25, 465 y 475 son utilizados para el transporte al buzón de correos.
- Una transacción SMTP tiene 3 secuencias:
- MAIL:  Dirección Remitente/retorno.
- RCPT: Destinatario del mensaje.
- DATA: Envió de mensaje de texto.

**Servicios de Internet POP 3 :Protocolo de Oficina de Correo Versión 3**
- UA : Agente de Usuario (Usuario final)
- El UA utiliza POP 3 para comunicarse con el MTA.
- El UA Envía y recibe paquetes desde/hasta otros Servidores.
- No trabaja en tiempo Real (Carga de la Red).

**Servicios de InternetServidor (Relevador) de Correo  Electrónico**
- Configuración del Buzón de Correos
- Nombre de la Cuenta  pepe@gmail.com
- Alias.
- Fecha de Expiración.
- Nombre del archivo buzón de correos.

- Dirección de Forwardeo.

**Servicios de Internet: Webmail**
- Correo electrónico en sitio WEB
- Acceso a cuenta a través de Navegador WEB
- Administración de Correo electrónico a través de Internet.
- Espacio de Almacenamiento Limitado.
- Puede replicar con Servidor SMTP.
- Privacidad
    - Nombres de Usuario
    - Contraseña

**Servicio DHCP: Protocolo de Configuración Dinámica de Hosts**
- DHCP (Dynamic Host Configuration Protocol).
- Servicio de asignación automática de direcciones IP.
- Protocolo Cliente -Servidor - Asigna parámetros (Mascara de Subred, Puerta de enlace y Otros).
- Servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres.
- Mantiene estado de la posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

**Servicios de Internet:Telnet**
- Acceso en modo terminal remoto.
- Emulación de terminal en modo Texto.
- Característica Crítica de Un Sistema de Computación.
- Puede realizarse mediante conexión Telefónica.
- La sensación que percibe el usuario es que la sesión de terminal tiene lugar en la computadora local mientras que el Host Remoto procesa interactuando con la terminal local .

**Servicios de Internet: Secure Shell o SSH**
- Protocolo de red que permite el intercambio de datos utilizando un canal seguro entre dos dispositivos conectados en red.
- Acceso en modo terminal remoto.
- Emulación de terminal en modo Túnel.
- Puede realizarse mediante conexión Telefónica.
- La sensación que percibe el usuario es que la sesión de terminal tiene lugar en la computadora local mientras que el Host Remoto procesa interactuando con la terminal local.
- SSH utiliza la criptografía de clave pública para autenticar el ordenador remoto y permitir autenticar al usuario.
- SSH es utilizado habitualmente para entrar en una máquina remota y ejecutar comandos, sino que también soporta túneles, transmisión arbitraria en puertos.
- Un servidor SSH, por defecto, escucha en el puerto 22. Es utilizado para el establecimiento de conexiones a un demonio / conexiones remotas.
- Ambos están presentes comúnmente en la mayoría de sistemas operativos modernos.
- Autentifica los dos extremos de la conexión.
    - . – El servidor se autentica ante el cliente con un certificado
    - α. – El cliente se autentica ante el servidor
- Usuario y Password
- Certificados
- Encripta los datos intercambiados.

- No se transmiten usuarios ni Passwords en claro. La información transmitida viaja también encriptada
  .
  α.

**Servicios de Internet: Chat**

- Protocolo Mundial que se utiliza para comunicar intercambiando mensajes de texto en Internet (Ciberespacio).
- Por medio del Chat se realiza una comunicación en tiempo real para Intercambiar Mensajes que pueden Ser :
- Temáticos
- Segmentos de Población
- Libre acceso
- Restringidos

**Componentes de un Host de Internet**

**Encaminador Dinámico (Router) :**

- Permite el enrutamiento punto a punto de los paquetes entre la red y el nodo.
- Trabaja en la Capa Red (3).
- Se lo denomina fronterizo y utiliza el encaminamiento bajo búsqueda en tabla.
- Las tablas suelen ser dinámicas.
- Selecciona las rutas de los paquetes basados en estas rutas.
- El Proveedor del Servicio le asigna una Dirección IP.
- Examina los paquetes de datos entrantes y selecciona las ruta basada en la información en las tablas de enrutamiento.
- Utiliza Protocolos de Enrutamiento como por Ejemplo :
- RIP – IGRP = Interiores
- EGP – BGP = Exteriores
- Para el calculo de la mejor ruta utilizan distintas métricas como numero de saltos, retardos etc.

