FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

DESARROLLO DE UNA GUÍA DE LABORATORIO PARA EL USO DE DEVNET EN ENTORNOS ACADÉMICOS

AUTORES

Mauricio Alejandro Landázuri Vega

Pablo Alejandro Verdesoto Avilés

AÑO

2020

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

DESARROLLO DE UNA GUÍA DE LABORATORIO PARA EL USO DE DEVNET EN ENTORNOS ACADÉMICOS

Trabajo de Titulación presentado en conformidad a los requisitos establecidos para optar por el título de Ingeniero Electrónico y Redes de Información.

Profesor Guía

Ángel Gabriel Jaramillo Alcázar

Autores

Mauricio Alejandro Landázuri Vega

Pablo Alejandro Verdesoto Avilés

Año

2020

DECLARACIÓN PROFESOR GUÍA.

"Declaro haber dirigido el trabajo, Desarrollo de una guía de laboratorio para el uso de Devnet en entornos académicos, a través de reuniones periódicas con los estudiantes Mauricio Alejandro Landázuri Vega y Pablo Alejandro Verdesoto Avilés, en el semestre 202020, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

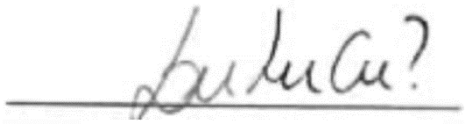
Ángel Gabriel Jaramillo Alcázar

Magister en Gerencia de Sistemas y Tecnologías de la Información

CI: 1715891964

DECLARACIÓN PROFESOR CORRECTOR.

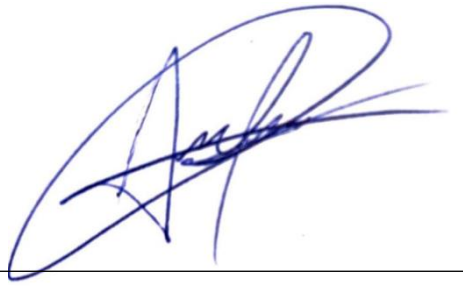
"Declaro haber revisado este trabajo, Desarrollo de una guía de laboratorio para el uso de Devnet en entornos académicos, de los estudiantes Mauricio Alejandro Landázuri Vega y Pablo Alejandro Verdesoto Avilés, en el semestre 202020, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación"

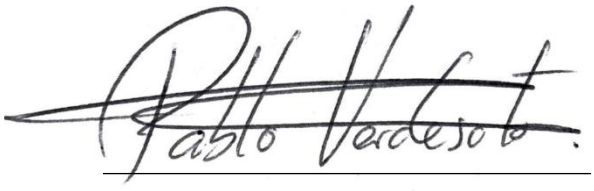


Luis Santiago Criollo Caizaguano
Máster en Redes de Comunicación
CI: 1717112955

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE.

“Nosotros, Mauricio Alejandro Landázuri Vega y Pablo Alejandro Verdesoto Avilés, declaramos que este trabajo es original, de nuestra autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”





Mauricio Alejandro Landázuri Vega

1725031965

Pablo Alejandro Verdesoto Avilés

1716755036

AGRADECIMIENTOS

Agradezco a Dios por permitirme continuar con mis estudios a pesar de las situaciones difíciles, a mis padres por su ejemplo y apoyo durante todo este tiempo de nuevos retos y sacrificios. A mi tía por su ayuda y apoyo con los cuales no hubiese terminado mi carrera.

A mi tutor Ángel Jaramillo por su guía, amistad y predisposición para que logre cumplir mis metas.

AGRADECIMIENTOS

En especial, a mi padre Juan Verdesoto por apoyarme en todas las decisiones que han llegado al punto de mi vida y ayudarme alcanzar este sueño. A mi hermano y a mi madre por apoyarme, guiarme, estar conmigo y con todo el amor incondicional.

A mi tutor Ángel Jaramillo quien con su experiencia y motivación llevó a tener una nueva proyección en el camino del conocimiento.

DEDICATORIA

Mi tesis dedico a mi padre Omar Landázuri y a mi madre Cecilia Vega por sus esfuerzos y fuerza para continuar ante cualquier adversidad.

DEDICATORIA

Mi tesis dedico con todo amor a mis padres Juan Verdesoto y Elena Avilés por su esfuerzo, a mi hermano Juan Verdesoto por su apoyo y motivación. A mis abuelos Antonio Verdesoto y Maria Luisa Riera que con su abrazo y calidez siempre estarán conmigo.

RESUMEN

Dentro del ámbito de las redes y las comunicaciones se han llevado grandes beneficios gracias a los diferentes cambios, impulsando un gran avance hacia la productividad en los diferentes entornos.

Todo esto conlleva a un mundo más tecnológico incluso llegando a tener una nueva revolución tecnológica, estos cambios han llegado a mejorar y simplificar los entornos. Por ejemplo, con nuevas técnicas de automatización o juntar grandes aristas como las redes de información y los lenguajes de programación. A la par esto ha creado nuevas amenazas y así el nacimiento de nuevos conceptos de seguridad para prevenir, meditar y contrarrestar posibles intentos maliciosos.

Lo que se pretende conseguir es aportar buenas prácticas enfocadas a los nuevos equipos que se encuentran en el mercado, de esta manera innovar y brindar soluciones con altos niveles tecnológicos vanguardistas.

Una de las principales empresas dedicadas a crear equipos y crecer en infraestructura de redes es Cisco, que con mira al futuro crea el programa Cisco DevNet, el cual ofrece una gran variedad de repositorios y librerías prácticas para poder llevar el entorno de las redes hacia un nuevo camino con la programación.

La idea primordial es que estas prácticas sirvan como retroalimentación para varias materias alineadas a la carrera de ingeniería en redes de información y así suplir las necesidades académicas, además de lograr que los futuros estudiantes tengan un acercamiento con equipos y laboratorios en redes orientadas al área de Cisco DevNet. Estas nuevas prácticas buscan complementar el conocimiento para lograr la familiarización de ambientes diferentes tales como, seguridad con AMP, networking e IOT con su línea inteligente Meraki.

ABSTRACT

Within the area of networks and communications, great benefits achieved thanks to the different changes, driving a great advance towards productivity in different environments.

All this leads to a more technological world even having a new technological revolution, these changes have come to improve and simplify environments. For example, with new automation techniques or joining great edges such as information networks and programming languages. At the same time, this has created new threats and thus the birth of new security concepts to prevent, meditate and counteract possible malicious attempts.

What is intended to achieve is to provide good practices focused on new equipment on the market, thus innovating and providing solutions with high levels of cutting-edge technology.

One of the main companies dedicated to creating teams and growing in network infrastructure is Cisco, which with a view to the future creates the Cisco DevNet program, which offers a wide variety of repositories and practical libraries to be able to take the network environment to a new way with programming. The main idea is that these practices serve as feedback for various subjects aligned to the career of engineering in information networks and thus meet the academic needs, in addition to ensuring that future students have an approach with equipment and laboratories in networks oriented to the area of Cisco DevNet. These new practices seek to complement the knowledge to achieve the familiarization of different environments such as, security with AMP, networking and IOT with its Meraki smart line.

ÍNDICE

1. Capítulo I. Introducción.

Los nuevos avances tecnológicos y acercamientos al mundo digital crean un enfoque de innovación, desarrollo y una carrera vanguardista. Estos avances llevan a una evolución por parte de las personas y su educación continua, con herramientas como Cisco DevNet que ofrece librerías y facilidades de aprendizaje.

“Es el programa de desarrolladores de Cisco que ayuda a desarrolladores y profesionales de TI para escribir aplicaciones y desarrollar integraciones con productos, plataformas y API. Incluye los productos en, redes definidas por software, seguridad, Internet de las cosas, y desarrollo de código abierto. El sitio también ofrece entornos controlados de aprendizaje, así como videos para aprender aplicaciones de codificación y prueba.” (Cisco, Cisco DevNet: APIs, SDKs, Sandbox, and Community for Cisco Developers, 2017).

La manera tradicional de administración de redes es mediante el uso de comandos o con paneles poco informativos, por esos motivos se decide diseñar un manual para impartir el conocimiento al personal docente de la Universidad de las Américas en temas de salud de redes con DNA, IOT, Cisco Meraki y prácticas desarrolladas con su respectiva documentación del paso a paso.

“Las API de Meraki hacen posible implementar y administrar rápidamente redes a escala, construir sobre una plataforma de productos de TI inteligentes conectados a la nube e interactuar con los usuarios de nuevas e innovadoras formas.” (Cisco, Cisco Meraki - Create with the Meraki Platform, 2020).

“IoT Dev Center permite conectar de forma segura sus dispositivos, extrayendo datos, con cálculos en el dispositivo final y mover datos a varias aplicaciones en su entorno distribuido para obtener el máximo valor de sus iniciativas de digitalización.” (Cisco, IoT Developer Center - Cisco Devnet, 2020).

“Cisco DNA Center está en el corazón de la arquitectura de red basada en la intención de Cisco. Cisco DNA Center admite la expresión de la intención comercial para casos de uso de la red, como las capacidades de automatización de base en la red empresarial. Las características de análisis y aseguramiento de Cisco DNA Center proporcionan visibilidad de extremo a extremo en la red con un contexto completo a través de datos e información.” (Cisco, Cisco DNA - Cisco Devnet, 2020).

1.1 Alcance

El alcance del presente trabajo de titulación es elaborar un manual de usuario y la resolución de guías prácticas que permita la apertura de esta metodología dentro de una nueva asignatura, la asignatura estaría enfocada al campo de DevNet, y posteriormente realizar la impartición del conocimiento a los futuros estudiantes de la Universidad de las Américas.

Las guías serán enfocadas en los temas de *networking* y seguridad de redes, temas en que se basa la malla actual, con detalle dentro de los puntos que se desea impartir hacia los estudiantes y el conocimiento que debe tener el docente instructor previo. Las prácticas de trabajo o laboratorios serán en conjunto con las guías prácticas las cuales cumplirán como refuerzos para mejorar el conocimiento adquirido y mostrar su implementación en entornos reales.

Se utilizará los espacios reservados provistos por Cisco, estos entornos son totalmente virtualizados y en los cuales se puede ir ejecutando diversas pruebas para llegar a cumplir las guías de laboratorio propuestas para la universidad. Adicional dentro de los diferentes equipos físicos propuestos por la universidad, se podrá implementar las prácticas con el fin de tener un visionamiento claro dentro de un entorno real no alejado a la realidad del sector laboral o empresarial.

1.2 Justificación

Con respecto al proyecto, se busca realizar un manual de usuarios para el entorno académico con la resolución de laboratorios enfocados principalmente en *networking* y seguridad, debido que en la actualidad son puntos principales en el sector de las comunicaciones, adicionalmente de la protección de activos evitando brechas de información.

El proyecto engloba temas de suma importancia relacionados con la carrera que hemos seguido para fomentar el nivel académico, este proyecto contempla las bases aprendidas en la carrera, llevando a un nuevo nivel que está en auge a nivel empresarial y lo cual se ha convertido en oportunidad de mejora y crecimiento personal.

El conocimiento de programación e implementación con equipos Cisco es fundamental, así como la investigación de temas nuevos como integración y despliegue de Redes definidas por Software o detección avanzada de amenazas. Estos temas de investigación estarán enfocados a la integración de todos los sistemas para su correcto funcionamiento y así posteriormente sean utilizados dentro de la unidad académica de la Universidad de las Américas.

1.3 Objetivo General

- Desarrollar una guía de uso e implementación de Cisco DevNet en un entorno académico.

1.4 Objetivos específicos

- Desarrollo de una guía de laboratorio orientado a entornos de Networking (Equipos Meraki).
- Determinar las prácticas de laboratorio orientados a entornos de Networking Cisco DNA.

- Implementar las guías de laboratorio orientadas a entornos de redes definidos para dispositivos IOT.

2. **Capítulo II. Marco Teórico.**

2.1 Cisco DevNet

Es una plataforma con inicios en el año 2014 gracias a Susie Wee, que ofrece repositorios, herramientas y código libre los cuales permiten la innovación, desarrollo y acercamiento a los usuarios de TI hacia la creación de soluciones en redes de infraestructura automatizadas.

