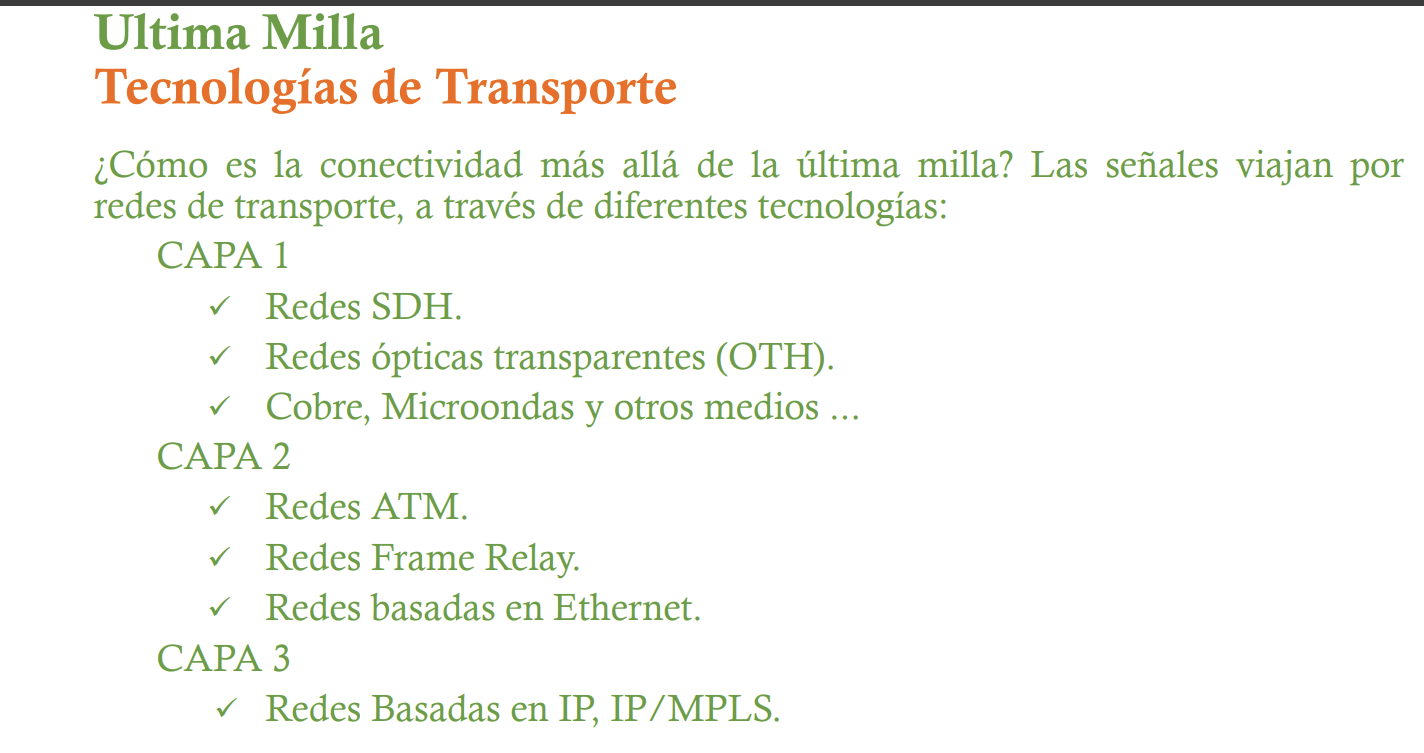
**RESUMEN TEORIA**

****

### Redes de Acceso por Par de Cobre (xDSL)

Las tecnologías xDSL (Digital Subscriber Line) permiten la transmisión de información digital a través de los pares de cobre de la red telefónica tradicional (PSTN). Antes, solo se utilizaba una pequeña fracción del ancho de banda disponible para la banda vocal (4 KHz). Ahora, se aprovecha un espectro mucho más amplio (hasta 1 MHz) para ofrecer servicios de datos de alta velocidad.

#### ADSL (Asymmetric Digital Subscriber Line)

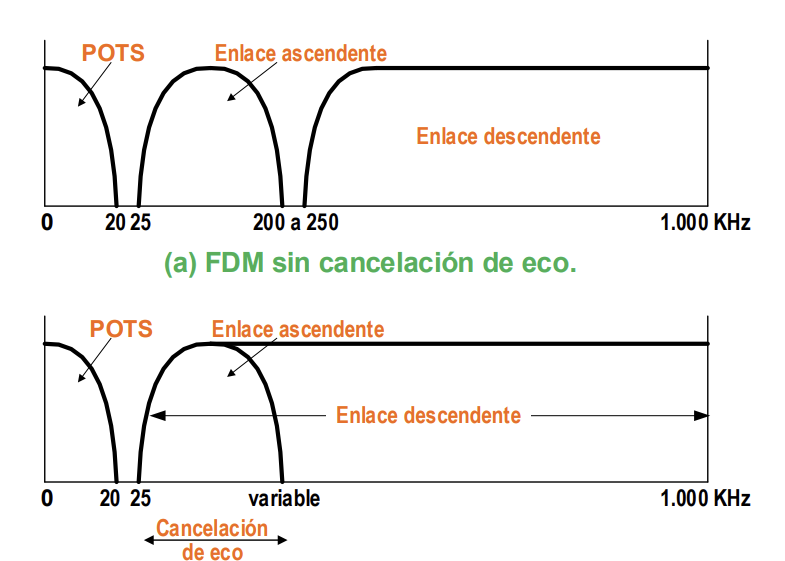
Es la tecnología xDSL más conocida y popular. El término "asimétrico" se debe a que la velocidad de bajada (downstream) es significativamente mayor que la de subida (upstream). Esto es ideal para aplicaciones como navegación web, descarga de archivos y video bajo demanda, donde el tráfico de bajada es predominante.

* **Estrategia de diseño:** ADSL utiliza la multiplexación por división de frecuencias (FDM) para dividir el ancho de banda del cable UTP. Los 25 KHz inferiores se reservan para la transmisión de voz analógica (POTS). El ancho de banda entre 4 KHz y 25 KHz se usa para evitar interferencias entre los canales de voz y datos. Para aumentar el ancho de banda, puede usar FDM o cancelación de eco.