**Servidor de Acceso (ACCESS SERVER) :**

- Se Encarga de filtrar los Accesos Remotos Vía Módem a través de un Software de Seguridad que almacena a los accesos con su clave de autenticación.
- Normalmente lo componen una cantidad de módems en Línea conectados a accesos telefónicos unitarios o rotativos.
- Se le asigna un Rango de Direcciones IP Fijas que le permita asignar a cada usuario una Dirección Dinámica en el momento de la conexión.

**Radius**
**Remote Authentication Dial-In User Service**

- Software de Administración y control para Servidores de Acceso Remoto (RAS).
- Autentica las acciones de acceso remoto sobre los RAS mediante las llamadas, protocolos y filtros.
- Soporta la Seguridad Adicional de Los Servidores Proxy
- Mantiene una Base de Datos con el Nombre de Usuario (LOGIN) y su Password.
- Simplifica y Consolida la Administración de Usuarios de Acceso Remoto al Nodo
- Facilita el Seguimiento y Documentación de Accesos Remotos.
- Administración y Configuración bajo Entorno Windows.
- Permiten configuración, comunicación y Autenticación en VPNs usando L2TP.
    - LDAP LAYER 2 TUNNELING PROTOCOL
        - Protocolo de Tunneling para Usuarios Remotos.
        - De Acuerdo al Usuario y configuración dentro de la VPN los paquetes son dirigidos aplicando Tunnelling en forma Dinámica en el momento de la Conexión Dial-UP

**Firewall**

- Servidor con Interfaz de Red Multipuerto que limita los Servicios/Procesos con respecto a nuestra red con respeto al resto de los componentes de Internet.
- Habilita/Deshabita servicios en forma parcial/global de acuerdo a las políticas establecidas en la Administración del Nodo:
- EJ. FTP , Telnet , Chat, Etc.
- Servidor especifico compuesto por Hardware y Software que actúa como barrera de seguridad de los recursos Informáticos de nuestra organización.
- Barrera de Seguridad entre la Intranet y la Extranet.

- Se encuentra ubicado inmediatamente después del Router Fronterizo.
- Puede albergar el DNS Externo.
- La regla básica es asegurar que todas las comunicaciones entre la Extranet y la Intranet se realicen conformes a las políticas de seguridad de la organización o corporación.
- Técnicas Utilizadas
- Filtros a nivel paquete
- Filtros a nivel circuito
- Filtros a nivel aplicación
- Filtros dinámico a nivel paquete
- La regla básica es asegurar que todas las comunicaciones entre la Extranet y la Intranet se realicen conformes a las políticas de seguridad de la organización o corporación.
- Técnicas Utilizadas
    - Filtros a nivel paquete:
        Cada paquete que entra o sale de la red es inspeccionado y lo acepta o rechaza basándose en las reglas definidas por el usuario. El filtrado de paquetes es difícil de configurar. Reglas para rechazar o aceptar un paquete :
            Si no se encuentra una regla que aplicar al paquete, el paquete es rechazado.
            Si se encuentra una regla que aplicar al paquete, y la regla permite el paso, se establece la comunicación.
            Si se encuentra una regla que aplicar al paquete, y la regla rechaza el paso, el paquete es rechazado.
    - Filtros a nivel circuito:
        Valida que los paquetes pertenezcan ya sea a una solicitud de conexión o bien a una conexión entre dos computadoras.
        Aplica mecanismos de seguridad cuando una conexión TCP o UDP es establecida. Una vez que la conexión se establece, los paquetes pueden ir y venir entre las computadoras sin tener que ser revisados cada vez.El firewall mantiene una tabla de conexiones válidas y permite que los paquetes de la red pasen a través de ella si corresponden a algún registro de la tabla. Una vez terminada la conexión, la tabla se borra y la transmisión de información entre las dos computadoras se cierra.
    - Filtros a nivel aplicación:
        Examina la información de todos los paquetes de la red y mantiene el estado de la conexión y la secuencia de la información. En este tipo de tecnología también se puede validar claves de acceso y algunos tipos de solicitudes de servicios.
        La mayoría de estos tipos de firewalls requieren software especializado y servicios Proxy.
        Un servicio proxy puede incrementar el control al acceso, realizar chequeos detallados a los datos y generar auditorias sobre la información que se transmite
    - Filtros dinámico a nivel paquete:
        Permite modificaciones a las reglas de seguridad sobre la marcha. En la práctica, se utilizan dos o mas técnicas para configurar el firewall.