Los temas que se encuentra son:

- IoT
- Cloud
- Networking
- Data Center
- Security
- Mobility
- Analytics
- Services

Las tecnologías usadas para las prácticas son Networking enfocado en Meraki, IoT y Cisco DNA.

2.2 Cisco DevNet Networking

Se enfoca en integrar las redes con soluciones como la nube, automatizando aplicaciones o controladores desde el uso de API e interfaces.

Gracias a Python se puede optimizar desde el día 0 hasta tener una automatización completa, con sistemas Plug and Play. Simplificando las configuraciones de manera completa y online, con plantillas para múltiples plataformas gracias a sus integraciones con Linux y Dockers. Además de la

facilidad de uso de la API para el sistema operativo IOS XE u integración con Meraki API.

2.3 Cisco Meraki

Es la línea de productos enfocados en paneles informativos para la administración y despliegue de redes en cualquier parte del mundo. Se puede visualizar las organizaciones, redes, dispositivos, reglas, subredes VLAN, etc.

“Meraki colabora para poder reducir el proceso de descontinuación y ayuda a con un control remoto en los equipos administrados desde la nube y sin restricciones, indicando el estado de la red, el uso en el ancho de banda y ofrece una experiencia in situ para el personal de TI como el resto de los colaboradores.” (Cisco Meraki Blog, 2020)

Automatiza los equipos en base al uso de API permitiendo a los desarrolladores generar tareas de manera rápida fácil y simple, se basa en el protocolo HTTP con datos de tipo JSON y permite la integración con Python para realizar código en base a los requerimientos para una red autómata propia.

2.4 Cisco IoT Dev Center.

IoT (Internet of Things) es una tecnología que consiste en la interconexión digital de dispositivos finales mediante internet. Este concepto comprende un sistema donde internet está conectado al mundo físico mediante sensores instalados en dispositivos finales.

Cisco IoT DevCenter es el desarrollo en base a una nueva semántica de programación orientada al control e integración de productos Cisco hacia productos de terceros. Este nuevo diseño de tecnología se basa en Cisco DevNet el cual mediante laboratorios *Sandbox* permite explorar y desarrollar casos específicos. A demás, de la aplicación en *switching* y *routing*.

2.5 Cisco DNA (Digital Network Architecture).

Su objetivo es facilitar el análisis de datos y optimizar la gestión de redes en base a Inteligencia Artificial. Esta solución tecnológica se basa en software y un panel de control para la administración de red.

“La red digital es la plataforma clave para los negocios digitales. Cisco DNA combina virtualización, automatización, analítica, Cloud y capacidad de programación para construir dicha plataforma cuyo acrónimo (*Digital Networking Architecture*, ADN en español) no es por casualidad; estamos transformando el ADN de la tecnología de red” (Rob Soderbery, 2016).

Las principales características de Cisco DNA son:

- Virtualización: implementación de cualquier servicio en cualquier lugar para mayor libertad de administración para las empresas.
- Automatización: facilidad para despliegue, gestión y manutención de las redes y los servicios.
- Servicios gestionados desde Cloud: unificación de políticas, integración de la tecnología Cisco y terceros, API abiertas y plataformas de desarrollo.

“Cisco DNA y Cisco DNA Center proporcionan automatización y garantía muy necesarias en la red. Las capacidades de plataforma abierta de Cisco DNA Center ofrecen el siguiente paso a la evolución de las redes.” (Cisco DNA Center, 2020)

2.6 Lenguaje Python.

Desde sus orígenes ha sido uno de los lenguajes con mayor relevancia y apego entre las comunidades de desarrolladores, hasta en la actualidad siendo usado en convergencia de equipos.

Es de código abierto para su uso y disponible para todos los sistemas operativos, especialmente para distribuciones Linux. Actualmente se encuentra en la versión 3.8.X y todavía se da soporte a la versión 2.7 que sigue en uso.

2.7 Postman.

Es una plataforma de libre uso, para el uso de API y su publicación con una simplificación de pasos al usar e integrar de manera rápida y sencilla. Colabora de manera integral con el ecosistema Cisco especialmente con DevNet, facilitando la integración de aplicaciones en la comunidad dentro de los laboratorios de práctica, ofreciendo repositorio de librerías ayudando en el desarrollo de profesionales TI. (Postman, 2020)

2.8 API (interfaz de programación de aplicaciones).

Es una interfaz que relaciona una aplicación con componentes de un sistema facilitando la comunicación entre ellos. Esto se logra mediante un intercambio de solicitudes y respuestas para el envío de información en tiempo real.

Son totalmente personalizables en base a los dispositivos que existen en el mercado, pueden ser diseñadas en base los requerimientos de empresas o negocios. Dado que son desarrolladas o aplicadas para un sistema específico en el cual su funcionamiento es mediante una clave pre compartida única o *API key*.

2.9 JSON.

Conocido como (JavaScript Object Notation) es un lenguaje de programación el cual sirve para el intercambio de datos.

Este lenguaje facilita la lectura y escritura para un ser humano ya que es simple interpretarlo en una computadora y de igual manera generarlo. A pesar de que es un lenguaje externo funciona con el resto de los lenguajes de programación como Python, C++, C#, etc. (JSON, 2020).

2.10 PowerShell.

Es un terminal de comandos basados en tareas y en lenguaje de script desarrollado en .NET. Con esto permite tener una administración del Sistema de manera básica, el cual ayuda a elevar permisos o privilegios para realizar una optimización del SO. A demás, facilita el acceso a repositorios de datos, registros y sistema de archivos. (PowerShell Microsoft Docs, 2020).

3. Capítulo III. Desarrollo e Implementación

Para el desarrollo de estas prácticas Cisco ha facilitado al público el uso de sus plataformas de aprendizaje y desarrollo, en este caso Cisco DevNet y Cisco DCloud. Estas plataformas son un repositorio con prácticas orientadas a las varias áreas ya mencionadas anteriormente. El objetivo de estas plataformas es permitir la visualización e interacción de los varios recursos, plataformas, equipos o soluciones que Cisco tiene para ofrecer.

3.1 Creación de cuenta Cisco DevNet y reserva de Sandbox.

Para el uso de la plataforma es necesario contar con una cuenta o crear una gratuita.

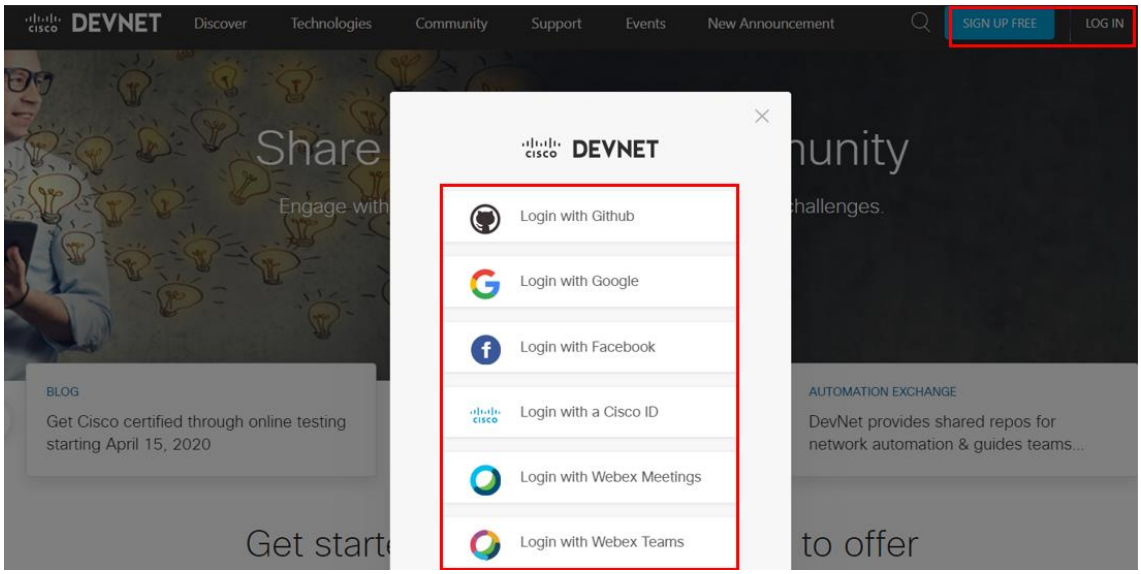


Figura 1. Acceso DevNet

Una vez dentro se visualizan los cursos, productos, reserva de laboratorios, *Sandbox*, la comunidad y guías. Para acceder, en la parte superior *Resources* se despliega el menú que expone el contenido.

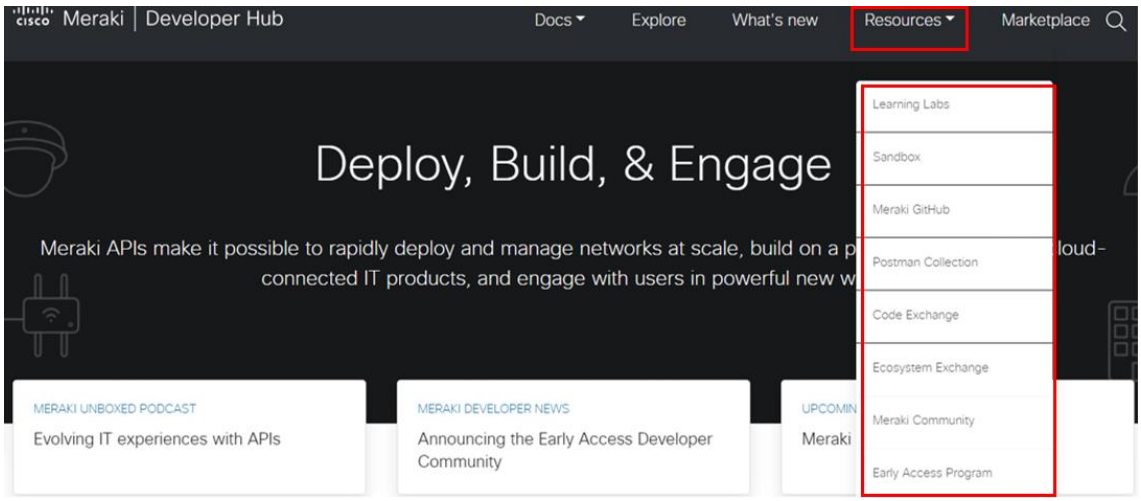


Figura 2. Recursos DevNet

Para reservar un entorno *Sandbox* se debe dirigir en el menú de inicio en *Discover* y seleccionar *Sandobox Remote Labs.* En este apartado, se encuentran

los tipos de entornos de las diferentes categorías que se encuentran disponibles para reservar.

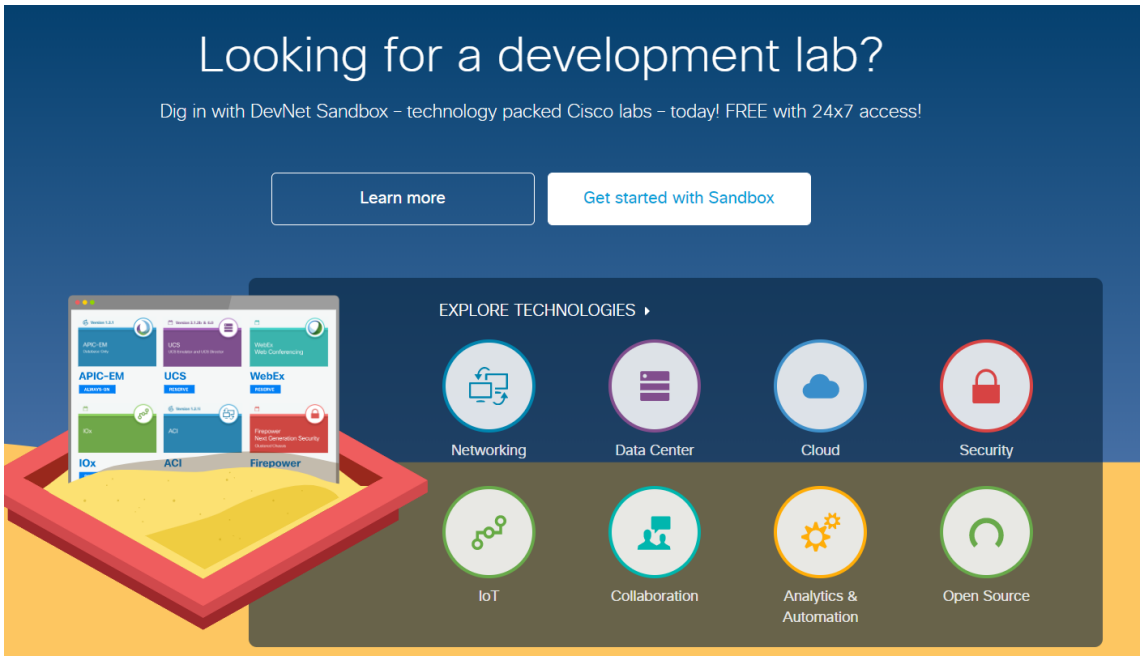


Figura 3. Menú Sandbox

Ingresando en el menú *Sandbox Labs* hay 71 entornos disponibles para reservar o visualizar. Adicionalmente, estos están divididos en algunas categorías en base a su alcance y existen laboratorios de tipo *ALWAYS-ON* que están siempre disponibles para poder utilizarlos y otros los cuales para acceder se debe hacer la reserva en el botón *RESERVE*.