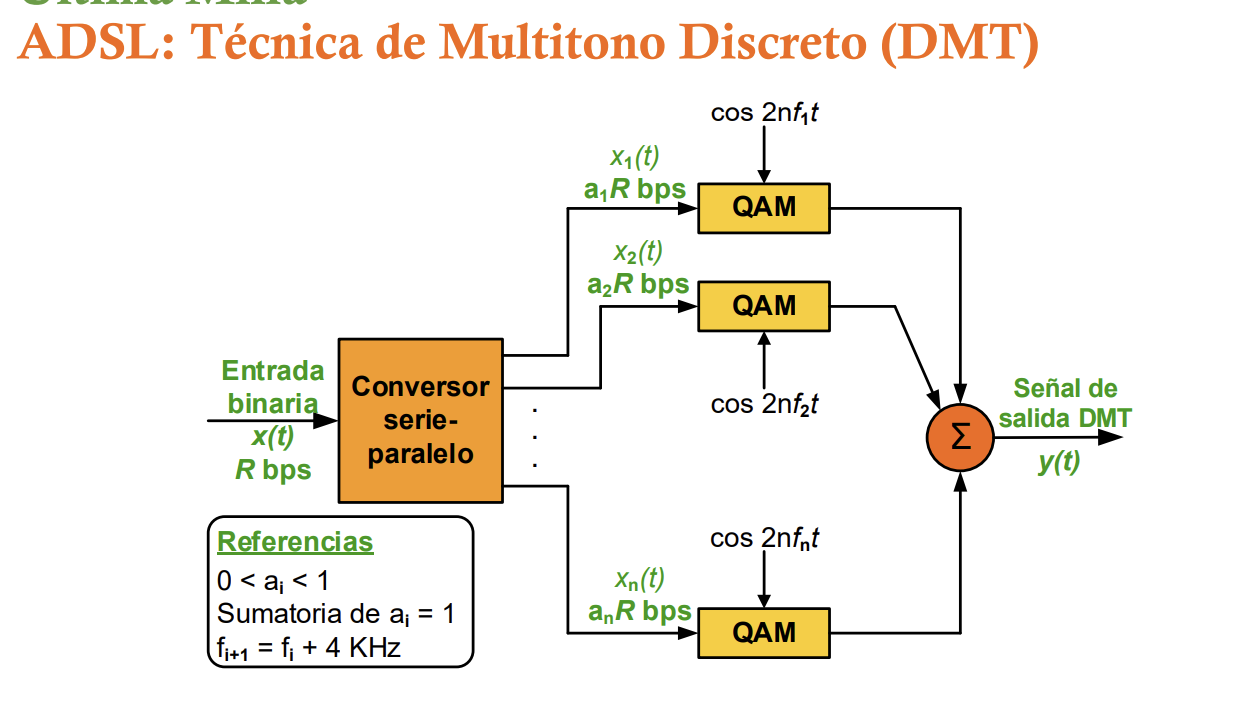
La cancelación de eco es una técnica de procesamiento de señales que se utiliza en la tecnología **ADSL** para permitir la transmisión simultánea de datos en ambos sentidos (subida y bajada) sobre un único par de cobre.

El eco en el contexto de ADSL ocurre porque la señal que el módem envía a la central (señal de subida) se "acopla" con la señal que viene de la central (señal de bajada) en la misma frecuencia, causando interferencia.

Al "cancelar" el eco, el módem puede aislar y procesar la señal de bajada sin la interferencia de su propia transmisión, permitiendo la comunicación dúplex sobre la misma banda de frecuencia.



* **Técnica de Multitono Discreto (DMT):** El ancho de banda se divide en varios subcanales de 4 KHz. Un módem DMT realiza un test inicial para medir la relación señal-ruido en cada subcanal y asigna más bits de datos a los que tienen mejor calidad. A medida que aumenta la frecuencia, la atenuación es mayor, por lo que los subcanales de frecuencias superiores transportan menos bits. Los diseños actuales de ADSL/DMT usan 256 subcanales de bajada.



* **Velocidades y alcance:** Ofrece velocidades de 41.5 Kbps a 8 Mbps en bajada y de 16 Kbps a 1 Mbps en subida en un par de cobre. Puede alcanzar hasta 3 km, con un máximo de 5.5 km en función de la calidad del cable.

#### Otras variantes de xDSL:

* **HDSL (High bit-rate Digital Subscriber Line):** Diseñada para ofrecer una transmisión más eficiente que el enlace E1/T1. Es una tecnología simétrica , usa dos pares de cobre y puede alcanzar velocidades de hasta 2 Mbps a través de 2 pares.
* **SDSL (Single-pair Digital Subscriber Line):** Desarrollada para usar un solo par de cobre, a diferencia de HDSL. Es también **simétrica**.
* **VDSL (Very High Bit-rate DSL):** Ofrece velocidades muy altas a distancias cortas. Es una tecnología **asimétrica** que se utiliza a menudo en conjunto con **FTTC** (Fiber to the Cabinet). Las velocidades pueden ser de 413 Kbps a 52 Mbps en bajada y de 1.5 a 13 Mbps en subida.
* **G.SHDSL (Single-pair High-speed Digital Subscriber Line):** Un estándar internacional que transmite datos de forma **simétrica** hasta 2.3 Mbps sobre un par o 4.6 Mbps sobre dos pares. Puede alcanzar distancias de hasta 3.9 Km.

### Redes de Acceso por Fibra Óptica (FTTx)

Esta tecnología se utiliza para superar las limitaciones del cobre. El término FTTx es un concepto genérico que indica que la fibra óptica se instala cerca del hogar o la oficina.

* **FTTH (Fiber to the Home):** La fibra óptica llega directamente al interior de la casa del abonado. Es una de las tecnologías que ofrece velocidades de acceso a Internet de hasta 300 Mbps o más.
* **FTTB (Fiber to the Building):** La fibra óptica termina en un punto de distribución dentro o cerca del edificio. Desde este punto, la conexión final al usuario se realiza a través de tecnologías como **VDSL2** sobre par de cobre o **Gigabit Ethernet** sobre par trenzado.
* **FTTC (Fiber to the Curb) y FTTN (Fiber to the Node):** En estos casos, la fibra termina en una cabina o nodo que se encuentra más cerca del usuario que en una red tradicional.

La arquitectura más común para FTTH es la **PON (Passive Optical Network)**. Esta red es pasiva, lo que significa que no requiere equipos energizados para amplificar o procesar la señal. La PON usa divisores ópticos en sentido de bajada y combinadores ópticos en sentido de subida. Los dos tipos de PON más comunes son **GPON** (Gigabit-capable PON) y **EPON** (Ethernet PON).

