# Resumen Examen 1 Redes Avanzado

Capa de seguridad de Google

1. Los limites de la propiedad o perímetros físicos: Son medidas físicas como cercas, muros y sistemas de vigilancia
2. Perímetros seguros: Puerta de entrada principal, cámaras, patrullas de vigilancia
3. Acceso al edificio: Tarjeta de acceso, escaneo de ojos (iris)
4. Monitoreo del centro de datos
5. Niveles de acceso del centro de datos (Autorización)
6. Destrucción de medios almacenados en desuso

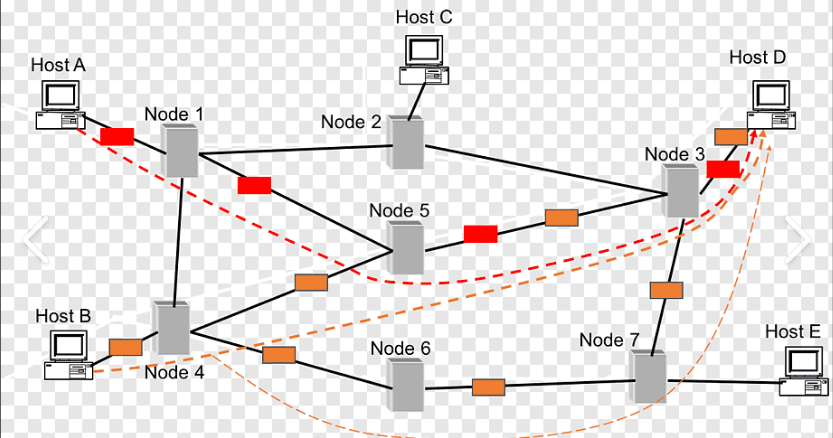
Tolerancia a fallas, escalabilidad, calidad y seguridad

**Tolerancia a fallas**: Una red que tolera fallas es que limita los dispositivos afectados para que no sea una falla total, pudiendo recuperaciones rápidas. Si una ruta falla, se enviarán por otra funcional, teniendo **múltiples caminos**. Teniendo muchos caminos la hace **redundante (significa duplicación o repetición del proceso).** Esto hace que sea mas **confiable** y **disponible**

Diagrama

Descripción generada automáticamente

La **conmutación de paquetes** **es dividir los datos en pequeños paquetes**, tienen información de control, dirección de origen y destino. Usan diferentes rutas estos paquetes, pero buscan llegar al mismo destino



**Escalabilidad**: Para que sea escalable, debe tener el poder de **admitir nuevas opciones sin degradar el rendimiento que ya estaba antes**. Agregar sin modificar lo anterior. Al seguir estándares con protocolos aceptados los hacen escalables

Diagrama

Descripción generada automáticamente

**Calidad del Servicio (Quality of Service):** **Conjunto de técnicas y mecanismo para mejorar el rendimiento sin tener interrupciones en la red**. Intentan reducir al mínimo las congestiones de red (Cuando la demanda supera las capacidades)

* Para mejorar la calidad, se hacen:
* Priorizaciones de tráfico (Cual es más importante que otro)
* Controlando la gestión (Limitar tasas de transferencia con flujo de datos)
* Garantizar ancho de banda (Reserva un ancho de banda como plan B)
* Controlando latencias y jitter para aplicaciones en vivo (Como llamadas)
* Gestionar errores y perdidas de paquete (Minimizar)

**Seguridad de la Red:** Seguridad en **infraestructura de red** y seguridad de la información (Como login para acceder), como también **seguridad física** (Robo, desastres ambientales, etc). Se necesita ser:

* **Confidencial**: Que solo el emisor y destinatario tengan autorización de acceder a los datos
* **Integro**: Que la información no se va a alterar
* **Disponible**: Que se pueda acceder en forma confiable y cuando quiera al ser un usuario autorizado

HUB, SWITCH, MAC ADDRESS Y ARP

**HUB**: Es de la **capa Física**. Es un equipo que permite conectar entre si equipos y retransfiere los datos desde cualquiera de los conectados (**Básicamente un** **repetidor**). No realiza procesamientos o filtrado de datos (Cualquiera conectado al HUB podría ver los datos, **poca seguridad**). Antes se usaba para red LAN (Ya no por tener **muchas colisiones**)