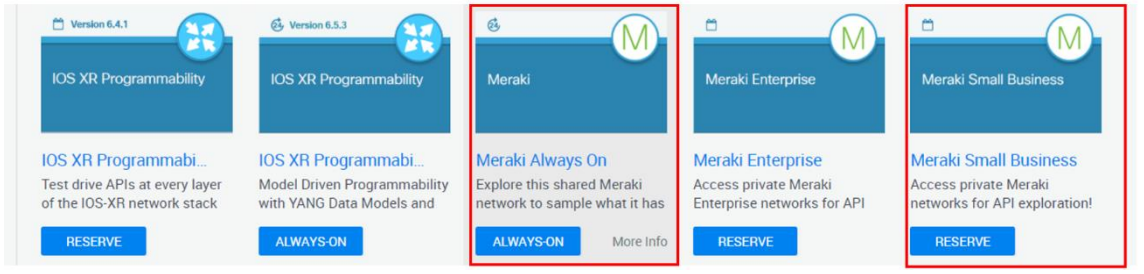


Figura 4. Reserva de Sandbox

Una vez seleccionado el *Sandbox* se debe confirmar y completar un formulario el cual mediante un pop-up solicita cierta información requerida como: el entorno, el nombre asignado y las fechas de uso.

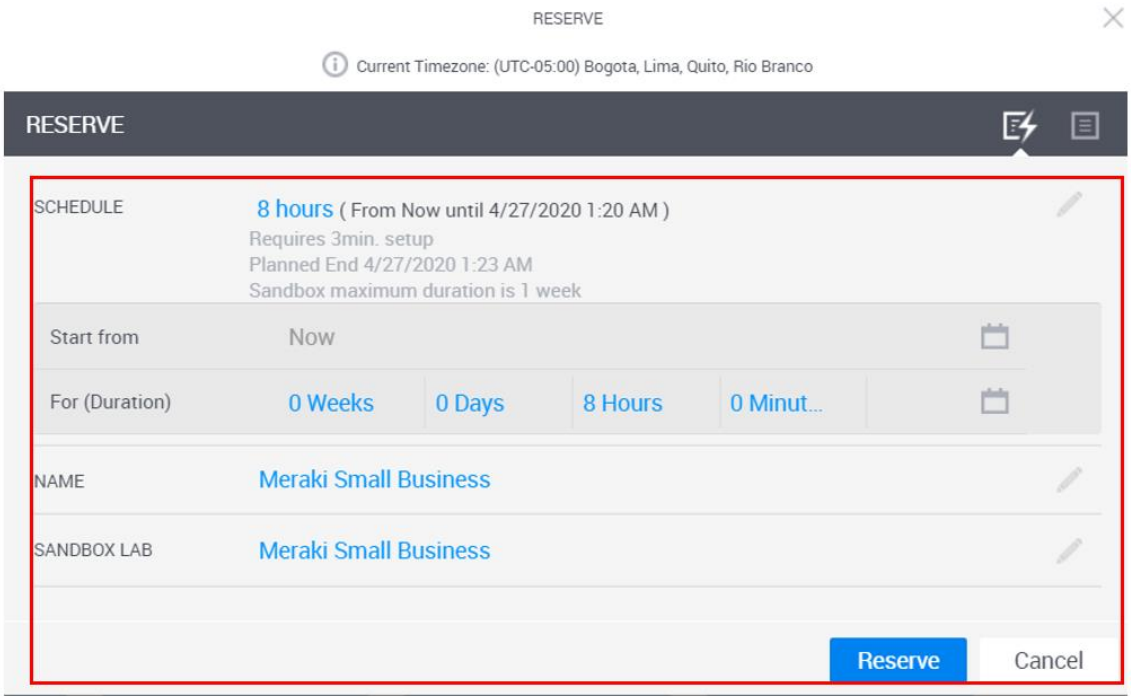


Figura 5. Reserva del Sandbox de Meraki

3.2 Panel informativo de Meraki con API.

El panel informativo o Dashboard se maneja en base a la integración de una clave API, la cual utiliza el protocolo HTTP para transporte y JSON para serialización.

Para acceder al panel informativo se lo debe realizar mediante la siguiente dirección web https://account.meraki.com/login/dashboard_login?go=%2F y con las credenciales de Cisco ID.

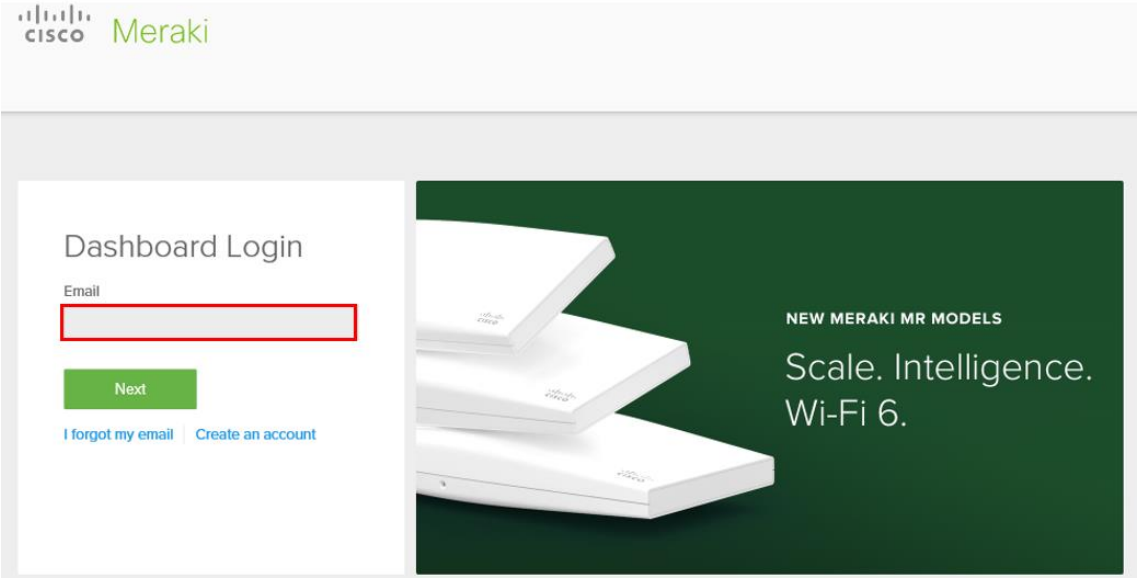


Figura 6. Ingreso Dashboard Meraki

Una vez realizado el ingreso exitoso como primera vista se muestra el acceso a las diferentes Organizaciones, en las cuales se detalla cada una con sus respectivos equipos o, si se está usando un entorno *Sandbox*.

Solo los usuarios designados como administradores tienen acceso a la consola.

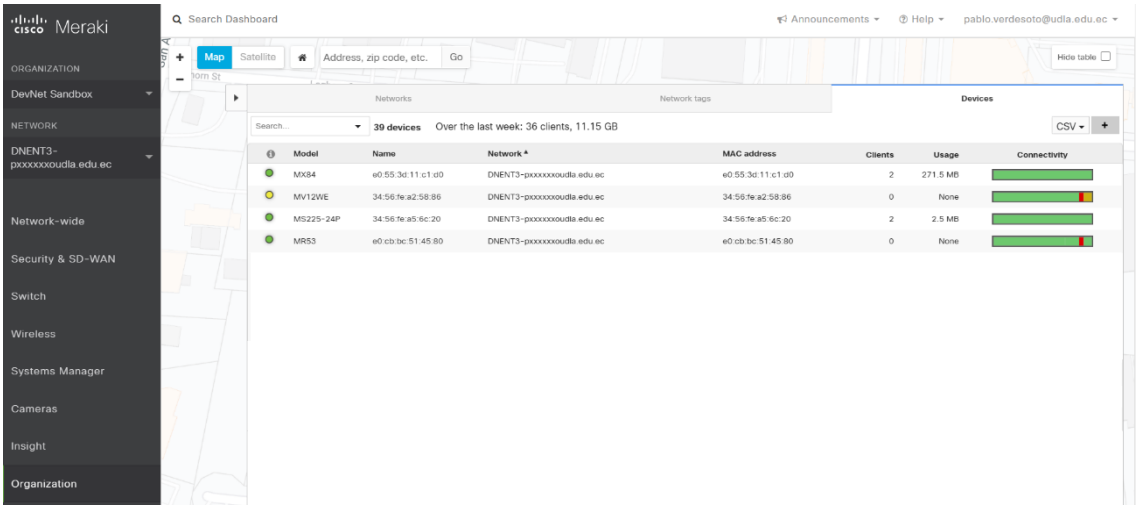


Figura 7. Dashboard Meraki

En esta consola se maneja un esquema organizativo en el cual el padre es *Organization*. Este abarca el segmento de *Network* que está constituido por diferentes redes en una organización y cada red posee sus características tales como: propiedades, VLAN, equipos, Políticas de grupos, etc.

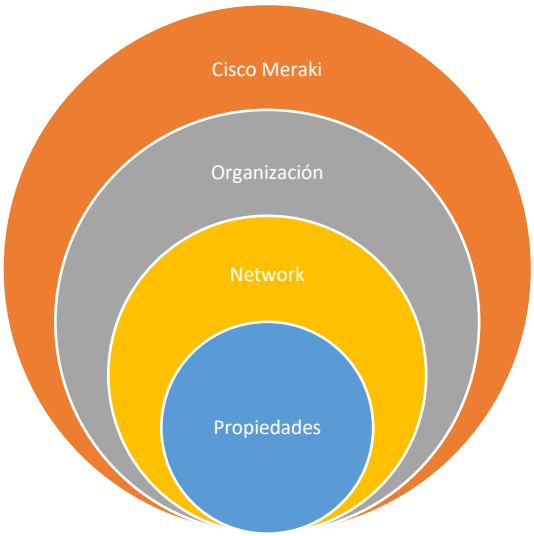


Figura 8. Jerarquía Cisco Meraki

Para poder habilitar el uso de la API para Meraki primero se debe activar su uso, para lo cual se sobrepone el cursor en el menú flotante de *Organization* y se debe seleccionar *Settings*.