La arquitectura PON (Passive Optical Network) es una topología de red de fibra óptica punto-multipunto que utiliza divisores ópticos pasivos para transmitir datos desde un único hilo de fibra a múltiples usuarios finales. A continuación se detallan sus componentes clave:

### Componentes y Arquitectura de una Red PON

Una red PON está compuesta por tres elementos principales que trabajan juntos para llevar la fibra desde la central hasta el hogar del cliente.

#### OLT (Optical Line Terminal)

La OLT es el equipo activo ubicado en la **central del proveedor** de servicios. Es el punto de partida de la red PON.

* **Función:** La OLT se encarga de la agregación de tráfico de datos (voz, video y datos) proveniente de la red troncal (backbone) del proveedor de servicios. Distribuye esta información a las ONU de los clientes en sentido de bajada (downstream). En sentido de subida (upstream), recibe y gestiona los datos de los usuarios, enviándolos al núcleo de la red.
* **Comunicación:** Utiliza una sola longitud de onda para el tráfico de bajada para todos los usuarios conectados y una longitud de onda diferente para el tráfico de subida. Para evitar colisiones en la subida, utiliza un protocolo de acceso múltiple llamado **TDMA (Time Division Multiple Access)**, asignando ranuras de tiempo específicas a cada ONU.

#### ODN (Optical Distribution Network)

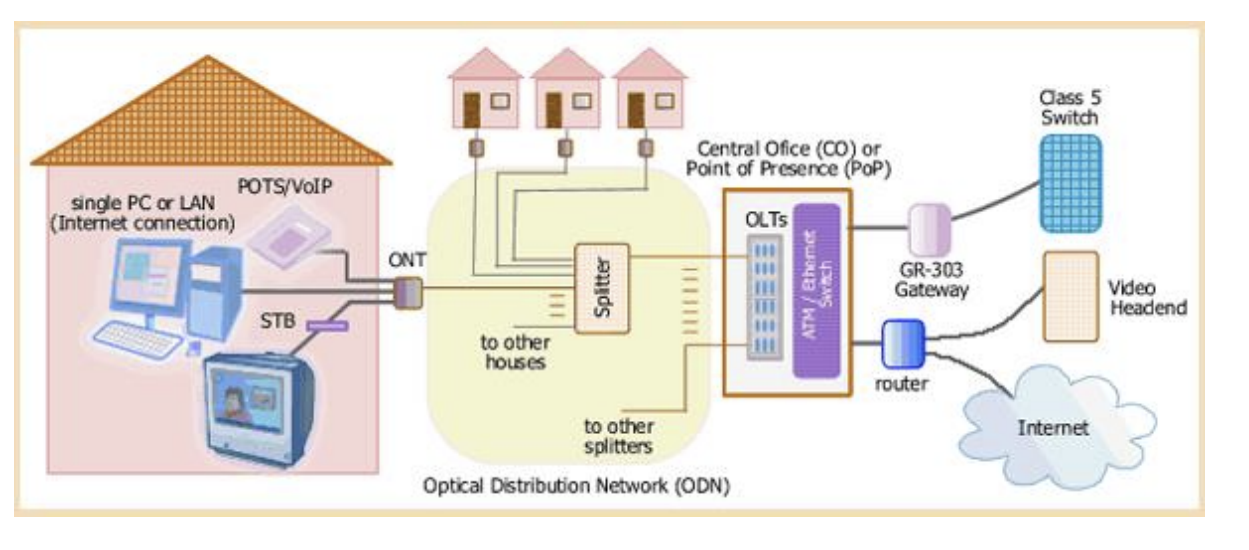
La ODN es la **red de fibra óptica pasiva** que interconecta la OLT con las ONU de los usuarios. Es el componente pasivo de la red y no requiere energía eléctrica.

* **Función:** Su principal componente son los **splitters ópticos**, que dividen la señal de fibra óptica para que una sola fibra de la OLT pueda servir a múltiples usuarios. Estos divisores pueden tener diferentes relaciones de división (por ejemplo, 1:4, 1:8, 1:16, 1:32 o 1:64).
* **Topología:** La ODN permite una topología en árbol o punto-multipunto, minimizando la cantidad de fibra necesaria y, por lo tanto, reduciendo los costos de despliegue.

#### ONU (Optical Network Unit) / ONT (Optical Network Terminal)

La ONU o ONT es el equipo activo ubicado en el **punto final** de la red, ya sea en el hogar del cliente o en un edificio.

* **Función:** Recibe la señal óptica de la OLT a través de la ODN y la convierte en señales eléctricas para ser utilizadas por los dispositivos del usuario (PC, televisores, teléfonos, etc.). También realiza el proceso inverso, convirtiendo las señales eléctricas del usuario en señales ópticas para ser enviadas a la OLT.
* **Diferencia ONU vs. ONT:** A menudo, los términos ONU y ONT se usan indistintamente. Sin embargo, en una definición más estricta, la **ONU** es el equipo final de la red de acceso óptico, que puede estar fuera de la casa del cliente (por ejemplo, en un sótano o en la calle), mientras que la **ONT** es un tipo de ONU que está dentro del local del usuario.



### Internet por Cable Módem (HFC)

Esta tecnología utiliza un sistema híbrido de fibra óptica y cable coaxial, conocido como

**HFC (Hybrid Fibre Coaxial)**. La fibra se usa para las distancias largas, y el cable coaxial se extiende desde un nodo de fibra hasta las casas.

* **Diferencia clave con ADSL:** En un sistema de cable, los usuarios de un vecindario **comparten el mismo cable coaxial**. Esto significa que, si un usuario descarga un archivo grande, el ancho de banda se reduce para los demás. En contraste, en una red ADSL, cada casa tiene su propio lazo local privado, por lo que el uso de un vecino no afecta a los demás.

### Internet por Cable Módem (HFC)

Esta tecnología utiliza un sistema híbrido de fibra óptica y cable coaxial, conocido como

**HFC (Hybrid Fibre Coaxial)**. La fibra se usa para las distancias largas, y el cable coaxial se extiende desde un nodo de fibra hasta las casas.

* **Diferencia clave con ADSL:** En un sistema de cable, los usuarios de un vecindario **comparten el mismo cable coaxial**. Esto significa que, si un usuario descarga un archivo grande, el ancho de banda se reduce para los demás. En contraste, en una red ADSL, cada casa tiene su propio lazo local privado, por lo que el uso de un vecino no afecta a los demás.