- Un Firewall suele tener un mínimo de tres Zonas, aunque las primeras implementaciones sólo incluían dos.
    - Interior
    - Exterior
    - DMZ (zona desmilitarizada)
- Dispositivos de defensa perimetral: Separa redes.

- Filtra trafico dependiendo de reglas predefinidas.
- No protege de ataques internos.
- No protege de accesos no autorizados.
- No protege de todos los ataques dañinos
- Conexiones de Intranet a Extranet
- Correo Electrónico
- FTP
- SSH
- Telnet
- Conexiones de Prueba desde el monitor de Red.
- Pruebas de Conectividad (Ping)
- Pruebas de Conectividad con Proxy y Otros
- Exploración de Redes de Terceras Partes (Extranet)
- IRC/ICQ (Chat).
- Real Audio (Entrantes y Salientes).

**Proxy Server**

- Gestionador de comunicaciones entre Internet e Intranet de una LAN.
- Proporciona Protección a nuestra LAN utilizando EL SOFTWARE N.A.T. (Administrador de Traducciones de Red).
- Proporciona Restricciones de Servicios parciales  a nivel Individual.
- Aislamiento completo de Nuestra Intranet
- Puede Mantener un Cache Configurable (Activo/Pasivo) de los datos más solicitados o recientemente recuperados para mejorar la performance de respuesta ante solicitudes.
- Posee un Direccionador asociado al NAT.
- Asocia Puertos (8080-80)44Peticiones del usuario
- El Servicio se basa en HTTP pero admite
- FTP - Gopher - SSL (Datos Encriptados)

**LDAP SERVER**

Microsoft Active Directory
OpenLDAP
Sun Java System Directory Server
IBM Tivoli Directory Server
Apache Directory Server
Apple Open Directory

- 
- Servicio de Internet, que implementa un  directorio (metadirectorio) Jerárquico y Distribuido.
- Repositorio centralizado de usuarios, aplicaciones y recursos.
- Define permisos, configurados por el administrador para permitir el acceso a ciertos usuarios a la base de datos, y mantener información en privado.
- Control de Acceso a Recursos a través de reglas de provisionamiento .
- Uso de canales seguros para comunicarse con el cliente.
- Tres tipos de autenticación: No autenticación, Autenticación Simple y Usando SASL o SSL/TLS.

**Web Server**

- Colección de Ficheros o Páginas WEB que incluyen información  en forma de textos, gráficos, sonidos y video además de Links o Vínculos con otros ficheros.
- Dependiendo de la configuración del Proxy o Firewall puede ser :

- Interno
- Externo o Institucional
- Acepta peticiones HTTP desde clientes web, y envía la información solicitada.
- Almacena información detallada acerca de las peticiones de los clientes y las respuestas del servidor.
- Funcionalidades: Autenticación, Manejo de Contenido Estático y Dinámico, HTTPS, Compresión, Limitación de Ancho de Banda

**Mail Server o Servidor de correo**
- SMTP :Protocolo Simple de Transferencia de Correo
- MTA : Agente de Transferencia de Correo.
    - Envía y recibe paquetes desde/hasta otros servidores de correo.
    - Proporciona una interfaz para las aplicaciones accedan al sistema de correo.
    - Proporciona a los usuarios buzones de correo dotados de una dirección.