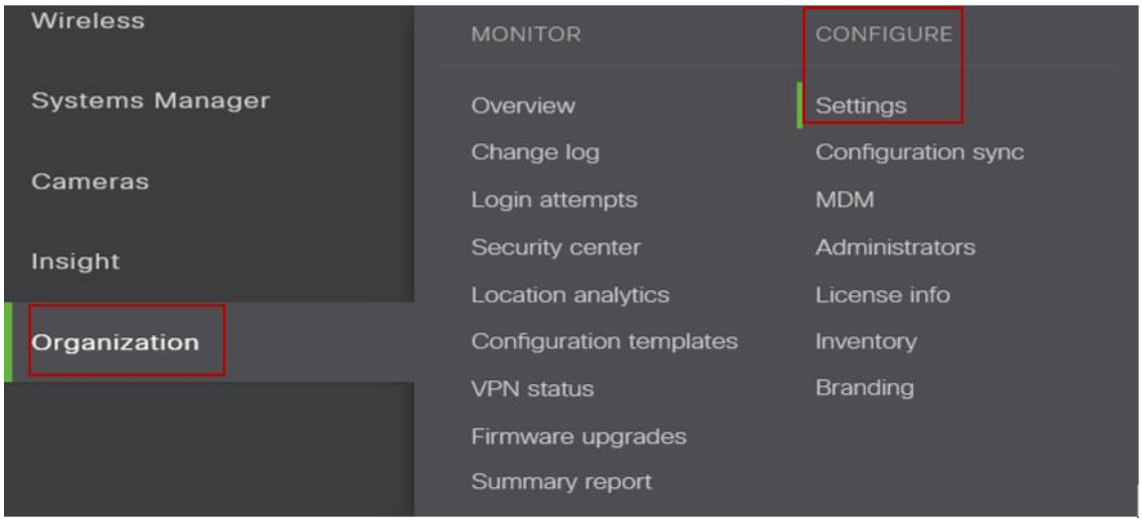


Figura 9. Menú flotante Organization

Al cargar la nueva página se debe direccionar hasta la parte inferior y se selecciona la casilla *Enable Access to the Cisco Meraki Dashboard API.*

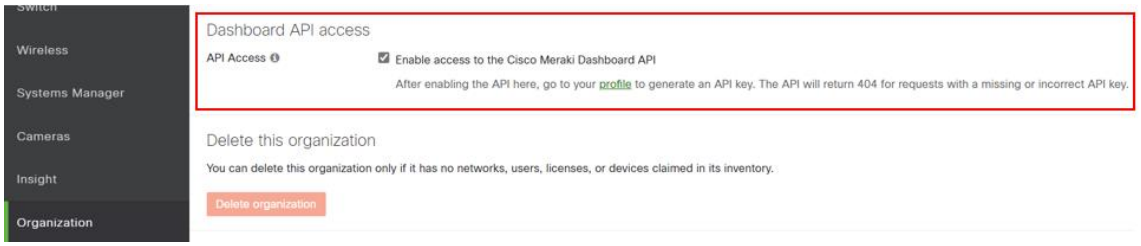


Figura 10. Habilitación de API en Menú Organization.

Con el acceso habilitado se debe generar una API key de único valor, para lo cual en la esquina superior derecha se encuentra el correo de la cuenta, al dar clic en el correo se despliega un submenú y se debe seleccionar *My profile*. Esto se puede apreciar en la Figura 11.

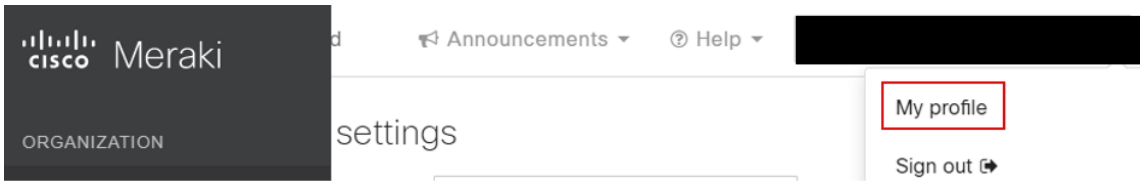


Figura 11. Ingreso My Profile

Se debe deslizar la página hasta encontrar el acceso API y se da clic en *Generate new API key.* Esto en el caso de no disponer de alguna creada anteriormente o en caso de no poder visualizar cuales están en uso. Un ejemplo de una API Key generada se puede apreciar en la Figura 12.

Figura 12. API Key

Por otro lado, Postman es una conexión entre la API y JSON, es de libre uso e incluso recomendado por DevNet ya que cuenta con una gran disponibilidad de librerías y repositorios, adicionalmente puede transformar varios lenguajes de programación como Java, C#, PowerShell, Python, etc.

Una vez descargado e instalado Postman, en la interfaz de bienvenida se puede crear una solicitud de respuesta HTTP dando clic en *Create a request*.

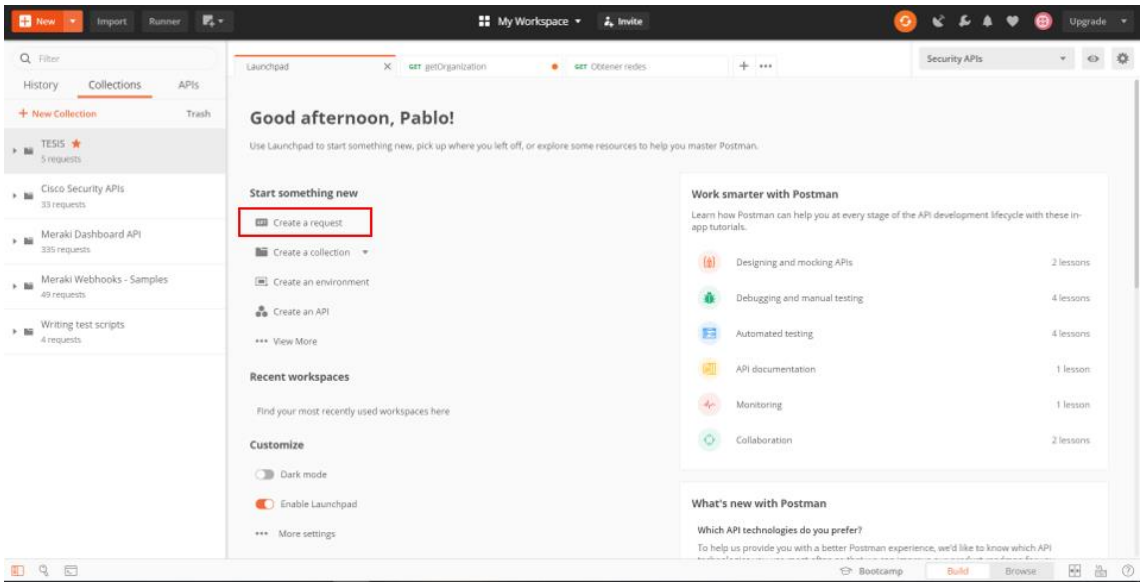


Figura 13. Postman interfaz de bienvenida.

Para poder acceder a la información a la API de Meraki se debe ingresar la solicitud a la siguiente dirección: https://api.meraki.com/api/v0/organizations.

Una vez ingresada la dirección con el valor de la API key se selecciona el tipo de solicitud para obtener una respuesta. En base a los valores ingresados se visualiza su estado, el cual puede ser:

- Si la solicitud es un GET siempre se obtiene **200 Ok**.
- Si la solicitud es rechazada devuelve un **404 Not Found**.

Esta información es la misma proporcionada por el Dashboard, pero aquí se obtiene valores propios de cada una como el ID, nombre y URL. Estos datos se pueden apreciar en la Figura 14.

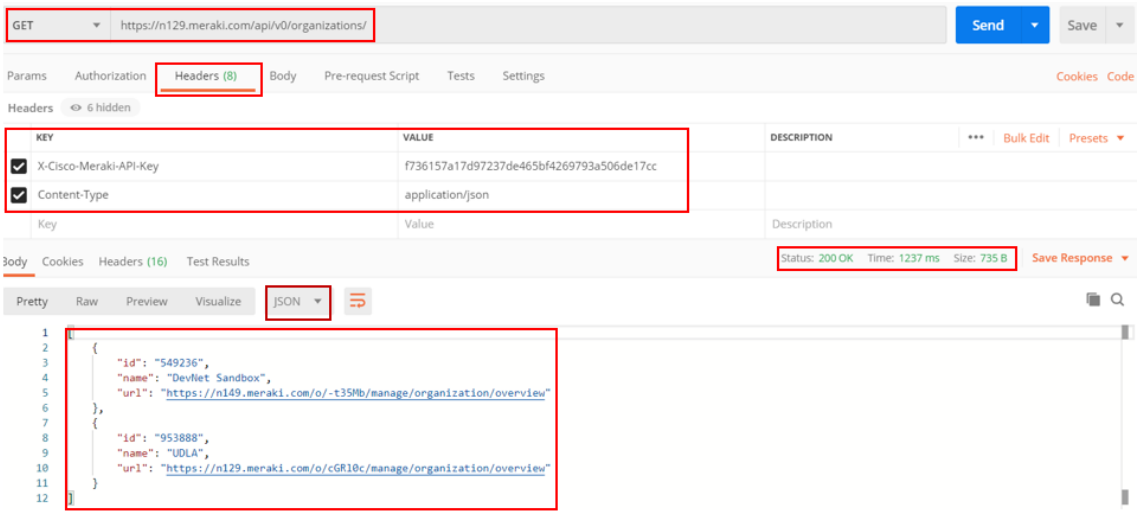


Figura 14. Visualización método GET para Organization

Con el ID de la Organización se puede obtener el resto de los componentes de una red, para lo cual se cambia la URL de la solicitud y se usa el ID propio de cada red.

De igual manera cada red que conforma una organización tiene un respectivo ID para funciones internas. *Postman* permite la ejecución de código en diferentes lenguajes por ejemplo PowerShell, el cual refleja la misma información generada

el cual esta está basado en HTTP, permitiendo su ejecución desde cualquier lugar con una conexión a internet.

En las siguientes imágenes se encuentra un paso a paso de la ejecución del código en Postman y posteriormente ejecutado PowerShell.

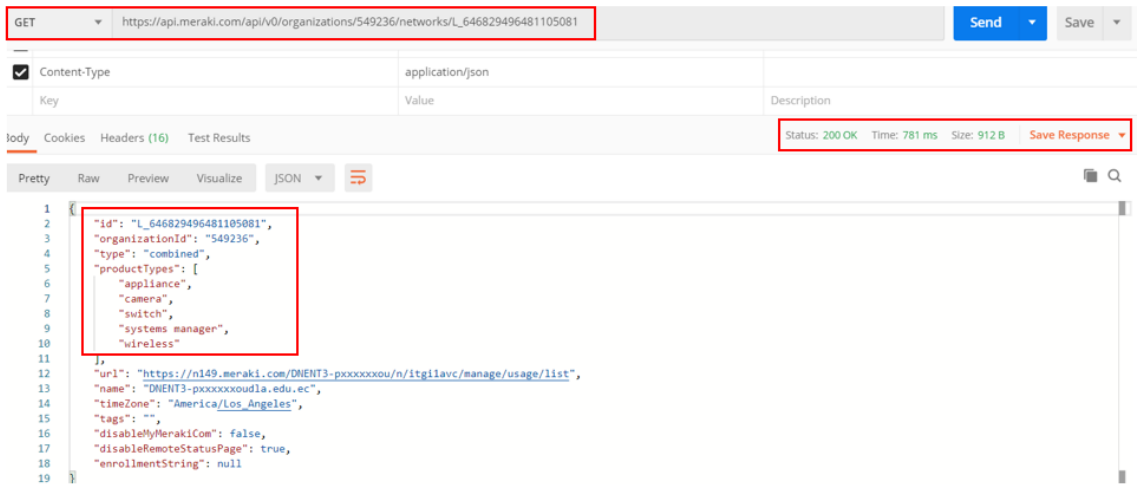


Figura 15. Método GET para Network

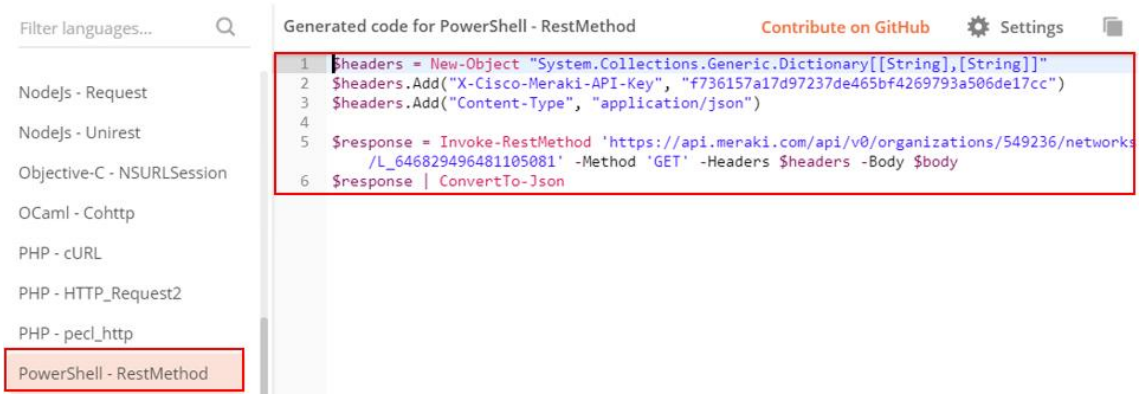


Figura 16. Generación automática de código

```
PS C:\Users\Pablo> $headers = New-Object "System.Collections.Generic.Dictionary[[String],[String]]"
>> $headers.Add("X-Cisco-Meraki-API-Key", "f736157a17d97237de465bf4269793a506de17cc")
>> $headers.Add("Content-Type", "application/json")
>>
>> $response = Invoke-RestMethod 'https://api.meraki.com/api/v0/organizations/549236/networks/L_646829496481105081' -Method 'GET' -Headers $headers -Body $body
>> $response | ConvertTo-Json
{
    "id":  "L_646829496481105081",
    "organizationId":  "549236",
    "type":  "combined",
    "productTypes":  [
                         "appliance",
                         "camera",
                         "switch",
                         "systems manager",
                         "wireless"
                     ],
    "url":  "https://n149.meraki.com/DNENT3-pxxxxxxou/n/itgi1avc/manage/usage/list",
    "name":  "DNENT3-pxxxxxxoudla.edu.ec",
    "timeZone":  "America/Los_Angeles",
    "tags":  "",
    "disableMyMerakiCom":  false,
    "disableRemoteStatusPage":  true,
    "enrollmentString":  null
```

Figura 17. Código generado para PowerShell

Con el ID propio de red se pueden realizar consultas específicas para cada una de las redes. Por ejemplo, se puede consultar el número y características de las VLAN.