### Metro Ethernet

Una red Metro Ethernet es una arquitectura tecnológica que suministra servicios de conectividad de datos en una **Red de Área Metropolitana (MAN)** a través de interfaces Ethernet. Opera en la capa 2 del modelo OSI y es un servicio ofrecido por los proveedores de telecomunicaciones para interconectar redes de área local (LAN). Su principal objetivo es ser utilizada como una red de transporte o **Backbone** metropolitano para transportar tráfico Ethernet.

### Características y beneficios

* **Costos y fiabilidad**: Las interfaces Ethernet son considerablemente más económicas que las de las redes de jerarquía digital síncrona (SONET/SDH). Además, estas redes ofrecen una alta fiabilidad, ya que los enlaces están constituidos por múltiples pares de líneas de cobre o enlaces de fibra óptica.
* **Simplicidad y escalabilidad**: Se simplifican las operaciones de red, la administración y la actualización debido al uso de Ethernet. Las tramas Ethernet se pueden escalar mediante la modificación de sus encabezados para manejar una mayor capacidad de usuarios y servicios.
* **Topología**: La topología de una red Metro Ethernet puede ser en forma de anillo, estrella o malla total o parcial. La estructura jerárquica está compuesta por una parte de Distribución (Dorsal) y una de Agregación o acceso.

### Tipos de servicios (EVC)

El Metro Ethernet Forum (MEF) ha definido tres tipos de Conectividad Virtual Ethernet (EVC) para sus servicios:

* **E-Line (Punto a Punto)**: Proporciona un EVC punto a punto entre dos interfaces UNI (User Network Interface). Se utiliza para conexiones de ancho de banda dedicado, como se muestra en el diagrama a continuación.
* **E-LAN (Multipunto)**: Proporciona una conectividad multipunto donde los datos enviados desde una UNI pueden llegar a una o más UNI de destino. Desde la perspectiva del usuario, este servicio se comporta como una red LAN.
* **E-Tree (Punto a Multipunto)**: Este tipo de servicio conecta una UNI a varias UNI de destino, pero sin interconexión entre los destinos. Es un servicio unidireccional utilizado para tráfico broadcast o multicast.

### Acceso Inalámbrico a la Última Milla

Se refiere a las tecnologías que usan ondas de radio o microondas para conectar al usuario con la red.

* **Bucle Inalámbrico (WiLL):** Un sistema de acceso inalámbrico que puede incluir tecnologías como **LMDS** (Local Multipoint Distribution Service) y **MMDS** (Multichannel Multipoint Distribution Service).
* **WLAN y Wi-Fi:** Se refieren a redes de área local inalámbricas. Wi-Fi es el término comercial para WLAN. Operan en bandas de frecuencia no licenciadas (2.4 y 5 GHz).
* **HiperLAN2:** Otro estándar de red local inalámbrica.

# Primera Parte: Servicios de Datos a Empresas y PoDs

1. ¿Que tipos de servicios de internet ofrece TELECOM?

### **Internet Fibra Óptica para Hogares**

* Ofrecen acceso a internet residencial a través de distintas tecnologías:
  + **FTTH (fibra hasta el hogar)**
  + **HFC (fibra híbrida + cable)**
  + **VDSL** y **ADSL**, dependiendo de la zona [Wikipedia](https://es.wikipedia.org/wiki/Telecom_Argentina?utm_source=chatgpt.com).
* Este tipo de conexión es ideal para empresas, pymes y hogares que necesiten velocidad y estabilidad. Algunos beneficios clave:
  + **IP Fija**: Permite un acceso remoto más seguro (por ejemplo, cámaras o servidores).
  + **Telefonía IP integrada**: Permite realizar llamadas con buena calidad y tarifas reducidas.

### **GPON Corporativo (Fibra Semi-Dedicada)**

* Pensado para empresas que requieren alta calidad y conexiones más controladas.
* Utiliza tecnología GPON (Gigabit-capable Passive Optical Network), ideal cuando se busca optimizar tiempos de instalación sin obras civiles costosas.
* Proporciona mayor estabilidad, seguridad y velocidad gracias a su arquitectura de fibra óptica FTTH.

### **Internet Dedicado por Fibra (Empresas)**

* Enlaces exclusivos de fibra óptica con conexión directa al backbone de Telecom.
* Ofrece **SLA (99.75% de disponibilidad anual)**, ancho de banda ajustable, IP pública (subredes de 8 IPs), equipo CPE de calidad portadora y monitoreo web del enlace.

### **Internet Satelital**

* Servicio pensados para empresas en ubicaciones remotas o sin acceso a redes fijas.
* Proporciona acceso vía satélite, con opciones de ancho de banda garantizado (CIR) y adicional (PIR). Incluye IP pública fija, NAT, soporte 24/7 y asesoramiento técnico [Telecom](https://www.telecom.com.ar/web/productos/internet-satelital?utm_source=chatgpt.com).

### **Internet+ (Híbrido con Respaldo 4G)**

* Diseñado para asegurar conectividad continua: combina una conexión fija (fibra o HFC) con respaldo automático a través de la red móvil Personal 4G.
* El equipo (router Carrier Class) conmuta el tráfico automáticamente entre ambas redes manteniendo la misma **IP fija**, evitando interrupciones en servicios críticos.

1. ¿Qué significa PIR y CIR en Internet Satelital?

En los servicios de Internet Satelital, los términos CIR (Committed Information Rate) y PIR (Peak Information Rate) definen la calidad del ancho de banda contratado: el CIR corresponde a la velocidad mínima garantizada que el proveedor asegura de forma permanente, incluso en situaciones de congestión de la red, mientras que el PIR representa la velocidad máxima que se puede alcanzar en momentos de baja demanda, aunque no está garantizada y depende de la disponibilidad de recursos. En otras palabras, el CIR es el piso asegurado del servicio y el PIR es el techo al que se puede llegar de manera eventual.

1. ¿Qué significa SLA en el Internet dedicado?

Un SLA (Service Level Agreement, o Acuerdo de Nivel de Servicio) en el contexto de Internet Dedicado es un contrato formal entre el proveedor del servicio y el cliente donde se establecen garantías técnicas, de calidad y disponibilidad que el operador debe cumplir respecto a la conexión.

1. ¿Qué servicios de Datacenter e Infraestructura ofrece Telecom? ¿Cuáles son sus características?