Diagrama

Descripción generada automáticamente

**SWITCH: Capa de Enlace de datos. Es como el HUB pero mejor**. **Toma decisiones** dependiendo las direcciones **MAC.** Significa que al **mandar datos solo del emisor al receptor** (No como el HUB que se los mandaba a todos). Se administran por puerto y/o usuario con clave. Todo esto hace que sea mas seguro, mejora la transferencia y rendimiento

Imagen que contiene guitarra

Descripción generada automáticamente

**MAC Address (Media Access control):** Es un identificador de 48 bits (6 bytes) para dispositivos de red. Es la tarjeta de red para el Switch, no se puede cambiar en general. Cada Mac es **única**. Entonces el Switch no busca IP, sino MACs

Diagrama

Descripción generada automáticamente con confianza media

**ARP (Address Resolution Protocol):** Es un protocolo de comunicación que asocia IP con direcciones MAC en una red local. **Básicamente convierte el IP a una dirección física tal como dirección de Ethernet.** Cuando se envía datos de un dispositivo a otro en la misma red se usa ARP para tener la dirección MAC de esa IP

Redundancia en componentes de Red (HA)

**La redundancia en HA (Alta disponibilidad)**: **Es una estrategia** de diseño que busca minimizar tiempos inactivos y garantiza continuidad operaria de la red haciendo **duplicaciones de componentes críticos** (Routers, Switchers, firewalls, servidores). **Se multiplican por si en caso de fallar uno, el otro pueda tomar el control sin interrumpir el servicio.** Al estar todos conectados están sincronizados también teniendo mecanismos de detección de fallos para esas soluciones rápidas y automáticas

Imagen de ejemplo:

Imagen que contiene medidor

Descripción generada automáticamenteImagen que contiene computadora

Descripción generada automáticamente Tabla

Descripción generada automáticamente

¿Que es la redundancia?

En sistemas se refiere a procesos, componentes o mecanismos que se agregan en un sistema para aumentar fiabilidad, disponibilidad y tolerancia a fallos. **Es tener un respaldo o alternativa.** (Un ejemplo la topología red)

* **Redundancia activa**: Todos los componentes están activos y operando al mismo tiempo, compartiendo la carga de trabajo. Si un componente falla los demás se harán completamente cargo
* **Redundancia pasiva**: Los componentes redundantes (Los que se repiten) están en espera o un estado de reserva hasta que se los necesiten. Entonces solo el componente principal esta activo, si ese activo falla, se “despertaran” el componente en espera y tomara su trabajo

Por otro lado, esta

* **Redundancia Hardware**: Duplicar componentes físicos de un sistema
* **Redundancia Geográfica**: Duplicar el centro de datos en otra ubicación geográfica del mundo

**Diferencia entre HA y Redundancia:** La redundancia interconecta Data Centers en caso de fallas y no perder tiempo. Mientras que HA es la capacidad de tener operando un sistema sin interrupciones (Básicamente van de la mano en su objetivo)

Imagen de alta disponibilidad con redundancia:  
Diagrama

Descripción generada automáticamente

Conectividad a la nube: Se refiere a la capacidad de acceder a utilizar recursos informáticos, almacenamiento, apps y servicios alojados en la nube, en lugar de depender de recursos locales.

Los principales beneficio son:

* Seguridad ya que la información no esta expuesta al internet publico
* Tener un ancho de banda asegurado para carga y descarga de información
* QoS: Puedes establecer prioridad al trafico

Nube privada VS Nube Publica

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Internet de alta capacidad en Data center: Básicamente son redes de fibra óptica de alta capacidad, con mantenimiento e infraestructura estable. Teniendo MPLS (Multiprotocol Label Switching) (Conmutación de etiquetas multiprotocolo), que es un estándar (Como una técnica) para transmitir datos bajo etiquetas, mejorando el flujo de trabajo en Internet. Administrando en redes WAN por prioridad

Interfaz de usuario gráfica, Sitio web

Descripción generada automáticamente

Comunicación de Host to Host

**OSI** (Open System Interconnection)

Es una normativa formada por **7 capas** que definen **diferentes fases por las que pasan los datos para viajar de un dispositivo a otro sobre la red.** Del 1984 por ISO