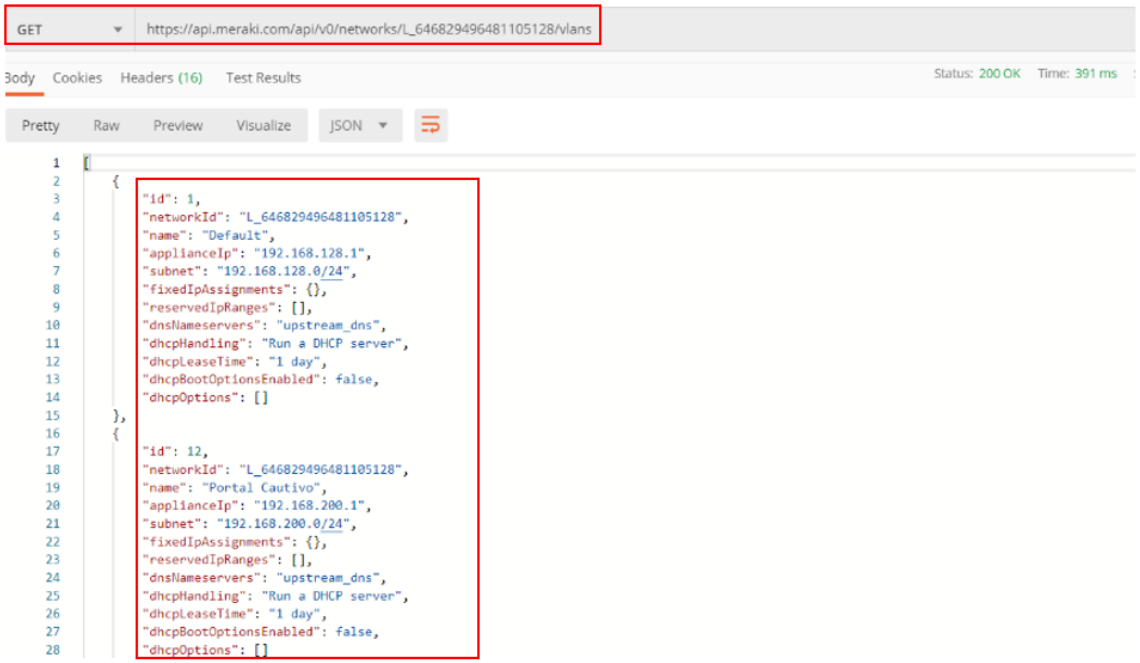


Figura 18. Consulta propiedades de VLAN

Otra consulta que se puede realizar es listar cada uno de los equipos de red y obtener sus características.

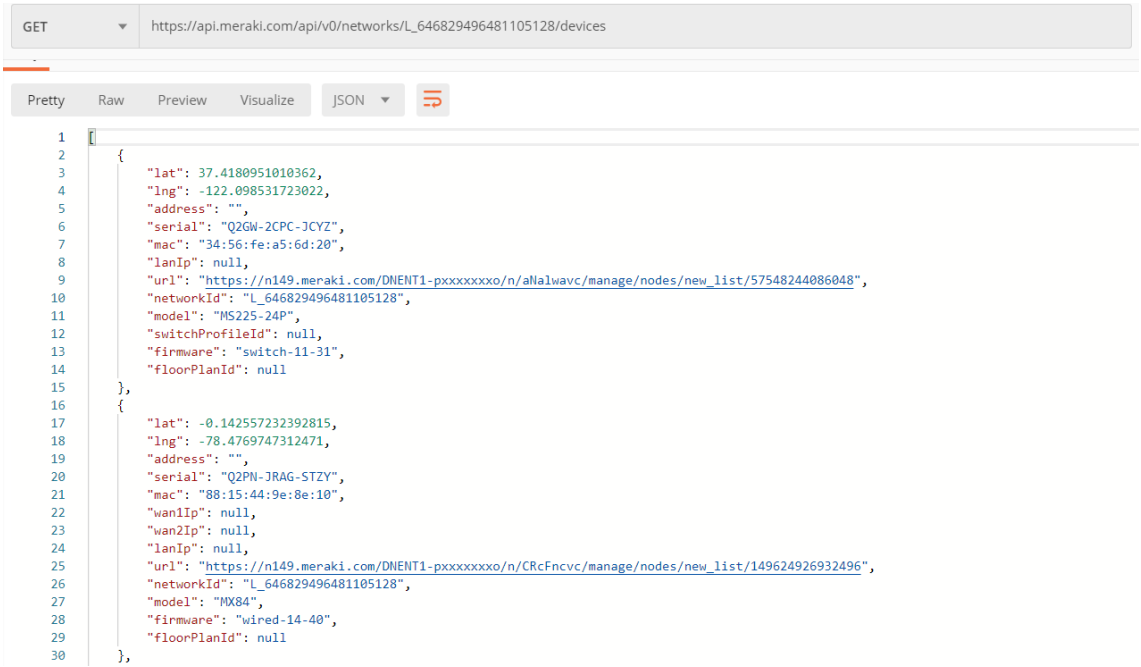


Figura 19. Obtener características dispositivos de una red

Otra consulta que se puede realizar en una red es la obtención de subredes SSID donde se puede visualizar sus parámetros, adicionalmente se logra conocer si alguna de ellas está publicada por una dirección WAN. Esto es utilizado para tareas administrativas o conexiones a servidores.

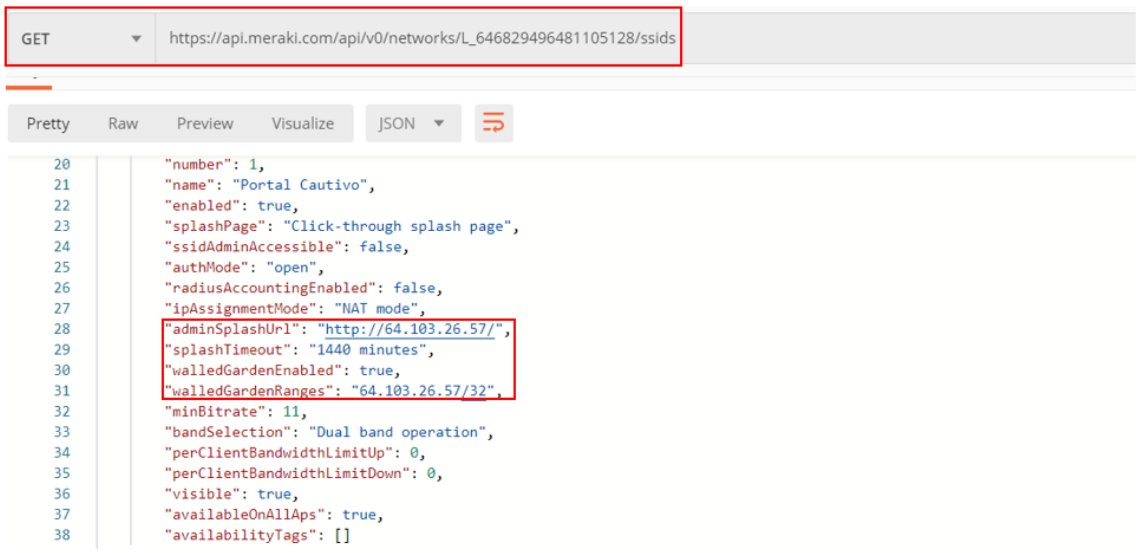


Figura 20. Consulta SSID de una subred

Mediante la consulta se puede revisar el estado de la dirección WAN y la red SSID utilizando un Ping, con esto se logra verificar que la interfaz pertenece al *Sandbox* asignado por parte de Cisco.

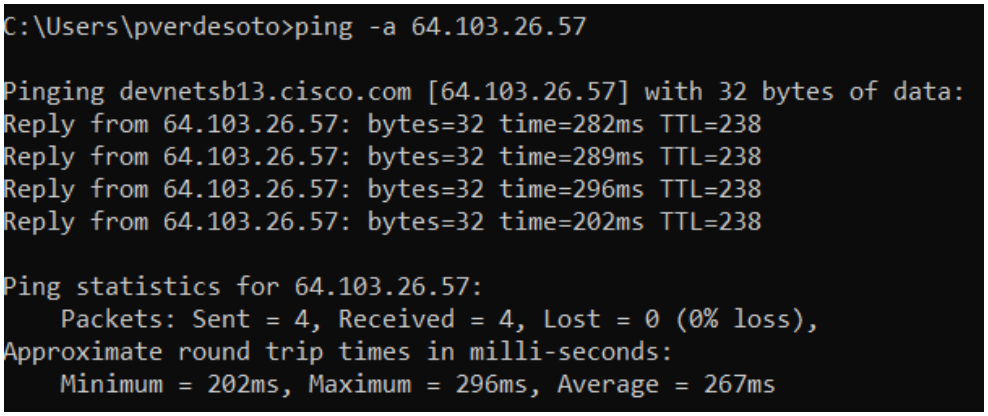


Figura 21. Respuesta de Ping a la SSID vía WAN

El método GET permite obtener información. Existen otros métodos como: POST que permite crear, PUT hacer una actualización y DELETE para eliminar.

El método POST contiene ciertas limitaciones ya que no todas las solicitudes permiten crear información por restricciones en su ingreso. Por ejemplo, se realiza una creación de una red (Network) dentro de una organización.

A diferencia del método GET, el método POST se debe incluir los parámetros solicitados. En el apartado *Body* se selecciona el tipo de formato, lenguaje y la estructura de ingreso de la información. En la Figura 22 se puede apreciar un ejemplo con el método POST.

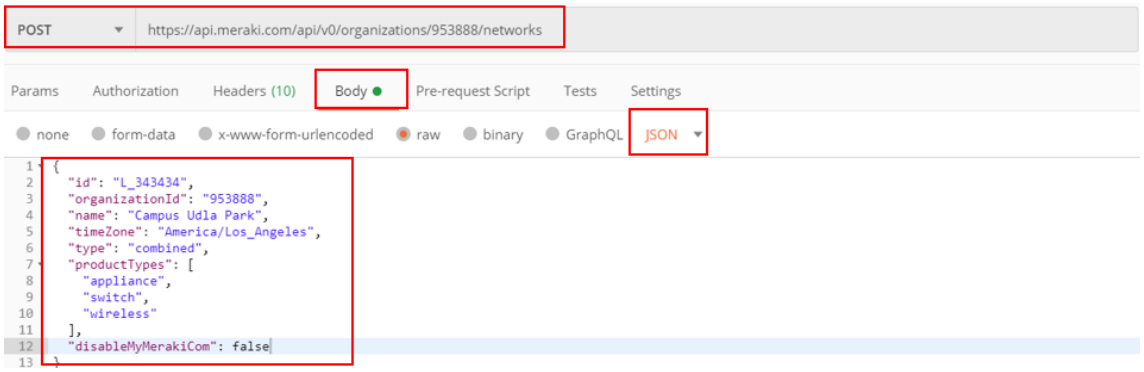


Figura 22. Creación de una red con POST

Con el botón *Send* se ejecuta la tarea con mayor tiempo de ejecución y al ser exitosa se obtiene como respuesta un estado 201 Created.