## Servicios de Datacenter e Infraestructura de Telecom Argentina

### 1. **Housing (Colocation)**

* Alojamiento de servidores en racks estándares (½ rack de 20U o rack completo de 40U) en instalaciones seguras con monitoreo 24/7, energía redundante (UPS, PDU duales), control de acceso y vigilancia.
* Ofrece conectividad pública (Internet) y privada (MPLS, L2L), Backbone redundante con carriers locales e internacionales.
* SLA garantizado: disponibilidad del **99,9 %** anual.
* Servicios complementarios: **Cross-connect**, jaulas físicas ("jaula"), acometidas, cableado, puestos de contingencia e infraestructura adicional, más **Servicios Profesionales** (packs básicos o avanzados con intervenciones incluidas).

### 2. **Backup / Respaldo de Servidores**

* Servicio de backup para servidores físicos o virtuales alojados en el datacenter de Pacheco. Gestiona políticas de retención y recuperación. El espacio mínimo de almacenamiento se define como el 80 % del disco útil total.

1. ¿Cuáles son los servicios que ofrece Claro para Empresas en el manejo de Datos? ¿Cuáles son sus características?

## Servicios de Datos para Empresas

### 1. **Red Privada Virtual Multiservicios (VPN multiservicios)**

Una solución para conectar de manera segura diversas sedes o usuarios remotos mediante redes privadas. Combina conectividad segura para distintas aplicaciones sobre una infraestructura común.

### 2. **LAN y WAN Administrada**

Permite a las empresas delegar en Claro la gestión técnica de sus redes locales (LAN) y amplias (WAN), ideal para entornos con múltiples sedes o poca capacidad interna para manejar infraestructura. Facilita la modernización tecnológica y optimiza la administración de redes.

### 3. LAN to LAN

Los servicios Ethernet permiten conectar sus oficinas de manera transparente en capa 2, a muy alta velocidad y baja latencia. Soluciones punto a punto para interconexión de centros de cómputo, y opciones multipunto para oficinas centrales.

### 4. **SD-WAN**

Tecnología para diseñar redes empresariales más ágiles, donde la administración, priorización del tráfico, enrutamiento y seguridad se gestionan centralmente, separando la infraestructura física. Permite una configuración dinámica y eficiente según aplicaciones o políticas específicas.



1. ¿Qué servicios de conectividad terrestre y que servicios de conectividad satelital ofrece ARSAT?

## Servicios de Conectividad Terrestre de ARSAT

1. **Internet**
   * Proporciona acceso a Internet con velocidades ajustables a las necesidades del cliente.
   * Apalanca la **Red Federal de Fibra Óptica (REFEFO)** de más de 31.000 km iluminados.
   * Ofrece tráfico nacional mediante su propio data center y cachés estratégicos, y tráfico internacional gracias a los cables submarinos SAM-1 y SAC.
   * Garantiza alta tasa de transmisión, seguridad y rendimiento del servicio.
   * **Modalidades disponibles**: Internet Dedicado y Tránsito IP.
2. **Tráfico Nacional**
   * Permite a los clientes del servicio de Internet acceder directamente a los cachés alojados en el backbone de Internet de ARSAT, optimizando tiempos de acceso a contenidos nacionales.
3. **Lan to Lan**
   * Servicio punto a punto que extiende LANs entre dos ubicaciones del cliente, funcionando como una red extendida.
   * Se basa en Ethernet y utiliza “pseudowires” VLAN sobre la red MPLS.
   * Ideal para aplicaciones exigentes gracias a su simplicidad y soporte sobre MPLS.
4. **MPLS**
   * Red de servicios construida sobre transporte DWDM.
   * Ofrece velocidades desde **50 Mbps hasta 10 Gbps**, con alta confiabilidad y desempeño.
5. **DWDM**
   * Red de transporte DWDM/OTN desplegada a nivel nacional con equipos de última generación.
   * Soporta interfaces multiprotocolo (UNI) y múltiples velocidades; incluye protocolos como Ethernet, SDH, OTN, FibreChannel y Video.[arsat.com.ar+1](https://www.arsat.com.ar/conectividad-terrestre/?utm_source=chatgpt.com)
6. **Multicast**
   * Servicio de multidifusión IP (IP multicast) multipunto sobre la REFEFO.
   * Permite enviar datos una sola vez por la red IP/MPLS y que lleguen únicamente a los sitios definidos.
   * Es eficiente para enviar grandes volúmenes de datos simultáneamente a múltiples ubicaciones.

## Servicios Satelitales de ARSAT

### 1. **Capacidad Satelital**

ARSAT ofrece espacio satelital sobre sus satélites geoestacionarios **ARSAT-1 y ARSAT-2**, en **Banda C o Banda Ku**. Existen dos modalidades:

* **Capacidad fija**: asignada de forma permanente.
* **Uso ocasional**: activación bajo demanda según necesidad del cliente.

### 2. **Housing Satelital**

Permite al cliente alojar o implementar señales satelitales como redes **VSAT**, señales de TV, enlaces de datos o contribuciones dentro de la infraestructura de ARSAT. El servicio incluye flexibilidad y conectividad integrada a redes terrestres.

### 3. **Uplink de Señales (VSAT)**

Mediante los satélites ARSAT-1 y ARSAT-2, ARSAT ofrece **servicios VSAT (Very Small Aperture Terminal)** para transmisión de Internet y datos en todo el país, ideal para zonas remotas o que carecen de infraestructura terrestre.

### 4. **IoT Satelital**

Utilizando el satélite geoestacionario **ARSAT-1**, la empresa brinda conectividad para **Internet de las cosas (IoT)**, con mensajes bidireccionales en aplicaciones fijas o móviles. Ofrece baja inversión en instalación y mantenimiento, consumo energético reducido y cobertura nacional completa.

### 5. **Banda Ancha Satelital / Conectividad Satelital (o VNO)**

Se ofrece para revendedores y clientes corporativos una solución de **banda ancha satelital en Banda Ka**, con planes de consumo variables y cobertura nacional. Bajo la modalidad VNO ("Virtual Network Operator"), ARSAT provee toda la infraestructura central, permitiendo escalar sin necesidad de inversión en infraestructura por parte del cliente.