Interfaz de usuario gráfica

Descripción generada automáticamente

1. **Aplicación**: Es la interfaz que ve el usuario de forma directa (**HTTP**, FTP, SMTP, H323), usa PDU **(Protocol Data Unit)** de **datos**
2. **Presentación**: Convierte los datos para comunicarlo entre aplicaciones, restructurándolo y modificando la sintaxis (**ASCII**, JPEG, QUICKTIME), PDU de **datos**
3. **Sesión**: Establece, mantiene y termina la conexión entre capas de forma sincronizada, PDU de **datos**
4. **Transporte**: Entrega los datos de manera confiable y ordenada por conexión (**TCP**) o sin conexión (**UDP**). Además de corregir errores de transmisión, establece, mantiene, controla y termina circuitos virtuales. PDU de **segmento**
5. **Capa de Red**: **Enruta** y direcciona los paquetes por la red. Mira la mejor ruta para enviarlos por la red. Los **firewalls** y **router** actúan en esta capa (**IP**, IS-IS, RIP, DHCP, **ARP**). PDU de **paquete**
6. **Enlace de datos**: Se encarga de que la trasferencia será confiable entre las capas, controla acceso **MAC** y **LLC** (El direccionamiento físico)**.** PDU de **trama**
7. **Capa Física**: Transmisión física en PDU de **bits**, como con cables, fibra óptica, señales de radio, etc.

Diagrama, Escala de tiempo

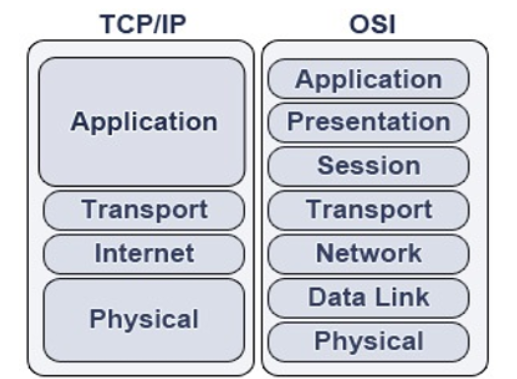
Descripción generada automáticamente

Primero que nada, un **estándar** **es una serie de reglas y criterios establecidos para mantener un orden entre una comunidad o grupo**. Una regulación de procedimientos. Estos surgen para mantener orden y ser interoperables entre todos, siendo así compatible.

Encapsulación de datos y PDU (Unidad de Datos de Protocolo)

Básicamente la encapsulación de datos se refiere al **proceso de agregar información adicional a los datos originales a medida que se transmiten en una red (Envolviéndolo con otra estructura de información).** Esa información se usa para que los datos sean enviados mas efectivo y que lleguen correctamente, por eso usan el protocolo PDU

Internet es una red basada en TCP/IP, un modelo en el cual se trabaja el encapsulamiento (Al igual que OSI)

Un ejemplo de encapsulación: Al mandar un mensaje de “Hola” no puede ser enviado así al natural en la red, necesita mas datos para enviarse exitosamente. Piénsalo como una carta escrita a mano para alguien, no solo mandas un papel que dice “Hola”, necesita estar “encapsulado” para eso le agregamos un sobre con tu nombre como prueba de que eres vos y al destinatario a quien le llegara, y la dirección a donde se va a mandar específicamente y la compañía de envio se encarga del transporte seguro a su destino

Repaso de las instancias PDU:

Diagrama

Descripción generada automáticamente

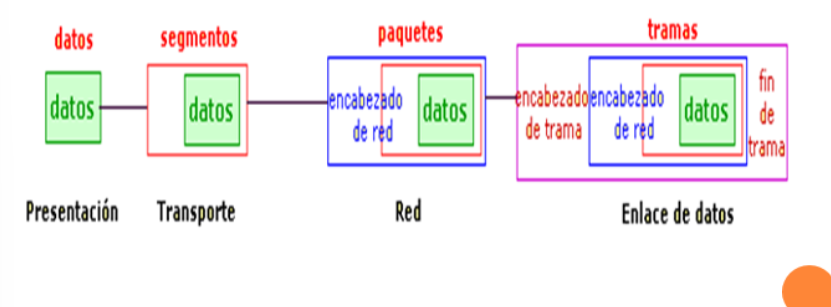
Cada capa agrega su encabezado al PDU (header), con información especifica para su restro

Tabla

Descripción generada automáticamente

Cada capa encapsula así:

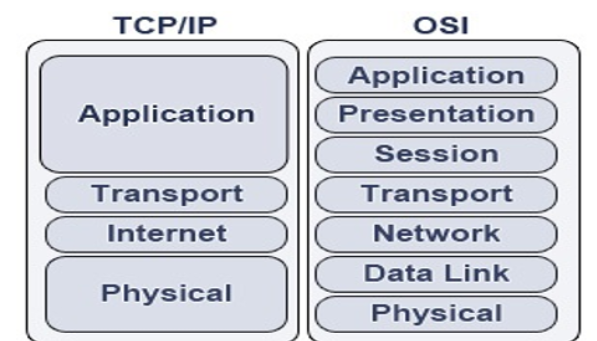
1. **Aplicación**: Encapsula en datos con encabezando **(header)** con HTTP, SMTP, FTP
2. **Presentación**: Cifra y codifica los datos para que sean interoperables en sistemas heterogéneos (ASCII por ejemplo)
3. **Sesión**: No tiene uno específico para los datos
4. **Transporte**: Encapsula los datos en **segmentos** dependiendo el protocolo
5. **Capa de Red:** Encapsula en paquetes, agregando al encabezado el **IP origen y destino, información de enrutamiento y control de red**
6. **Enlace de datos**: Encapsula datos en **tramas**, agrega al encabezado dirección **MAC de origen y destino, detección de errores y flujos**
7. **Capa física**: No encapsula datos en sentido tradicional, trasfiere en **bits**



Interfaz de usuario gráfica, Diagrama

Descripción generada automáticamente

Comparación entre modelo OSI y TCP/IP



Se puede describir en diferente agrupación entre cada una, con subdivisiones entre capas. Entonces como se ve **TCP/IP agrupa en 4 capas**. (OSI se usa para aprender a profundidad, pero se usa mas TCP/IP en redes modernas). **Entonces combina la capa de Aplicación, Presentación y sesión del modelo OSI en una sola capa llamada Aplicación, y también combina la capa enlace y física del modelo OSI en una sola capa llamada Física**

* En la capa 1 de TCP/IP (Fisica), no especifica los protocolos que utiliza al trasmitir, solo describe la entrega desde la capa de Red (Internet) con los protocolos.
* En OSI la capa 1 y 2 pasan por procedimientos para acceder a medios para enviar datos por la red

Son similares en la capa 3 y 4 (Red y transporte) de OSI con la capa 2 y 3 (Red y transporte) de TCP/IP: La Red se usa para discutir y documentar para enrutar mensajes, usando la **IP (Protocolo de Internet)** que es de la suite de TCP/IP

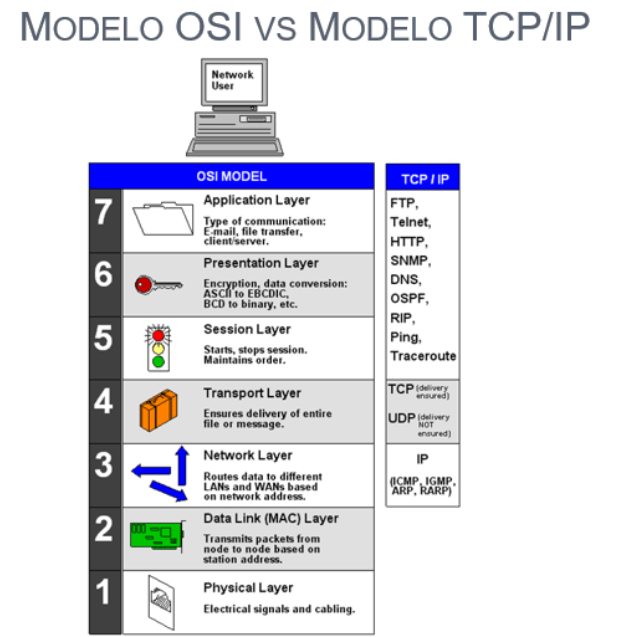
La capa transporte (OSI), administra las conversaciones entre los hots de origen y destino. Esta capa el protocolo TCP/IP, TCP y UDP proporcionan la funcionalidad necesaria