Figura 23. Creación con éxito.

De igual manera se ve reflejado en el Dashboard la red creada.

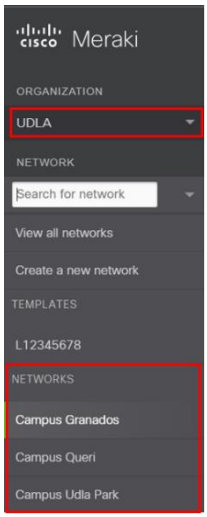


Figura 24. Creación reflejada en el Dashboard

El método PUT realiza actualizaciones en los campos permitidos. Esto no significa que en todas las solicitudes se puede aplicar este método.

Dentro de una red se tiene una subred SSID de nombre “EJEMPLO” la cual sirve de ayuda para conocer el método PUT, la primera tarea es identificar las características de la subred por lo cual mediante el *Dashboard* se obtiene esta información.

Configuration overview

SSIDs Showing 4 of 15 SSIDs. Show all my SSIDs.

	DNENT1 - wireless WiFi	Portal Cautivo	EJEMPLO
Enabled	enabled	enabled	enabled
Name	rename	rename	rename
Access control	edit settings	edit settings	edit settings
Encryption	Open	Open	Open
Sign-on method	None	Click-through splash page	Click-through splash page
Bandwidth limit	unlimited	unlimited	unlimited
Client IP assignment	Meraki DHCP	Meraki DHCP	Meraki DHCP
Clients blocked from using LAN	yes	no	no
Wired clients are part of Wi-Fi network	no	no	no
VLAN tag	n/a	n/a	n/a
VPN	Disabled	Disabled	Disabled
Splash page			
Splash page enabled	no	yes	yes
Splash theme	n/a	n/a	n/a
Custom splash URL	n/a	http://64.103.26.57/	n/a

Figura 25. Redes SSID de Meraki

Otra manera de obtener la información de la red es con una consulta mediante el método GET de la subred SSID.


```
    "number": 2,
    "name": "EJEMPLO",
    "enabled": true,
    "splashPage": "Click-through splash page",
    "ssidAdminAccessible": false,
    "authMode": "open",
    "radiusAccountingEnabled": false,
    "ipAssignmentMode": "NAT mode",
    "adminSplashUrl": null,
    "splashTimeout": "1440 minutes",
    "walledGardenEnabled": false,
    "minBitrate": 11,
    "bandSelection": "Dual band operation",
    "perClientBandwidthLimitUp": 0,
    "perClientBandwidthLimitDown": 0,
    "visible": true,
    "availableOnAllAps": true,
    "availabilityTags": []
},
```


Figura 26. Método GET de una red SSID

Con los datos obtenidos en *Postman* y con el método PUT se escribe la dirección web, el ID de red y el ID del SSID. Para posteriormente ingresar estos valores en lenguaje JSON y en el apartado *Body* y así realizar la actualización de datos dentro de una red.

Por último, con el estado 200 OK nos refleja que no se han actualizado los datos sin error.

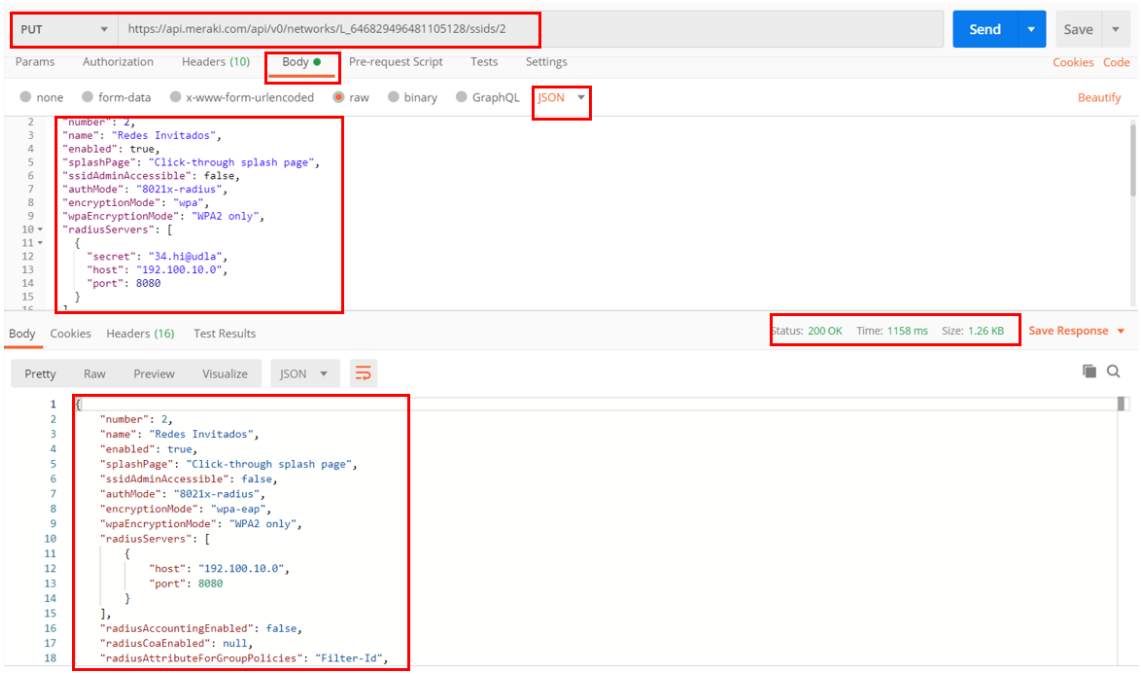


Figura 27. Actualización de Red SSID

Una vez realizada la actualización, mediante el *Dashboard* se visualiza los cambios realizados con los parámetros ingresados mediante *Postman*.

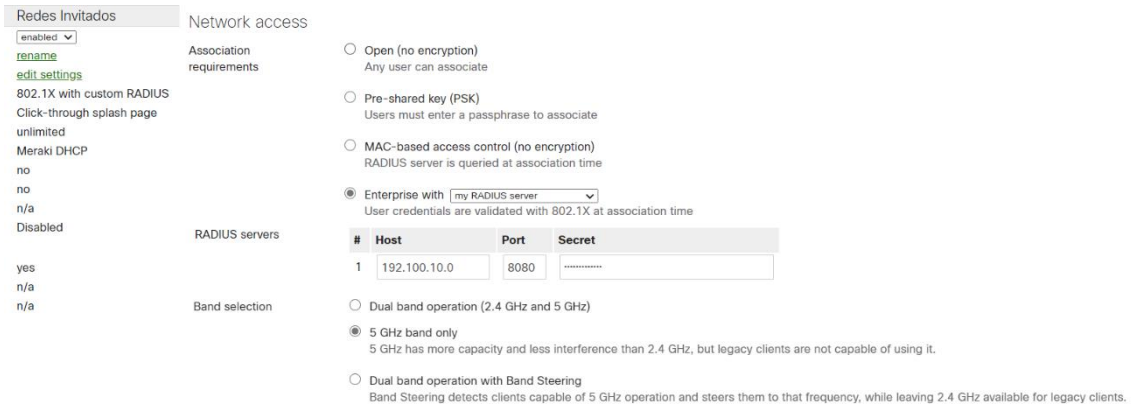


Figura 28. Cambios verificados por Dashboard

El método DELETE sirve para eliminar configuraciones u objetos que son prescindibles en la redes, organizaciones o componentes.

Para eliminar una VLAN se necesita dos parámetros de identificación: *networkId* y VLAN ID. Consultando la tabla de *Subnet*, se encuentran las VLAN de la red.

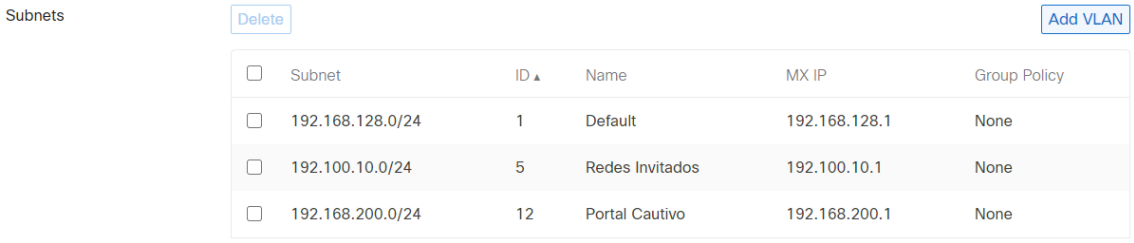


Figura 29. VLAN usadas actualmente

Finalmente, en *Postman* se ingresa la URL, el método y se envía la información.

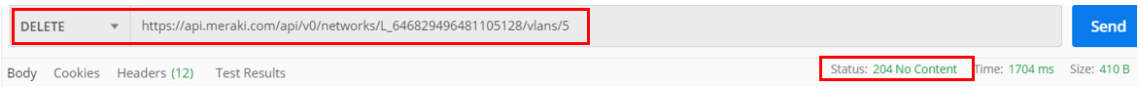


Figura 30. Eliminar un VLAN

A continuación, mediante código generado en PowerShell se revisa la VLAN que ha sido eliminada.

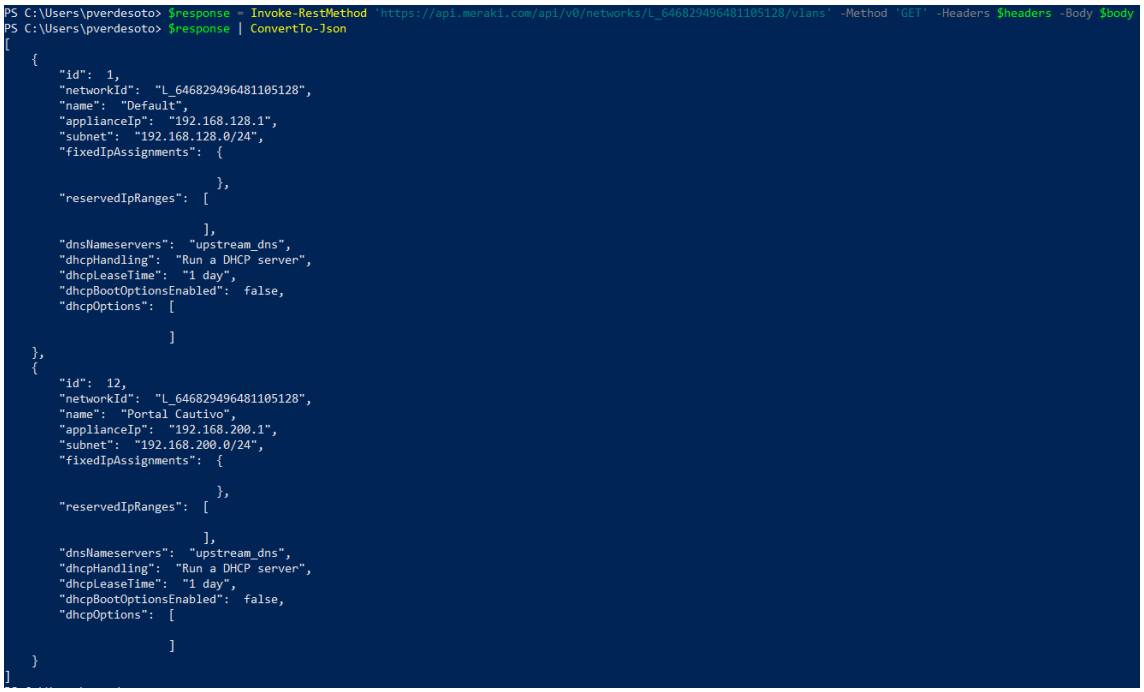


Figura 31. Eliminación de VLAN completa

3.3 Portal Cautivo con Meraki

3.3.1 Propuesta de Diseño

En el siguiente diseño se muestra el funcionamiento de los componentes más importantes del servicio de Meraki, Portal Cautivo (Ej: Windows Server 2019) y dispositivos móviles.

