1. Defina:
   1. BSS

Es un conjunto de estaciones controladas por una función de coordinación que compiten por el mismo medio inalámbrico. Cada BSS puede estar aislado o conectado a un sistema de distribución (DS) mediante un punto de acceso (AP).

* 1. ESS

Es un conjunto de uno o más BSS interconectados por un sistema de distribución (DS), que actúan como un único BSS lógico desde el punto de vista de las estaciones conectadas.

* 1. Red infraestructura

Configuración en la cual una o más estaciones se conectan a través de un punto de acceso (AP) a un sistema de distribución. Es la forma común de conexión en redes Wi-Fi con acceso a LAN cableadas y a Internet.

* 1. Red AdHoc

Red temporal entre estaciones sin necesidad de infraestructura o punto de acceso. Las estaciones se comunican entre sí directamente, útil para reuniones o intercambios espontáneos de información.

* 1. Sistema de Distribución

Es el sistema que interconecta múltiples BSS para formar un ESS, permitiendo la movilidad entre celdas y facilitando la entrega de datos entre estaciones que están en diferentes BSS.

1. Cuales son las distancias y velocidades máximas para las normas 802.11 b,802.11 g, 802.11 n,

802.11 ac.

| **Norma** | **Velocidad Máxima** | **Distancia Aproximada** |
| --- | --- | --- |
| **802.11b** | 11 Mbps | ~100 m |
| **802.11g** | 54 Mbps | ~100 m |
| **802.11n** | 100-600 Mbps | ~250 m |
| **802.11ac** | hasta 1 Gbps o más | ~100 m |

1. ¿Qué servicios debe proporcionar una red inalámbrica según la norma ? explique en qué consisten?

La norma IEEE 802.11 establece un conjunto de nueve servicios fundamentales que una red inalámbrica debe proporcionar para ofrecer una funcionalidad comparable a la de una LAN cableada. Estos servicios se agrupan en tres grandes categorías: entrega de datos, gestión de asociación y seguridad y control de acceso.

En primer lugar, se encuentran los servicios destinados a la entrega de datos, cuyo objetivo es asegurar que las tramas lleguen correctamente desde el emisor al receptor. El servicio básico en esta categoría es la entrega de MSDU (MAC Service Data Unit), que se encarga de transportar los datos entre estaciones utilizando los mecanismos del protocolo MAC.

Para permitir la comunicación entre estaciones ubicadas en distintos conjuntos de servicio básico (BSS), se emplea el servicio de distribución, que canaliza la información a través del sistema de distribución (DS). Este sistema puede ser una red cableada, como Ethernet, que interconecta los distintos puntos de acceso (AP) de la red inalámbrica.

Por otro lado, el servicio de integración permite que estaciones de una red IEEE 802.11 se comuniquen con estaciones de otras redes locales que utilicen estándares diferentes, como IEEE 802.3. Este servicio realiza las conversiones lógicas necesarias, como el mapeo de direcciones, para garantizar la interoperabilidad entre redes.

En segundo lugar, los servicios de gestión de asociación tienen como función controlar el vínculo entre las estaciones móviles y los puntos de acceso.

Antes de que una estación pueda intercambiar datos, debe establecer una asociación con un AP, lo que implica el registro de su identidad y su localización dentro del sistema de distribución. Este procedimiento permite que el sistema sepa por qué AP debe encaminar las tramas destinadas a esa estación.

Cuando una estación se desplaza de un BSS a otro dentro del mismo ESS, se utiliza el servicio de reasociación, que transfiere la asociación activa de un AP a otro sin necesidad de interrumpir la comunicación.

Finalmente, el servicio de disociación permite a una estación o a un AP informar que una asociación existente ha terminado, por ejemplo, cuando una estación se apaga o abandona el área de cobertura.

Por último, los servicios relacionados con la seguridad y el control de acceso garantizan que solo las estaciones autorizadas puedan participar en la red, y que las comunicaciones sean privadas.

El servicio de autenticación permite que una estación pruebe su identidad antes de asociarse a la red. IEEE 802.11 no impone un método específico, pero admite desde claves compartidas simples hasta mecanismos más seguros como certificados digitales. Una vez que la autenticación ya no es necesaria, se puede invocar el servicio de fin de autenticación, que concluye de forma formal la relación de confianza establecida previamente.