* **UDP**: Es protocolo orientado a **SIN CONEXIÓN**, o sea que se puede enviar algo de X a Y sin tener la conexión, se enviara sin tener la confirmación
* **TCP**: Es protocolo orientado **CON CONEXIÓN**, o sea que se puede enviar algo de X a Y teniendo conexión, se enviara una confirmación de llegada, con controles CRC. Si hay datos corruptos, TCP permite que el destinatario solicite otra emisión de los datos. **TCP envía el tráfico en forma de segmentos y utiliza números en secuencia para reordenarlos en el destino**

La capa 4 (Aplicación) de TCP/IP tiene varios protocolos para funciones especificas para el usuario final, seria las capas 5, 6 y 7 (Sesión, presentación y aplicación) del OSI

**Modelo TCP/IP:**

* **Aplicación**: Representa los datos al usuario directamente
* **Transporte**: Admite comunicación entre dispositivos en distintas redes
* **Red o Internet:** Determina la mejor ruta a través de la red
* **Acceso a la red:** Controla hardware y medios que forman la red



Es necesario usar TCP/IP para estandarizar tecnologías y normas para compartir recursos

Capa de red del modelo OSI

Profundiza la información de esta capa

Por lo general **el Router desencapsula** **la trama** para leer la dirección del host destino en el encabezado del paquete. El Router utiliza la identificación de esta red para **dar la mejor rutar**, el **Router vuelve a encapsular el paquete** **en una nueva trama** agregando el tiempo de vida (**TTL**) en su encabezado y lo manda a el dispositivo destino. Cuando llega la trama y encabezados **se eliminan y los datos se suben a la Capa 4** (Transporte)

Diagrama

Descripción generada automáticamente

Dynamic Host Configuration Protocol (DHCP)

Es un protocolo de red para asignar de manera dinámica las direcciones IP y otra información, es mas utilizado en redes locales LAN, como también en servidores de internet ISP. Puerto 67/UDP (Servidor), 68/UDP (Cliente)

Diagrama, Esquemático

Descripción generada automáticamenteSecuencia del funcionamiento:

Discovery: Solicitud realizada por cliente para encontrar un servidor activo DHCP que le asigne una dirección IP como mascara de red

Offer: Respuesta de un servidor DHCP al cliente, involucra dirección MAC para representar transferencia segura

Request: El cliente selecciona la configuración recibida, otra vez solicita dirección IP especifica

Acknowledge: Se inicia la fase de reconocimiento del envío de paquete con los datos solicitados. Incluye el paquete la duración de concesión e información que el cliente quiso, ya paso por configuraciones TCP/IP, reconoce la solicitud y la envía

# Cosas a tener en cuenta

¿Que es la comunicación?

La comunicación en nuestra vida cotidiana tiene diferentes formas y existe en muchos entornos. Tenemos diferentes expectativas según si estamos conversando por Internet o participando de una entrevista de trabajo. Cada situación tiene su comportamiento y estilo correspondiente

La comunicación debe tener:

* + Emisor y receptor identificados,
  + Método de comunicación consensuado (cara a cara, teléfono, carta, fotografía)
  + Idioma y gramática comunes
  + Velocidad y puntualidad en la entrega
  + Requisitos de confirmación o acuse de recibo.

Comunicación a través de redes

* reglas y acuerdos para regular cómo se envían, redireccionan, reciben e interpretan los mensajes,
* los mensajes o unidades de información que viajan de un dispositivo a otro,
* una forma de interconectar esos dispositivos, un medio que puede transportar los mensajes de un
* dispositivo a otro, y
* los dispositivos de la red que cambian mensajes entre sí.

Provisión de seguridad de red

* Algunas de las consecuencias de la ruptura en la seguridad de la red son:
* interrupciones de red que impiden la realización de comunicaciones y de transacciones, con la consecuente
* pérdida de negocios,
* mal direccionamiento y pérdida de fondos personales o comerciales,
* propiedad intelectual de la empresa (ideas de investigación, patentes o diseños) que son robados y utilizados
* por la competencia, o
* detalles de contratos con clientes que se divulgan a los competidores o son hechos públicos, generando una
* pérdida de confianza del mercado de la industria.

LAN Y WAN

Una red LAN (Local Area Network) y una red WAN (Wide Area Network) son dos tipos de redes de computadoras que se utilizan en diferentes contextos y para diferentes propósitos.

Diagrama

Descripción generada automáticamente