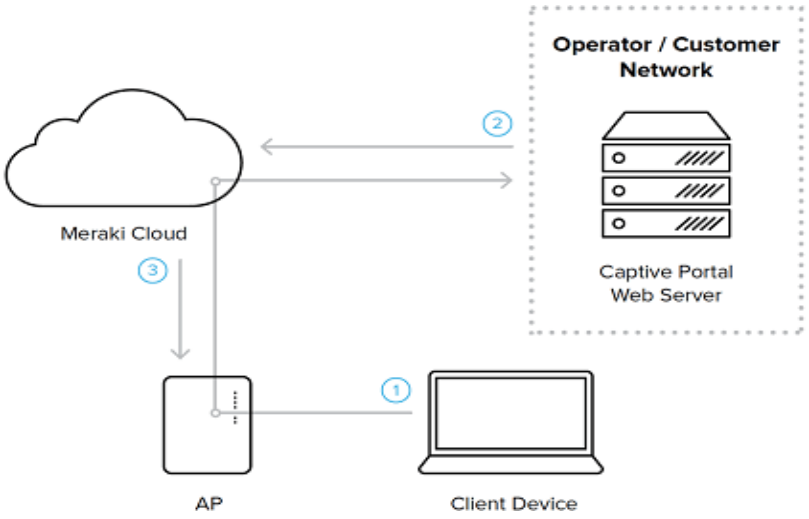


Figura 32. Arquitectura Portal Cautivo

En el *Web Server* se realiza la configuración de un servicio IIS (*Internet Information Services*) con *Windows Server* mediante *Server Manager*. Una vez listo el servicio se debe instalar la plataforma web de Microsoft. Adicionalmente, se debe instalar los componentes de PHP para levantar y generar una página web los cuales sirven de interfaz de ingreso y registro.

La configuración en el Administrador de PHP se realiza a través de scripts tanto en HTML para visualizar y en PHP para almacenar los datos que, en este caso, son un correo electrónico y un nombre de usuario. Ambos archivos están ubicados en la carpeta “rootwww” que es la ruta predeterminada del IIS.

Se añaden los parámetros del *Website* en el *Web Server*: nombre, dirección del código fuente, dirección IP y puerto que conforma el socket. Finalizado se ingresa la dirección para presentarse de manera predeterminada en el servidor.

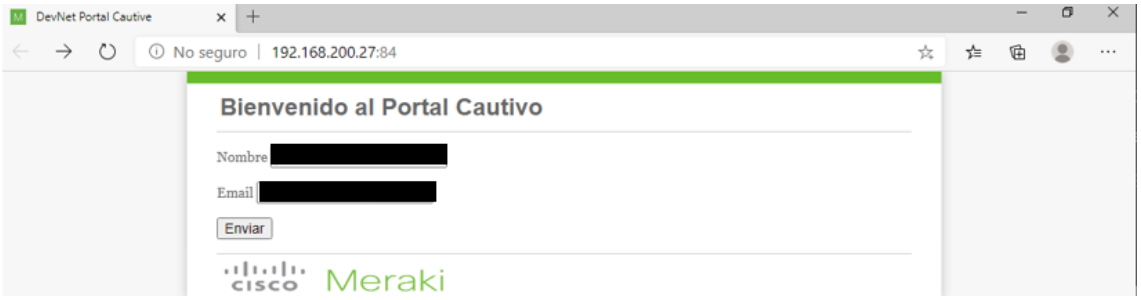


Figura 33. Servicio IIS levantado

Para permitir que las solicitudes lleguen al servidor, se genera un permiso de tráfico de entrada en el Firewall. Para lo cual se asigna la entrada por un puerto específico caso contrario las solicitudes no ingresan al servidor.

Con el equipo Meraki, en este caso el router MX, se añade la ruta para el envío de paquetes mediante el Firewall. Se especifica la dirección IP, el puerto y el de protocolo. Configurados estos parámetros se accede mediante una dirección WAN a los recursos del servidor.

Figura 34. Acceso al servidor mediante un dirección WAN

En las redes SSID se configura la señal de portal cautivo. Se genera un rango específico de direcciones en la cual el Access Point propaga las direcciones IP mediante DHCP. Posteriormente, se redirecciona el dominio de la dirección WAN para replicar la configuración en los portales de red externa dentro de los APs. Una vez conectado al AP se ingresa y presenta por defecto la página web previamente cargada.

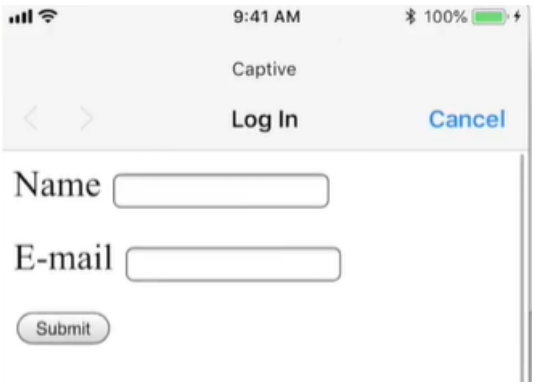


Figura 35. Portal de Acceso

3.3.2 Configuración del Portal Cautivo

Se configura una máquina virtual con un *Web Server* en Windows Server 2019 que usa el motor IIS 10.

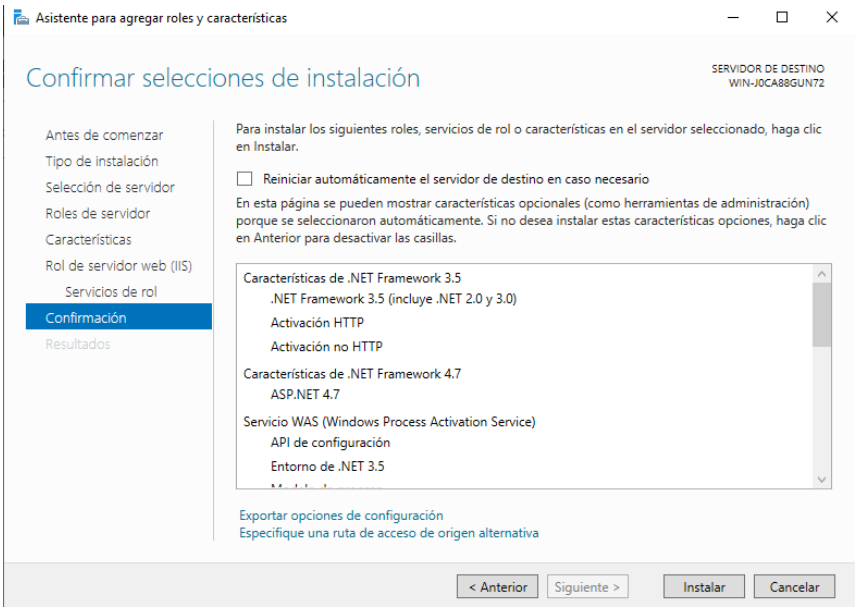


Figura 36. Agregar roles y características de IIS

Finalizado el proceso del servicio IIS se agrega los componentes de la plataforma Web y las características de PHP. Finalmente, se ejecuta hasta completar el proceso de instalación.

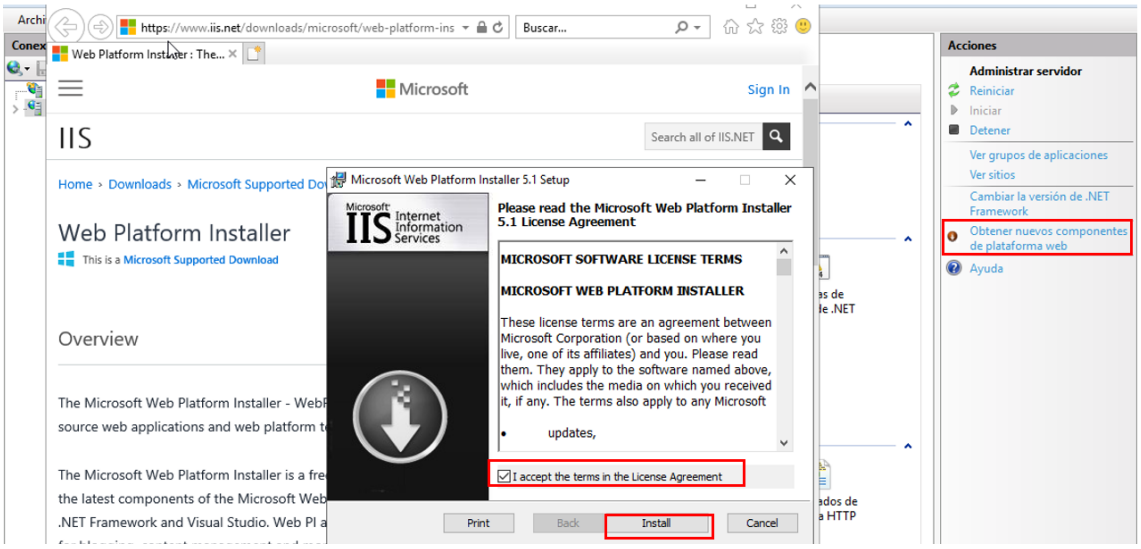


Figura 37. Instalación de complemento para IIS

Se debe instalar una versión de PHP de la familia 7.2.X en adelante, en base a la arquitectura si es de 32 o 64 bits. Esta instalación depende de la conexión de internet y las características del servidor.

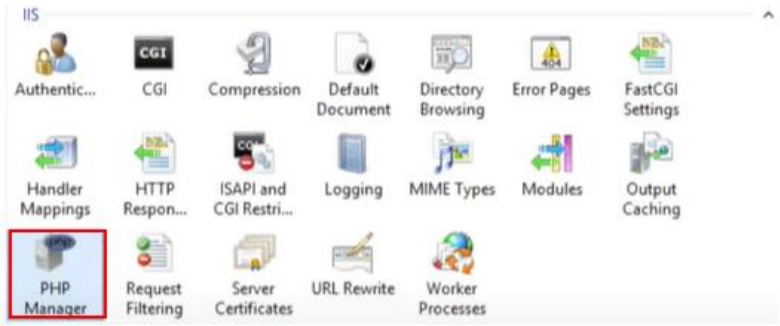


Figura 38. Proceso de finalización de instalación

En la ruta por defecto del servidor se crea una carpeta, misma que va a leer el código de página web (PHP) y el formato (HTML). En este caso en la siguiente dirección se añade la carpeta de nombre *"Portal Cautivo"*.

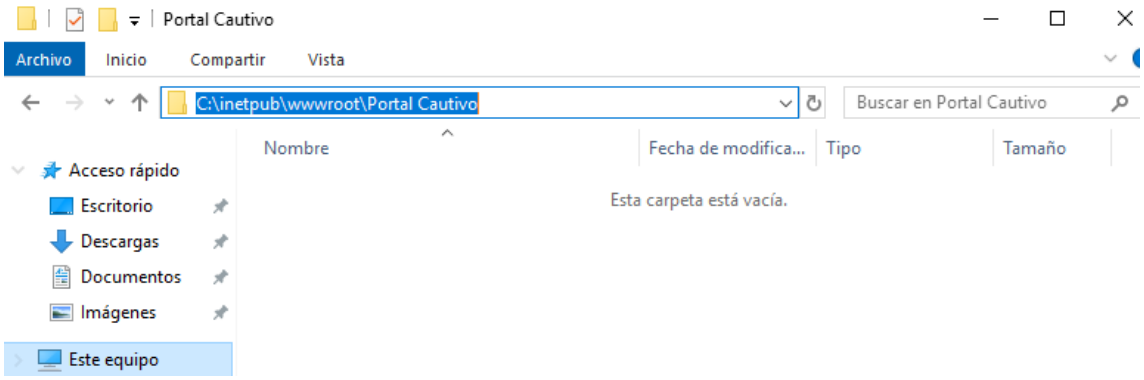


Figura 39. Creación de Carpeta

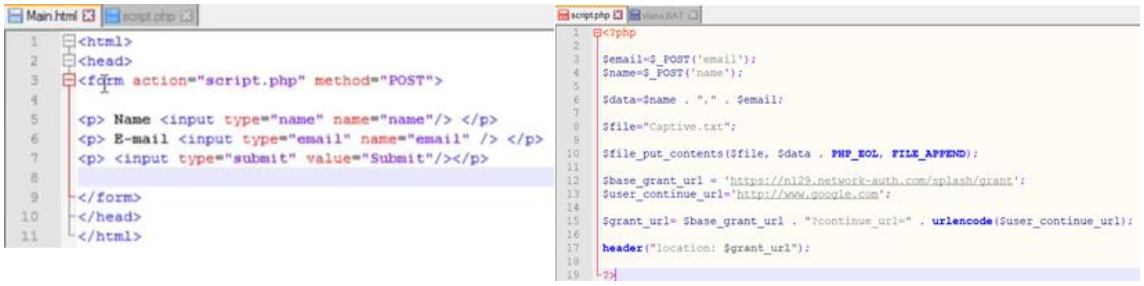


Figura 40. Código HTML y PHP

Una vez finalizada la configuración de la página y el *Web Server* se debe agregar un nuevo sitio web en el administrador de IIS con los parámetros necesarios.