1. Describa los servicios de Internet para empresas que ofrece iptel en Argentina.

## Servicios de Internet que ofrece IPTel para Empresas

1. **Internet Dedicado**
   * Conexión permanente, exclusiva y segura con ancho de banda comprometido.
   * Velocidad simétrica: misma velocidad de subida y bajada.
   * Incluye IP pública fija y soporte técnico 24/7. Ideal para sistemas de gestión (ERP, CRM), VPNs, videoconferencias, e-commerce, streaming, e-learning y transferencia de archivos grandes.
2. **Internet Inalámbrico**
   * Conexión vía antena directa a los nodos de IPTel, similar a un enlace cableado o de red.
   * Disponible en ubicaciones estratégicas; útil cuando la infraestructura tradicional no es viable.
3. **Fibra Óptica**
   * Servicio de alta velocidad con planes que superan los 10 Mbps.
   * Permite elegir el plan según la necesidad del negocio. Ofrece bajadas rápidas, estabilidad y buena experiencia de uso, especialmente útil para aplicaciones en la nube.
4. **Internet Simétrico**
   * Conexión con igual velocidad de subida y bajada, pensada para uso empresarial crítico.
   * Alta calidad garantizada con disponibilidad anual del 99 %.
5. En base al artículo publicado “Especificación de arquitecturas de pods de IT para Data Centers”:
   1. Explique que es un chasis de PoD

Un **chasis de PoD** es una estructura autónoma que sirve como **punto de montaje** para los servicios comunes de un PoD de IT. En lugar de instalar la contención de aire, la red, la alimentación o incluso tuberías de refrigeración directamente en los racks o en el techo/suelo técnico, estos se montan en el chasis del PoD.  
Esto permite que los **racks completamente configurados** puedan añadirse o retirarse con facilidad, ya que el soporte de servicios ya está preinstalado en el chasis. En otras palabras, el chasis actúa como un “esqueleto” que concentra y organiza los elementos compartidos del PoD.

* 1. ¿Qué ventajas supone implementar un PoD, en lugar de implementar soluciones rack por rack)
     + **Escalabilidad modular**
       - Permite implantar IT en bloques más grandes (pods) en lugar de hacerlo rack por rack, acelerando la expansión y el despliegue de capacidad.
     + **Estandarización y simplicidad**
       - Los pods pueden diseñarse con configuraciones estándar (150 kW, 250 kW, etc.), lo que simplifica la planificación, reduce errores y acelera el tiempo de puesta en marcha.
     + **Flexibilidad tecnológica**
       - Facilita variar arquitecturas de alimentación, refrigeración y redundancia entre pods sin afectar a toda la sala. Ejemplo: un pod puede usar refrigeración líquida y otro aire, o distintos niveles de redundancia eléctrica.
     + **Mejor gestión operativa**
       - Organizar a nivel de pod permite aplicar políticas diferenciadas (seguridad, criticidad, redundancia) por grupos de racks, algo mucho más complejo si se hiciera rack por rack.
     + **Reducción de costos y tiempos de obra**
       - Con el uso de chasis de pod autónomos, no hace falta suelo técnico ni instalaciones de techo complejas, lo que reduce obra civil y facilita la adición/retiro de racks.
     + **Menor riesgo de errores**
       - Al delimitar recursos y dependencias a nivel de pod, se reducen las confusiones en la gestión de energía, refrigeración o redes, en comparación con un esquema de distribución rack por rack.

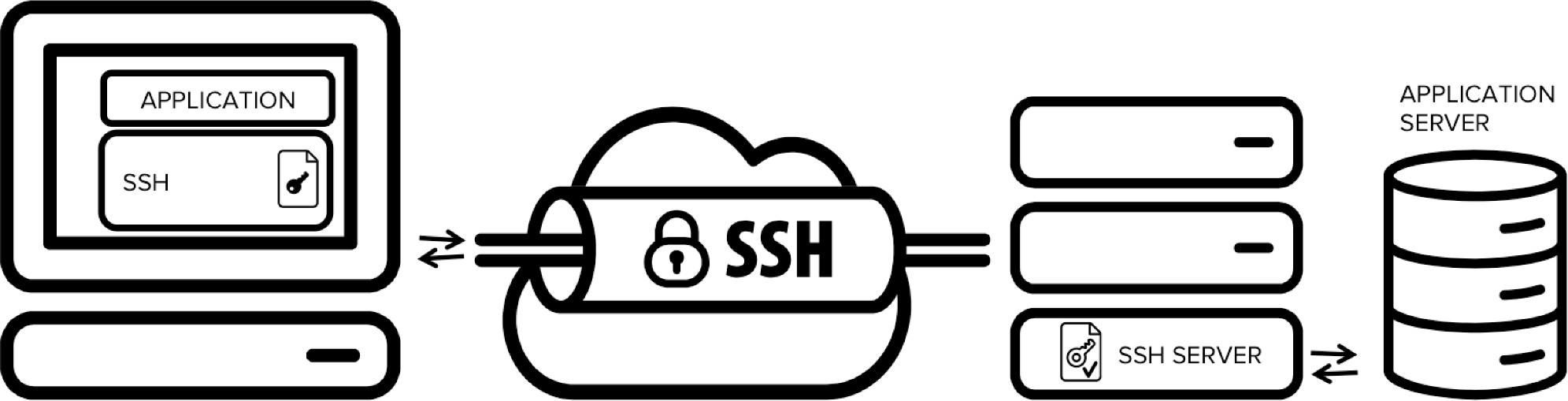
# Segunda Parte: Accesos Seguros sobre Vínculos Públicos

En esta segunda parte presentamos 2 opciones para asegurar nuestro tráfico a través de internet:

* ssh portforwarding
* VPN.

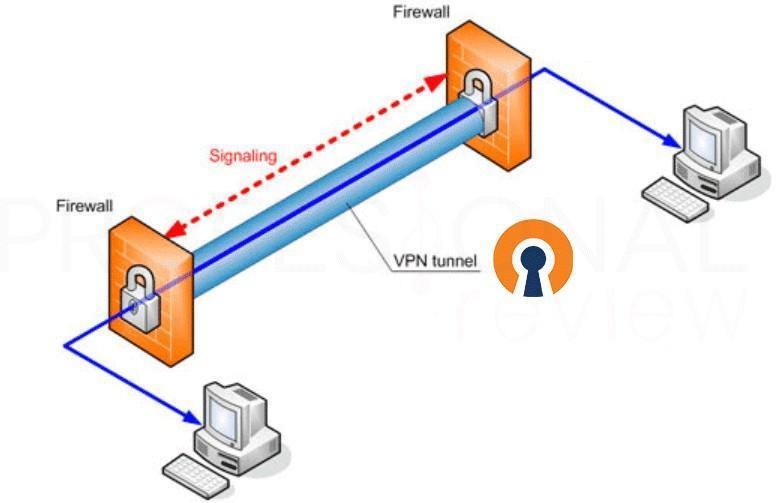
Ambas opciones permiten conectarnos a través de un canal seguro a través de un medio inseguro. Sin embargo, presentan ciertas características que pueden ayudarnos a elegir según nuestras necesidades.