Además, la norma contempla el servicio de privacidad, mediante el cual se cifran los datos transmitidos para evitar que sean interceptados por usuarios no autorizados. Esto es especialmente importante en un entorno inalámbrico, donde cualquier estación dentro del área de cobertura física puede potencialmente recibir señales.

1. ¿Existe compatibilidad entre las normas 802.11 b,802.11 g, 802.11 n? ¿Es posible que un equipo norma b se conecte a un ap norma n? si es así bajo qué norma se conectaría?

Si existe compatibilidad entre las normas mencionadas ya que todas utilizan la banda de 2.4 GHz. Un equipo de norma b podrá conectarse a un AP norma n siempre y cuando el AP esté configurado para trabajar en modo mixto (legacy compatible). La conexión se realizará bajo la norma más baja compatible. Se utilizará la banda de 2.4 GHz y se transmitirá a 11 Mbps.

1. ¿En qué consiste el acceso nómada? gracias a que servicio es posible?

El acceso nómada en las LAN inalámbricas consiste en proporcionar conectividad a dispositivos móviles (como notebooks, tablets o smartphones) que se desplazan dentro de un área cubierta por la red, permitiéndoles acceder a los recursos de la red sin necesidad de una conexión física por cable.

acceso nómada es posible gracias a los servicios de gestión de asociación definidos en el estándar IEEE 802.11, específicamente:

* + Asociación: Establece la conexión inicial entre un dispositivo móvil y un punto de acceso (AP).
  + Reasociación: Permite que un dispositivo móvil cambie de un punto de acceso a otro dentro de la misma red (ESS) sin perder la conexión, facilitando la movilidad.
  + Autenticación: Asegura que solo los dispositivos autorizados puedan acceder a la red.

El acceso nómada depende directamente de estos servicios para garantizar una conexión continua y segura mientras el usuario se mueve. Por ejemplo, cuando un dispositivo se desplaza de una celda a otra, el servicio de reasociación permite que el nuevo punto de acceso tome el control de la comunicación, asegurando una transición suave y sin interrupciones.

1. ¿Comente, qué tipos de protocolos de seguridad puede implementar dentro de una wlan? ordénelos desde el más seguro al más inseguro?

Dentro de una WLAN, se pueden implementar varios protocolos de seguridad, ordenándolos del más seguro al menos seguro:

1. **WPA2 (Wi-Fi Protected Access II):**
   * **Seguridad:** Es el protocolo más seguro y ampliamente recomendado en la actualidad.
   * **Características:** Utiliza el cifrado AES (Advanced Encryption Standard) con el protocolo CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). Ofrece una autenticación robusta y una protección fuerte contra ataques.
   * **Modos:** WPA2-Personal (PSK) para redes domésticas y WPA2-Enterprise (802.1X) para redes empresariales con autenticación centralizada.
2. **WPA (Wi-Fi Protected Access):**
   * **Seguridad:** Fue desarrollado como una mejora provisional sobre WEP para abordar sus debilidades, antes de la llegada de WPA2.
   * **Características:** Utiliza el TKIP (Temporal Key Integrity Protocol) con cifrado RC4. Aunque mejor que WEP, TKIP ha demostrado tener vulnerabilidades y no es tan robusto como AES.
   * **Modos:** WPA-Personal (PSK) y WPA-Enterprise (802.1X).
3. **WEP (Wired Equivalent Privacy):**
   * **Seguridad:** Es el protocolo más antiguo y menos seguro, considerado obsoleto y fácil de romper.
   * **Características:** Utiliza el algoritmo de cifrado RC4 y claves estáticas. Presenta graves vulnerabilidades que permiten a los atacantes descifrar el tráfico y obtener acceso a la red.
4. **Sin servicio de seguridad (Red Abierta):**
   * **Seguridad:** No ofrece ninguna protección.
   * **Características:** La información se transmite en texto plano, lo que la hace vulnerable a la interceptación por parte de cualquier persona con un dispositivo Wi-Fi dentro del alcance. No hay autenticación ni cifrado.
5. A ud se le solicita establecer un enlace punto a punto wireless entre ciudad universitaria en el cerro San Javier y la quinta agronómica. Para ello dispone de torres de 15 metros y dos opciones de equipos para adquirir (Powerbeam 5ac y Lite beam 5ac).
   1. Se le solicita un enlace que funcione a por lo menos 250Mbps con un ancho de canal de 40Mhz al menor precio posible. Realice una propuesta de los equipos a utilizar indicando precios estimados (mercado libre) y performance esperada del enlace. (puede utilizar [https://link.ui.com](https://link.ui.com/)) .