**Webmail**
- Correo electrónico en sitio WEB
- Acceso a cuenta a través de Navegador WEB
- Administración de Correo electrónico a través de Internet.
- Espacio de Almacenamiento Limitado.
- Puede replicar con Servidor SMTP.
- Privacidad
- Nombres de Usuario
- Contraseña

**Antivirus**
- Programa de chequeo de archivos de tráfico Entrante/Saliente trabajando sobre los Servicios :
- FTP
- HTTP
- MAIL

**Monitor Web**

BLOQUEA el acceso de usuarios o grupos a sitios web no productivos o no aceptados por las políticas de la empresa. El administrador define la política seleccionando aquellas categorías que son aceptables o no. Utilizan un motor de filtrado de sitios web de Cyber Patrol. Esto le otorga la posibilidad de filtrar cientos de miles de sitios web y su actualización es automática.

REGISTRA en detalle todo el tráfico web de la empresa. Guarda registro de los accesos a Internet de los usuarios y ofrece gráficos con información estadística para analizar y tomar decisiones. Estos reportes pueden configurarse en función de las necesidades de la empresa, y pueden generarse bajo demanda o en forma automática.

ADMINISTRA el uso del tráfico web configurando límites de tiempo y volúmen de información recibida por día, semana o mes. Pueden definirse cuotas especiales para usuarios particulares o grupos.

VERIFICA el tráfico de e-commerce ofreciendo mecanismos de rechazo automático de sitios web no válidos. Este sistema de verificación trabaja sobre las certificaciones digitales de las conexiones SSL. De esta forma se asegura que los servidores SSL al que los usuarios se

conectan son todavía válidos. Terminará aquellas conexiones a servidores no validados previniendo cualquier problema con las transacciones de los usuarios.

ALERTA a los administradores ante la presencia de eventos especiales relacionados con el uso del servicio web. Utilizando esta funcionalidad, el administrador puede definir aquellos eventos que considere no usuales o especiales. WebManager enviará automáticamente mensajes de correo electrónico con la información detallada del evento.

PROTEGE todo el tráfico web (HTTP) previniendo el ingreso a la red de virus y códigos maliciosos conocidos de Java y ActiveX. La tecnología de los motores de rastreo de 32 bits detectan miles y miles de virus y reconocen más de 16 formatos de compresión y codificación de archivos.

Control de la navegación por tiempo y ancho de banda, así como clasificación de sitios web y filtrado de URL para incrementar la productividad y la seguridad

Filtrado según la reputación del sitio web
Esperar a que un sitio web sea clasificado como peligroso puede ser un juego arriesgado.
La protección proactiva de las amenazas de Internet puede salvarle de ser infectado y por lo tanto de consecuencias potencialmente devastadoras.
El Monitor utiliza ahora filtrado basado en la reputación, que utiliza la puntuación de reputación de un sitio web o dirección IP para predecir el riesgo de seguridad implicado con la visita de ese sitio web. La reputación de un sitio web se calcula mediante cientos de indicadores que incluyen de infecciones, edad de establecimiento, popularidad, contenido y muchos otros;  a continuación se le otorga una puntuación de 1 (alto riesgo) a 100 (confiable).
El filtrado por reputación del sitio web agrega una capa proactiva de seguridad así como directivas flexibles de acceso a Internet. Por ejemplo, puede habilitar el acceso a sitios de "Compras" proporcionando simultáneamente protección mediante el bloqueo del acceso a sitios de compras con baja reputación.