SSH es una solución simple rápida y segura pensada originalmente para brindar acceso seguro a una consola shell pero además tiene otros múltiples usos.



VPN: se tomará como ejemplo una vpn roadwarrior implementada mediante openvpn. En este caso es una solución más compleja pero también más potente y quizás más segura.

La **VPN Roadwarrior** es un tipo de red privada virtual diseñada para usuarios móviles que necesitan acceder a la red corporativa desde ubicaciones externas, como sus casas, aeropuertos o cafés. En este esquema, el empleado instala un cliente VPN en su dispositivo (notebook, smartphone o tablet) y, al autenticarse en el servidor VPN de la empresa, se establece un túnel cifrado punto a punto. A través de ese túnel, el dispositivo recibe una dirección IP interna de la red corporativa, lo que le permite acceder a recursos como si estuviera físicamente dentro de la oficina: servidores de archivos, aplicaciones internas, impresoras o bases de datos. Este modelo está especialmente pensado para escenarios de teletrabajo o movilidad laboral, donde los usuarios —los llamados “roadwarriors”— requieren una conexión completa y segura desde cualquier parte del mundo. A diferencia del SSH port forwarding, que se limita a redirigir tráfico de un puerto o aplicación específica, la VPN Roadwarrior asegura **todo el tráfico de red del dispositivo**, proporcionando confidencialidad, integridad y autenticación a nivel de red, lo que resulta esencial para empresas que necesitan extender su infraestructura de manera segura a trabajadores remotos.



Algunos conceptos sobre SSH Local forwarding:

Permite redirigir el tráfico enviado a un puerto local hacia un puerto específico de un host remoto de manera bidireccional.

Remote forwarding: Establece un camino cifrado que permite que el tráfico generado contra un puerto específico de un host remoto sea redirigido hacia un puerto específico de un host local.

El **SSH port forwarding** o **túnel SSH** es una técnica que aprovecha la conexión segura establecida por el protocolo SSH para redirigir el tráfico de aplicaciones a través de un canal cifrado. De esta forma, incluso si la aplicación en sí no utiliza cifrado, los datos viajan protegidos dentro del túnel. Existen tres modalidades de reenvío de puertos.

El **local forwarding** permite que un puerto de la máquina cliente actúe como puerta de entrada hacia un servicio que se encuentra en un servidor remoto: por ejemplo, se puede mapear el puerto 8080 de la computadora local hacia el puerto 80 de un servidor web, logrando así que todo el tráfico pase cifrado por el túnel SSH.

En cambio, el **remote forwarding** habilita que un puerto del servidor remoto reenvíe tráfico hacia un servicio que está en la máquina local, lo cual es útil cuando queremos exponer una aplicación en desarrollo a usuarios externos sin necesidad de abrir puertos en el firewall o router.

Finalmente, el **dynamic forwarding** funciona como un proxy SOCKS: el cliente crea un puerto local que actúa como proxy y las aplicaciones pueden enrutar tráfico de forma dinámica a través de ese túnel seguro, lo que permite, por ejemplo, navegar por Internet como si lo hiciéramos desde el servidor remoto. En todos los casos, la ventaja principal es que el tráfico queda encapsulado en SSH, ofreciendo seguridad y confidencialidad sin necesidad de modificar la aplicación original.

Demo

Pasos previos

Del lado del **gateway-ssh**

* Se instaló ssh
* Se configuró AllowTcpForwarding para que permita el forwarding local y remoto.
* Se generaron claves rsa públicas y privadas para el usuario que se conectara
* Se vincularon las claves públicas a un usuario en particular a nivel SO para poder conectarnos de manera segura sin utilizar claves precompartidas.
* Se realizó un portforwarding en el modem redirigiendo el tráfico de un puerto específico de su ip pública contra el puerto ssh del **gateway-ssh**

En el cliente:

* Se instaló ssh
* Se copió y asoció la clave rsa privada ya generada a un agente ssh para su gestión.

# Conexión hacia una aplicación de una intranet alojada en un servidor A a través de un tunnel ssh establecido entre nuestro equipo y un gateway que tiene un puerto ssh expuesto a internet.

##generación de túnel

ssh -L 1270.0.010:8444:servidorA:8443 gatewayssh

#Evaluar conexiones establecidas netstat -ptnauo | grep ssh

# Conexión a una lan remota vía openvpn

conexión : openvpn usuario.ovpn

* + Revisar el log de la conexión.
  + Telnet hacia un equipo de la red remota a través de la vpn.
  + Relevar interfaces involucradas y conexiones establecidas.
  + Ver tráfico en la interfaz de la vpn.
  + Ver trafico en la interfaz hacia internet.
  + Buscar cadenas legibles en ambos casos.

Referencias

Comparativa entre ssh y openvpn para tunneling https://blog.backslasher.net/ssh-openvpn-tunneling.htm l

ssh tunneling https://[www.ssh.com/academy/ssh/tunneling](http://www.ssh.com/academy/ssh/tunneling)

https://[www.ssh.com/academy/ssh/tunneling/example#how-to-prevent-ssh-port-forwarding-from-circu](http://www.ssh.com/academy/ssh/tunneling/example#how-to-prevent-ssh-port-forwarding-from-circum) [m](http://www.ssh.com/academy/ssh/tunneling/example#how-to-prevent-ssh-port-forwarding-from-circum) venting-firewalls

Sitio oficial openvpn https://openvpn.net

Sitio oficial wireguard https://[www.wireguard.com/](http://www.wireguard.com/)

1. Luego de observar la demostración de cómo transmitir datos en forma segura a través de una red pública (que se va a comportar como una red privada virtual), responda lo siguiente:
   1. ¿Si usted desea capturar el tráfico antes de ser cifrado por ssh en que interfaz lo haría?