Los equipos a utilizar serían un PowerBeam 5AC 400 ISO y LiteBeam 5AC LR cuyos costos en mercado libre se encuentran a 279.990 y 229.000 pesos respectivamente. Con una potencia de 25 dBm, la performance esperada es de 275 Mbps trabajando en un canal con un ancho de 40 MHz.

* 1. ¿Cómo varían la capacidad del canal y la señal del enlace al cambiar entre 20, 40 y 80 Mhz de ancho de canal?

Podemos que a medida que aumentamos el ancho de banda del canal, la capacidad del mismo va aumentando.

* 1. ¿Qué contras ve a utilizar un ancho de canal demasiado alto?

Utilizar un ancho de canal demasiado alto (como 80 MHz, o incluso 160 MHz si el equipo lo soporta) presenta varias contras importantes, especialmente en entornos del mundo real:

Al usar un canal más ancho, estás ocupando una porción más grande del espectro de radio. Esto aumenta drásticamente la probabilidad de **chocar con otras redes Wi-Fi** y equipos inalámbricos no-Wi-Fi. Además, ocupan gran parte del ancho del canal disminuye los canales "libres" disponibles para otros enlaces o puntos de acceso en la zona, lo que puede llevar a una **saturación del espectro** y a que todos los dispositivos funcionen peor.

Otra desventaja es que un ancho de canal más amplio significa una **menor sensibilidad del receptor y** una **peor relación señal/ruido (SNR)** ya que a medida que aumentas el ancho de canal, también estás "escuchando" una banda de frecuencia más amplia. Esto significa que **recoges más ruido ambiental**. Por lo tanto se quiere de una señal mas potente.

1. A ud se le solicita cubrir un edificio de 5 pisos con redes wifi una para cada piso. Se decide utilizar equipos norma N ubicando uno por piso. ¿Cómo asignaría los canales a cada AP para evitar o disminuir los problemas dados por el solapamiento entre las wlan?

Los canales en la banda de 2.4 GHz que no se solapan son los canales 1, 6 y 11. Por lo tanto, colocaría en el primer piso el canal 1, en el piso 2 el canal 6 y en el tercer piso el canal 11. Luego, debemos repetir los canales. En el 4 piso colocaría nuevamente el canal 1 ya que hay dos pisos de diferencia lo que hace que se afecte en menor medida con el primero. Con el mismo razonamiento, asignaría el canal 6 en el piso 5.

# Parte 2: Ejercicio Análisis de Trama 802.11

Aclaración 1: Acerca de la captura de paquetes WLAN con Wireshark:

Wireshark hace uso de las librerías libpcap o winpcap en windows para capturar tráfico de red. Las librerías winpcap no están pensadas para integrarse con tarjetas inalámbricas, por lo que directamente no ofrecen soporte para capturar tráfico WiFi con Wireshark. Las limitaciones de captura de paquetes WiFi en Windows dependen de Winpcap y no propiamente de Wireshark.

El Sniffer WiFi de Acrylic también permite capturar paquetes WiFi en modo monitor con Wireshark desde Windows (en las versiones más actuales de Wireshark 3.0.0 o superior) y con otros productos de Acrylic Wi-Fi como Heatmaps o Professional. Debido a que fue diseñado para ser una alternativa

económica y fácilmente configurable al hardware específico tipo AirPCAP puede recuperar todos los datos disponibles con tarjetas de este tipo incluyendo los valores SNR y además siendo compatible con los últimos estándares 802.11ac con todos los anchos de banda (20, 40, 80 y 160 MHz).

Uds. lo pueden instalar en modo evaluación y corroborar si es que soporta la placa WIFI de sus notebooks. En caso afirmativo podrán capturar paquetes 802.11.

Debido a que la cátedra supone que no todos cuentan con una notebook con placa WIFI, se adjunta a este práctico un archivo de capturas de tráfico inalámbrico (Http.cap), para poder responder las preguntas del Trabajo Práctico.

Aclaración 2: ¿Qué es PPI?

Cuando se capturan datos de red en vivo, a menudo es útil recoger información adicional y proporcionarla junto con los datos de los paquetes. El método tradicional para hacerlo es anteponer a cada PDU una cabecera de meta información (a menudo llamada pseudocabecera). Las implementaciones actuales incluyen información como Información de radio 802.11, ID de usuario del servidor de acceso y dirección del enlace punto a punto.