-Directivas para bloquear el streaming multimedia
Como la difusión de audio y video se ha convertido en parte integral de muchos sitios web, el Monitor le permite ahorrar ancho de banda bloqueando el streaming.
El contenido de audio y video es una rutina en noticias, entretenimiento y deportes, y puede crear rápidamente un cuello de botella especialmente en horas punta o durante eventos de interés.
Las directivas de bloqueo de streaming le permiten habilitar el acceso a sitios web que estén proporcionando el medio y bloquear a la vez la difusión en curso, asegurando que se alcanza un medio positivo.
Esta característica también incluye un motor de actualización automática para poder distribuir nuevas firmas según son descubiertas.

Bloqueo ligero - Avisar y permitir
Permita a los usuarios de confianza superar el bloqueo después de avisarlos de que una URL está en disonancia con la directiva de la empresas; poniendo en práctica el concepto de auto vigilancia.

Registro de Actividad de la Monitorización de Acceso
Vea el camino exacto que ha realizado un usuario, incluyendo la fecha y hora en que se visitó un sitio específico.
Ofrece una opción para ver un listado de sitios/páginas a los se ha accedido junto con la fecha

y hora de acceso.

**Monitor de Correo Electrónico (E-Manager)**

- Filtro de Contenidos : Para material confidencial o inapropiado.
- Filtro de Atacheados
- Filtro SPAM : Bloqueador de E-Mails no solicitados.
- Administración de EMAILS : Monitor de  Patrones de Trafico.

**Bandwindth Manager (B-Manager)Monitor de Ancho de Banda**

- Sistema de Maquina Virtual utilizado para Administrar Ancho de Banda.
- Trabaja Sobre el canal adjudicando ancho de banda de acuerdo a las Políticas de Uso.
- Editor Integrado de Políticas de Uso del Canal.
- Adjudica en Forma General o Particular a usuarios conectados.
- Trabaja sobre Algún Servidor del Nodo Internet o del ISP.
- Monitoreo Gráfico en Tiempo Real.
- Sus Políticas son complementarias a las de un Firewall.
- El uso apropiado evita la congestión del canal cortando procesos que ocupan mucho Ancho de Banda.
- Puede operar en combinación con VPNs, y NAT en caso de Tener Intranets.

**Diodo de datos**
Dispositivo hardware (no existe firmware como el caso de los firewalls) que separa/protege dos redes asegurando la unidireccionalidad en el flujo de información asegurando que la información de una red llegue a otra red (pero no viceversa).
Son dispositivos de protección de perímetro utilizados habitualmente en interconexiones entre sistemas con diferentes categorías o políticas de seguridad.
Su funcionalidad principal es la de separar redes, permitiendo el flujo de información en un único sentido y haciendo inviable la transmisión de información en el sentido opuesto. Para ello, proporcionan las siguientes funciones básicas de seguridad:

a) Transmisión del tráfico de red de manera unidireccional, para lo que se deberá elegir si se desea que el sentido de la comunicación sea de entrada hacia, o salida desde, la red interna.

b) Capacidad de interpretar protocolos bidireccionales, “romperlos” y convertirlos en unidireccionales para luego presentarlos en la segunda red de nuevo como bidireccionales.

La protección tiene lugar a diferentes niveles dentro de las capas definidas por el modelo OSI (Open Systems Interconnection), fundamentalmente a nivel de capa física limitando el flujo de información en el sentido autorizado y haciendo inviable la transmisión de señales de comunicación en el opuesto, pero también a nivel de las capas de red, transporte y/o aplicación para habilitar el uso de protocolos bidireccionales.

Procesador Front-End (FEP): Comunicaciones Unificadas

- Plataforma de comunicaciones de presencia, mensajería instantánea, conferencia y voz para organizaciones distribuidas en WAN.
- Sobre una base de usuarios (Directorio) integra mensajes existentes en la organización y la infraestructura de telefonía.
- Permite a los usuarios realizar, recibir, reenviar o redireccionar las llamadas directamente desde su PC, teléfono fijo o teléfono móvil.
- Utilizan para validar usuarios certificado digital.
- Mensajería Instantánea y presencia ] Comunicación en tiempo real de persona a persona mediante texto, voz y video, a través de una organización.
- Conferencias Web
- E-mail y calendarios compartidos y contactos
- E-Manager (Protección/preservación e-mail).
    - Filtrado (Spam)
    - Archivo (backup)
    - Continuidad (Replicando)
    - Cifrado (TLS)

**Petición :** Es la simple acción de solicitud de datos que realiza el cliente web sobre el servidor web.

**Sesión de Web :** Es el acceso de los usuarios con intercambio de información con los mismos. En el intercambio el usuario accede y modifica esa información de acuerdo a su perfil dentro de dicho sitio.