Si quieres ver los datos antes de que SSH los cifre, deberías capturarlos en la interfaz de red local (por ejemplo eth0, wlan0 o enp3s0) del cliente, antes de que el tráfico sea enviado por SSH. Esto se hace con herramientas como tcpdump o Wireshark en la interfaz de red física que envía los paquetes.

* 1. ¿Si quiere ver el tráfico que pasa por el túnel, como lo haría?

Si quieres observar el tráfico **ya cifrado dentro del túnel SSH**, lo capturas en la interfaz **virtual creada por SSH**, normalmente lo (loopback) si es local forwarding, o el túnel creado (tun0, ssh0, según configuración). Ese tráfico estará cifrado, por lo que verás datos que no se pueden leer directamente sin descifrar.

1. Explique las conexiones observadas por el comando netstat -ptnauo | grep ssh”

El comando muestra las conexiones activas de SSH (cliente o servidor) con IP, puerto, estado (ESTABLISHED, LISTEN) y el PID del proceso ssh.

1. ¿Qué hace el siguiente comando?:

# ssh -L127.0.0.10:3390:servidorA:3389 gatewayssh

* -L → Local forwarding (redirige un puerto local hacia un host/puerto remoto).
* 127.0.0.10:3390 → en mi máquina local, escuchar en IP 127.0.0.10 y puerto 3390.
* servidorA:3389 → destino remoto al que quiero acceder (RDP normalmente usa 3389).
* gatewayssh → servidor SSH intermediario que crea el túnel.

**Resultado:** cuando en tu PC accedas a 127.0.0.10:3390, SSH lo redirige a servidorA:3389 a través de gatewayssh.

1. Explique la sintaxis del comando usado para generar el local forwarding

ssh -L [ip\_local]:[puerto\_local]:[host\_remoto]:[puerto\_remoto] [usuario@servidor\_ssh]

 [ip\_local] → IP de tu máquina donde escucha.

 [puerto\_local] → puerto local que se redirige.

 [host\_remoto] → host que quieres alcanzar desde el servidor SSH.

 [puerto\_remoto] → puerto del host remoto.

 [usuario@servidor\_ssh] → servidor que actúa como túnel.

1. ¿Cuál es el comando usado para generar las claves rsa públicas y privadas?

Las **claves RSA** son un tipo de **par de claves criptográficas** usadas en **criptografía asimétrica**, inventadas por **Rivest, Shamir y Adleman** (de ahí RSA). Se usan para **cifrar información y autenticar usuarios** sin necesidad de compartir una contraseña secreta directamente.

Se componen de dos partes:

1. **Clave pública**:
   * Se puede compartir libremente.
   * Permite que otros cifren mensajes que solo el propietario de la clave privada puede descifrar.
   * También se usa para verificar firmas digitales hechas con la clave privada.
2. **Clave privada**:
   * Se **mantiene secreta**.
   * Permite descifrar mensajes cifrados con la clave pública.
   * Se usa para firmar digitalmente mensajes, garantizando autenticidad y que provienen de quien dice ser.

**Funcionamiento básico:**

* Si alguien quiere enviarte información segura, usa tu **clave pública** para cifrarla.
* Solo tú, con tu **clave privada**, puedes descifrarla.
* Esto evita que un atacante que capture el mensaje pueda leerlo.

**Ejemplo en SSH:**

* Tu computadora tiene la **clave privada**.
* El servidor SSH tiene tu **clave pública** asociada a tu usuario.
* Cuando te conectás, SSH verifica que tengas la clave privada correcta para autenticarte sin usar contraseña.

Comando para crear claves rsa: ssh-keygen -t rsa -b 4096 -f ~/.ssh/id\_rsa

-t rsa → tipo de clave.

-b 4096 → tamaño en bits.

-f → archivo donde se guarda la clave privada (la pública se crea con .pub).

1. ¿Cómo se asocia la clave pública a un usuario de SO en el “gatewayssh”?

Copiar la clave pública al archivo ~/.ssh/authorized\_keys del usuario remoto:

ssh-copy-id usuario@gatewayssh

o manualmente: cat id\_rsa.pub >> ~/.ssh/authorized\_keys

1. ¿Cómo cargo su clave privada en el agente ssh del cliente?

eval "$(ssh-agent -s)" # iniciar el agente

ssh-add ~/.ssh/id\_rsa # cargar la clave privada

1. ¿Cómo se conecta a un puerto específico de un servidor remoto usando ssh y usando openvpn?

¿Contra qué dirección ip apunta su cliente en cada caso?

SSH (ejemplo local forwarding):

ssh -L 127.0.0.1:5000:remoto:80 usuario@gatewayssh

OpenVPN: se conecta a la VPN y accedes al puerto del destino a través de la IP asignada por la VPN.

Dirección IP del cliente:

SSH → IP local 127.0.0.1 o la interfaz donde escuchas.

OpenVPN → IP de la interfaz tun/virtual asignada por OpenVPN (10.x.x.x o 172.x.x.x según configuración).

1. ¿Qué información contiene el archivo “usuario.ovpn”?

 Dirección del servidor VPN y puerto.

 Certificados y claves del cliente.

 Configuración de cifrado (TLS, AES, etc.).

 Rutas y opciones de red (qué tráfico pasa por VPN).

1. ¿Podría analizar el tráfico cifrado por “openvpn” o ver el tráfico antes de que se cifre?

 **No** se puede leer directamente porque está cifrado.

 Puedes capturar tráfico en la interfaz tun (tun0) para ver **paquetes cifrados**.

 Para ver tráfico antes de cifrarlo, habría que capturarlo en la **interfaz física del cliente** antes de que OpenVPN lo cifre.

1. Si usted desea limitar los destinos del tráfico que pasa por el “gatewayssh” y/o el servidor “openvpn”, pero no el generado desde estos equipos; ¿cuál solución elegiría para hacerlo en forma más simple?

¿Por qué?

Usar **firewall o reglas de iptables** en gatewayssh o el servidor OpenVPN para limitar IP/puertos de destino. Esto permite filtrar **solo el tráfico que pasa por el túnel**, sin afectar tráfico generado desde esos equipos.

1. ¿Cómo le indico a mi pc que debe usar “openvpn” para llegar a un destino?

OpenVPN crea **una interfaz virtual** (tun0) y agrega **rutas en la tabla de enrutamiento**.

Para un destino específico:

route add <destino> <IP\_puerta\_de\_enlace\_tun>

o usando la opción route en el .ovpn:

route 192.168.10.0 255.255.255.0

MySQL:3306