La cabecera de información por paquete (PPI) es un formato de cabecera de meta información general y extensible desarrollado originalmente para proporcionar información de radio 802.11n, pero que también puede manejar otra información.

Comienzo del Ejercicio Análisis de trama 802.11:

1. Inicie el analizador “Wireshark” y abra el archivo que le entregará la cátedra: “Http.cap”
2. Despliegue el Frame 1. ¿Qué protocolo en capa física y que protocolo encapsula en capa MAC?

Usa el protocolo 802.11n.

1. Expandir “ppi” (per packet information Header). Abra “802.11 – Common” - ¿En qué velocidad y frecuencia está trabajando el canal?, ¿Cuáles son los valores dBm de la señal y del ruido?

Está trabajando a 300 Mbps y una frecuencia de 2422 GHz [2.4 GHz 3].

Los valores de la señal y el ruido en dBm es -56 y -96 respectivamente.

1. Expandir “802.11 – MAC+PHY, ¿Cuántas antenas tiene el dispositivo? ¿Cuál antena no está recibiendo datos?

El dispositivo tiene 4 antenas. La antena que no recibe datos es la número 3 ya que el valor de dBm de señal de la antena -128 que indica inválido.

1. Expandir “802 radio information” ¿Qué protocolo está usando el dispositivo? ¿Qué significa HT?

"PHY type: 802.11n (HT)" significa que la trama de Wi-Fi fue transmitida usando el estándar 802.11n con sus capacidades de **Alto Rendimiento (High Throughput)** activadas, lo que permite velocidades de datos superiores gracias a tecnologías como MIMO y canales de 40 MHz.

Las características clave que permiten el "High Throughput" incluyen:

* **MIMO (Multiple-Input, Multiple-Output):** El uso de múltiples antenas en el transmisor y el receptor para enviar y recibir múltiples flujos de datos simultáneamente. Esto aumenta drásticamente la capacidad de datos sin requerir más espectro.
* **Channel Bonding (Canales de 40 MHz):** La capacidad de combinar dos canales adyacentes de 20 MHz para formar un canal de 40 MHz, duplicando así el ancho de banda y, por lo tanto, la capacidad de datos.
* **Short Guard Interval (SGI):** Una opción para reducir el tiempo entre símbolos de datos, lo que permite transmitir más datos en el mismo período de tiempo.

1. Expandir “Frame Control Field”. Diga los valores del campo Version, Type y SubType. ¿Qué significan?

### 1. Version: 0

* **Significado:** Este campo indica la versión del protocolo IEEE 802.11 que se está utilizando.
* **Valor 0:** Prácticamente en todas las implementaciones modernas de Wi-Fi, este campo siempre tiene un valor de **0**. Esto se debe a que las especificaciones de Wi-Fi han mantenido la misma estructura básica del encabezado de la trama MAC. Si bien hay extensiones y mejoras, la versión fundamental del formato de la trama se ha mantenido consistente.

### 2. Type: Data frame (2)

* **Significado:** Este campo de 2 bits clasifica la trama en una de las tres categorías principales de tramas 802.11.
* **Valor 2 (Data frame):** Indica que esta trama es una **trama de datos**. Las tramas de datos son las que transportan la información real del usuario (por ejemplo, paquetes IP que contienen navegación web, correo electrónico, streaming, etc.).
* **Otras categorías (no visibles en tu ejemplo):**
  + **0 (Management frame):** Utilizadas para la gestión de la red inalámbrica (ej. beacon frames para anunciar una red, probe requests/responses para buscar redes, tramas de autenticación y asociación).
  + **1 (Control frame):** Utilizadas para controlar el acceso al medio y para las operaciones de retransmisión (ej. Request to Send (RTS), Clear to Send (CTS), Acknowledgement (ACK)).