**WORLD WIDE WEB - WWW:**

**Balanceo de Carga**

- Es una técnica de balanceo de solicitud de pedidos para optimizar el flujo de Información y la carga de procesamiento.

- Los Pedidos dejan de ser asignados a un único servidor para ser distribuidos en varios servidores ante las peticiones y/o sesiones Web.
- Permite preconfigurar redistribución de solicitudes ante tareas de mantenimiento o contingencia por caídas (redundancia).
- Asegurar una distribución de carga pareja para brindar un servicio mas rápido.
- Existen varios tipos de balanceo:
    - **RR – DNS (Round Robin DNS):**
      Se aplica una técnica de Round Robin sobre un servidor DNS particular que determina a que servidor asignara la petición, en función de su disponibilidad.
      Estas asignaciones pueden realizarse a partir de dos características a analizar:
      - Por sesión: El servidor asigna la conexión de un usuario en un momento determinado a una dirección IP (la que toque en el RR) y mantiene la asignación hasta que el usuario finalice la sesión de http hacia el mismo.
      - Por IP: El servidor DNS puede tener asignado el método de RR para direccionar la solicitud en función de la ubicación geográfica de la dirección IP origen, para así mejorar los tiempos de transmisión y evitar “hops” innecesarios.

    - **Reverse Proxy Server:**
      Como su nombre lo indica, su funcionamiento es inverso al concepto existente de servidor proxy, pues realiza solicitudes de una red no segura a una que si lo es.
      Basan su performance en un método llamado: “Cache de asignación”, donde se mantiene un Log de “a quien le dieron” la conexión anterior.-
      Pueden ser configurados para que mantengan un monitoreo de la cantidad de sesiones que están atendiendo cada uno de sus servidores para ver a cual asignar la próxima petición.
    - Servicios Avanzados de Redes y Clustering.
    - Routers de Capa 4

- **Ventajas :**
    - Fácil Implementación.
    - Configuración Adecuada del DNS.
    - Persistencia y redundancia en la disponibilidad de los servicios.
    - Evita ataques directos de tipo DDoS sobre los servidores web.
- **Desventajas :**
    - Se requiere equipamiento extra, o al menos un procesador e interfaz de red asignados de forma exclusiva.
    - Puede sufrir ataque DDoS al servicio DNS.

**Balanceo en Peticiones – Hardware**

- Switch por contenido :
    - Análisis de contenido de paquetes
    - Redireccionan pedidos dentro del ambiente LAN
    - Utilizan Capas Altas del Protocolo TCP/IP
    - (4 a 7)
    - “Conmutación Basada en Contenidos” – Poseen “Reglas de Filtrado básicas” pudiéndose definir otras manualmente.

- Asumen la función de Directores Locales y se configuran en par (Primario – Secundario) para prever caídas o contingencias.
- Se puede controlar ancho de banda usado por cliente (estadísticas de tiempos).
- Redefinir Sub-Granjas de acuerdo a la aplicación.
- Analisis sobre puertos TCP, URLs, HTTP Cabecera y Cookies, SSL Sessión ID, etc.
  -
  -

**Balanceo en Peticiones – Software**

- Aplicación Bajo S.O. :
  - Software embebido.
  - Nodos en Clustering (una subred).
  - Filtro Instalado en el servidor de WEB.
  - Cuando el cluster es muy numeroso (Subgranja) se lo combina con un DNS Local aplicando RR-DNS.
  - Se instalan en par - Contingencia ante caídas.
  - Algunos trabajan con “Inundación de Red”.