### 3. Subtype: 8

* **Significado:** Este campo de 4 bits proporciona una clasificación más específica (un "subtipo") dentro de la categoría de trama definida por el campo "Type".
* **Valor 8:** Cuando el "Type" es "Data frame" (2), un "Subtype" de **8** corresponde a una **trama de datos QoS (Quality of Service)**.
  + **QoS Data frames:** Son tramas de datos que incluyen un encabezado de QoS, lo que permite priorizar ciertos tipos de tráfico (por ejemplo, voz y video) sobre otros (como la navegación web o la descarga de archivos). Esto es fundamental en redes modernas para asegurar un buen rendimiento en aplicaciones sensibles a la latencia.
* **Otros subtipos comunes para tramas de datos (no visibles en tu ejemplo):**
  + **0 (Data):** Una trama de datos simple sin capacidades QoS.
  + **4 (Null Function - No Data):** Una trama usada para indicar que un dispositivo sigue activo pero sin enviar datos.
  + **12 (QoS Null - No Data):** Similar a Null Function, pero con capacidades QoS.

1. Expandir Flags. ¿Cuánto vale To DS y From DS? ¿Hay más fragmentos?

To DS: vale 1 y From DS vale 0. Esto significa que la trama proviene de una estación inalámbrica hacia un AP para ir **hacia el Sistema de Distribución**.

Podemos ver que las flags indican que es el último fragmento.

1. De acuerdo a los valores que posee To DS y From DS, explique el valor de los campos DA, RA,

SA y TA.

 **DA (Destination Address):** La dirección MAC del **destino final** del paquete de datos en la capa de enlace.

 **RA (Receiver Address):** La dirección MAC del **receptor inmediato** de la trama por el aire (el siguiente salto físico en el medio inalámbrico).

 **SA (Source Address):** La dirección MAC del **originador final** del paquete de datos.

 **TA (Transmitter Address):** La dirección MAC del **transmisor inmediato** de la trama por el aire (el que la está enviando en ese momento).

Tanto SA como TA contienen la dirección de la estación que envía el paquete al AP. RA contiene la dirección del AP al que está conectada la estación emisora y DA es la dirección de la estación receptora final.

1. Expandir LLC. ¿Cuál es el protocolo de red que está encapsulado en este Frame Wireless?

¿Tiene alguna diferencia con el protocolo LLC de las redes cableadas? ¿Qué puede concluir?

El protocolo que está encapsulado es IPv4. Este es el mismo que en redes cableadas ya que La subcapa LLC fue diseñada para proporcionar una **interfaz uniforme y agnóstica al medio** para los protocolos de capa superior (como IP), independientemente de la tecnología de acceso al medio (MAC) subyacente.

# Ejercicio Optativo: cálculo de factibilidad de enlace entre su casa y el edificio más alto de Tucumán (San Martín 930) de 90 mts. de altura

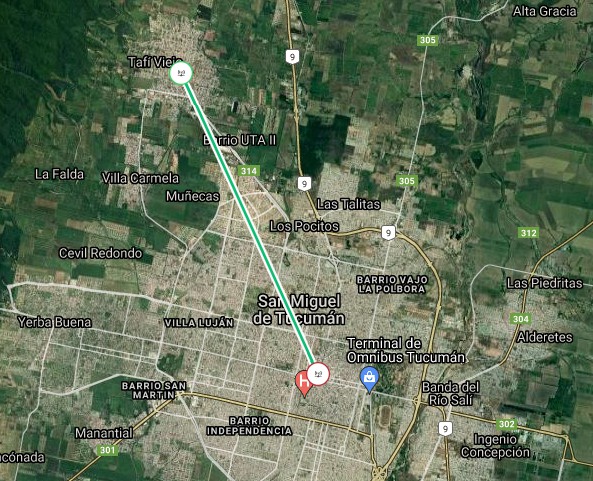
Para llevar a cabo este ejercicio utilice la herramienta de UBIQUITI airLink, el cual es un software de simulación gratis, diseñado por el fabricante para realizar enlaces PTMP y PTP. Es una aplicación Web muy intuitiva

1. Ingrese a la página: http:// link.ui.com
2. Ingrese en la parte superior derecha al Login, cree una cuenta, y valide con su mail
3. Inicie sesión con la cuenta que acaba de crear
4. Agregue un enlace punto a punto entre su casa y el Edificio Torre San Martin (San Martin 930 San Miguel de Tucumán) por O O. Entre los equipos a elegir en ambas puntas, pruebe con Lite Beam 5AC. Juegue con las alturas de las antenas y la potencia de la señal.

Ejemplo:

Este es un ejemplo de un enlace entre el centro de Tafí Viejo y el edificio más alto de Tucumán.

En la siguiente Figura 1 se puede apreciar una vista del enlace generado entre un punto ubicado en la calle 9 de Julio al 400 de la Ciudad de Tafí Viejo y el punto ubicado en San Martín 930.



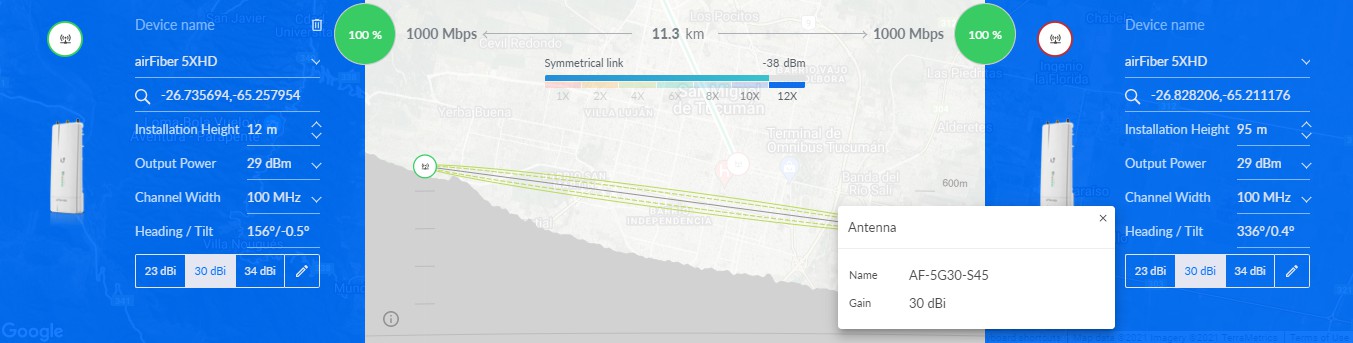
Figura 1: Vista general del enlace entre el Centro de T. Viejo y Edificio San Martín 930 Respecto al análisis detallado del enlace, podemos ver la Figura 2:

Figura 2: Vista detallada del enlace

Acá se puede observar que el extremo de Tafí Viejo está a 12 m de altura, y el extremo del Edificio San Martín 930 está ubicado a 5 mts. del último piso, es decir 95 mts. de altura. Se eligieron equipos airFiber 5XHD de Ubiquiti. Estos equipos tienen un ancho de banda del canal de 100 MHz y la antena AF-5G30-S45 una ganancia de 30 dBm

En cuanto al gráfico del medio, se puede concluir que el enlace tiene 11,3 Km, el enlace un nivel de energía de la señal -38 dBm, la velocidad del enlace puede llegar hasta los 1 Gbps, y se puede apreciar en forma clara que con las alturas a que fueron ubicadas las antenas no existe ningún obstáculo, e inclusive se respeta la zona de Fresnel (explicada oportunamente en el módulo 5).belu

Por último, es recomendable recorrer el mapa siguiendo en enlace para detectar si es que pudiera haber algún obstáculo que el aplicativo no esté detectando. La Figura 3 muestra parte de ese recorrido.

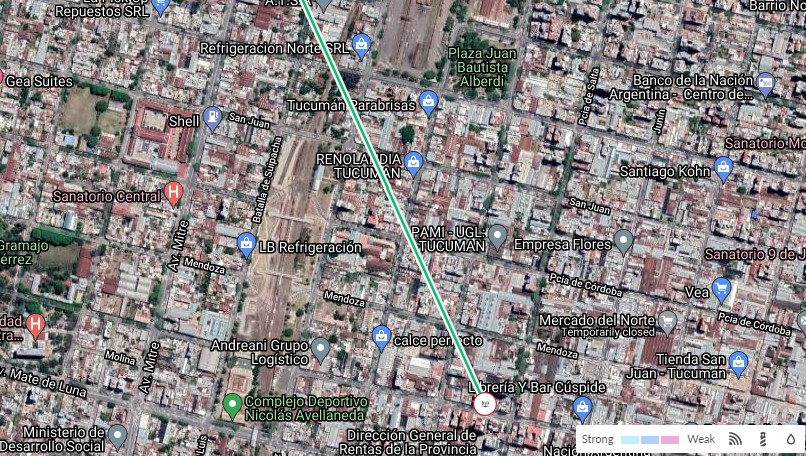


Figura 3: Analizando probables obstáculos en la línea del enlace

Identificar MDF

Identificar IDF

Definir normas entre MDF e IDF.