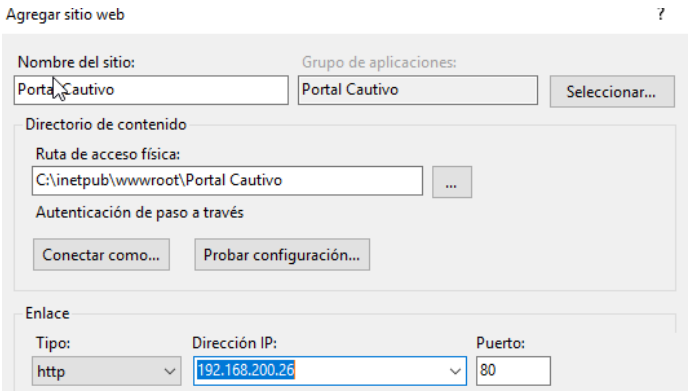


Figura 41. Configuración del sitio

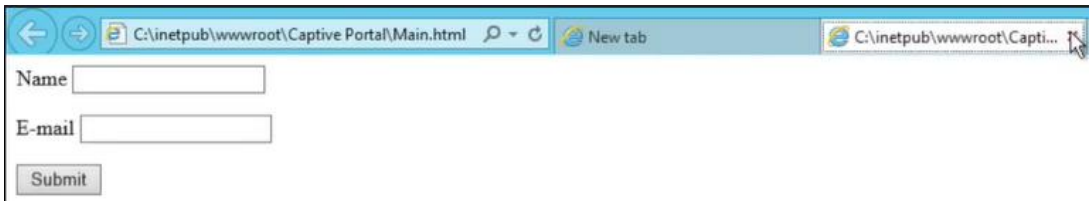


Figura 42. Servicio levantado IIS

En el equipo Meraki MX se configura la regla del firewall para hacer un reenvío de tráfico, es decir todo lo que esté publicado en la WAN con el puerto de ingreso se conectará a los servicios web. Con esto se realiza un direccionamiento que aplica a toda la Organización.

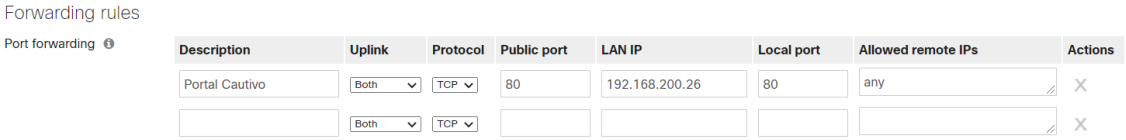


Figura 43. Configuración de Firewall Meraki

Con el ingreso de tráfico configurado al firewall se entabla la conexión hacia el SSID seleccionado. Para lo cual dentro de las configuraciones del SSID se modifica el campo *Walled Garden*. Esto ocurre porque al estar en la red local el ingreso es mediante el firewall, pero si se usa la WAN se debe redireccionar para lograr el acceso. Adicional se puede incluir si las peticiones serán abiertas, es decir, cualquier equipo se puede conectar a la red o restringidas en la cual, mediante listas blancas de clientes y con dispositivos registrados se permite el acceso a la red.

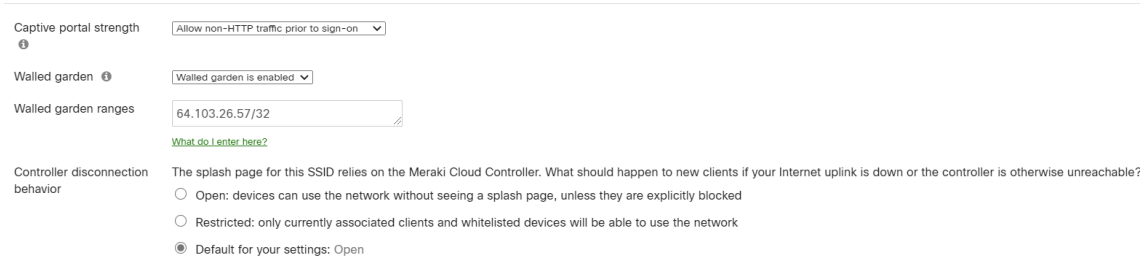


Figura 44. Configuración de SSID

Para finalizar, se realiza la conexión mediante el SSID seleccionado y se muestra la información del Portal Cautivo al momento de conectarse en la red.

3.4 Propuesta de diseño de una red básica IoT.

En el siguiente diseño propuesto se muestra la red en la cual se basa la guía de laboratorio introductoria para el área de IoT.

Figura 45. Diseño de red para guía introductoria IoT

El diseño cubre los componentes básicos de una red para una conexión a Internet. Estos componentes son el ‘Home Gateway’ (glosario) y Cable Modém.

Cada uno de estos componentes tiene su funcionalidad en la conexión de la red a Internet o a un ISP (glosario). Por ejemplo, el ‘Home Gateway’ cumple las funciones de:

- Administrar o modificar la red inalámbrica creada para la conexión de los dispositivos IoT.
- Permite la asignación de IPs mediante DHCP a los dispositivos IoT conectados a la red inalámbrica.

- Permite la conexión de la red inalámbrica local a la red del ISP.

Otra parte importante para la conexión de la red a Internet es el Cable Modem. El cable modem es un dispositivo utilizado actualmente en las redes CATV instaladas por los proveedores de servicio. El funcionamiento principal de estos dispositivos es modular la señal de datos y distribuir el acceso a Internet de banda ancha en la red CATV. Adicional a esto los cables modem utilizan una conexión por cable coaxial, esto se puede apreciar en la Figura 45.

La red está basada en el modelo del curso Cisco IoT Modulo 1.2.2.3 - 'Connect and Monitor IoT Devices'.

3.5 Propuesta de diseño de una red avanzada IoT.

En el siguiente diseño propuesto se muestra la red en la cual se basa la guía de laboratorio para una configuración de una red IoT.

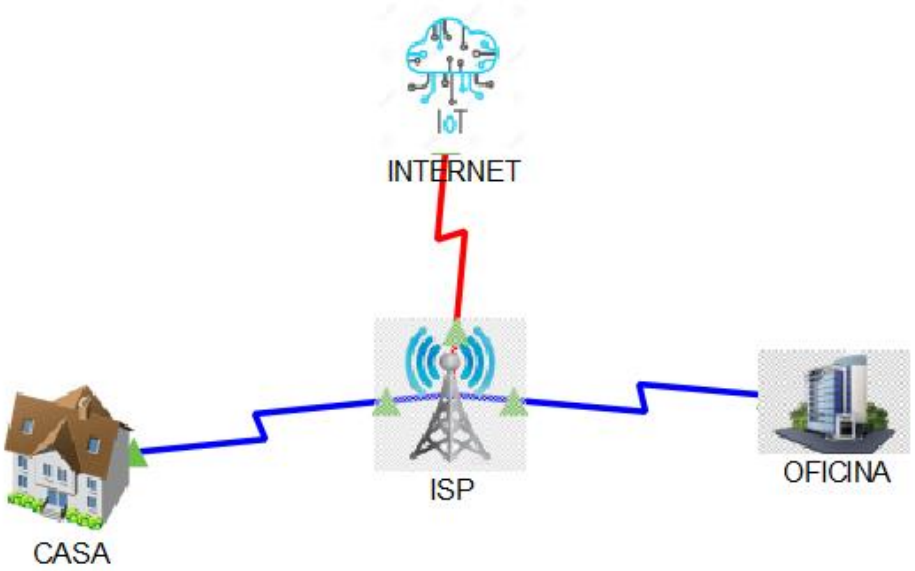


Figura 46. Diseño de red para guía avanzada IoT

En la red se muestra la interconexión de una red doméstica y una red de oficina mediante un ISP y esta permite la conexión a Internet. El diseño de esta red busca crear una práctica semejante a un escenario real en el cual se pueda entender el contexto de las partes esenciales para la interconexión de redes.

La red está creada en base al modelo de la práctica introductoria sobre IoT y en el diseño del curso de Cisco IoT Modulo 3.2.4.5 - 'Home IoT Implementation'.

3.6 Reserva de SandBox en DCloud.

Para el uso de la plataforma de DCloud es necesario contar con una cuenta de Cisco o crear una de forma gratuita.

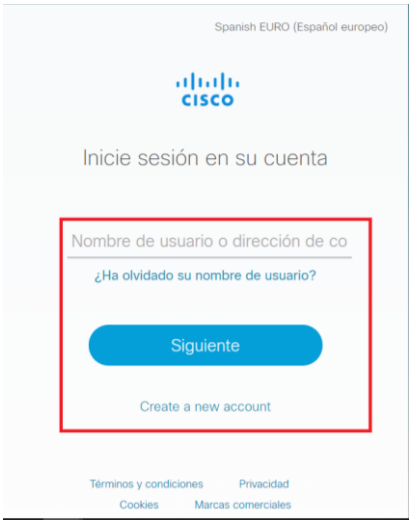


Figura 47. Ingreso a plataforma DCloud.

Una vez dentro de la plataforma se puede visualizar un catálogo de prácticas las cuales tienen como filtro productor, categorías, etc.

En el apartado de productor se puede apreciar las prácticas provenientes del área de *DevNet* o *DCloud*. En el área de *DevNet* se puede acceder a varias prácticas orientadas al desarrollo o programación con aplicaciones. Por otro lado, las prácticas en el área de *DCloud* son más enfocadas a la exploración e interacción de plataformas ofertadas por Cisco.

Igualmente se puede filtrar las prácticas ya sean por laboratorios, demos, *Sandbox*, etc. En casos específicos se utiliza la barra de búsqueda ya sea para laboratorios o prácticas de algún área en específico.

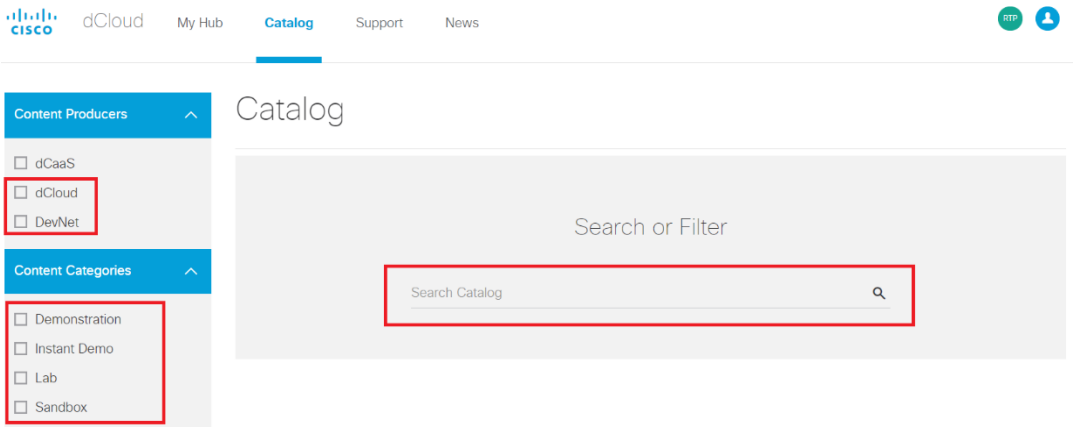


Figura 48. Catálogo de la plataforma DCloud.

Para la reserva de un laboratorio se debe seleccionar la opción *Schedule,* seleccionar el día y la hora a utilizar el laboratorio y posteriormente llenar una pequeña encuesta para completar la reserva.

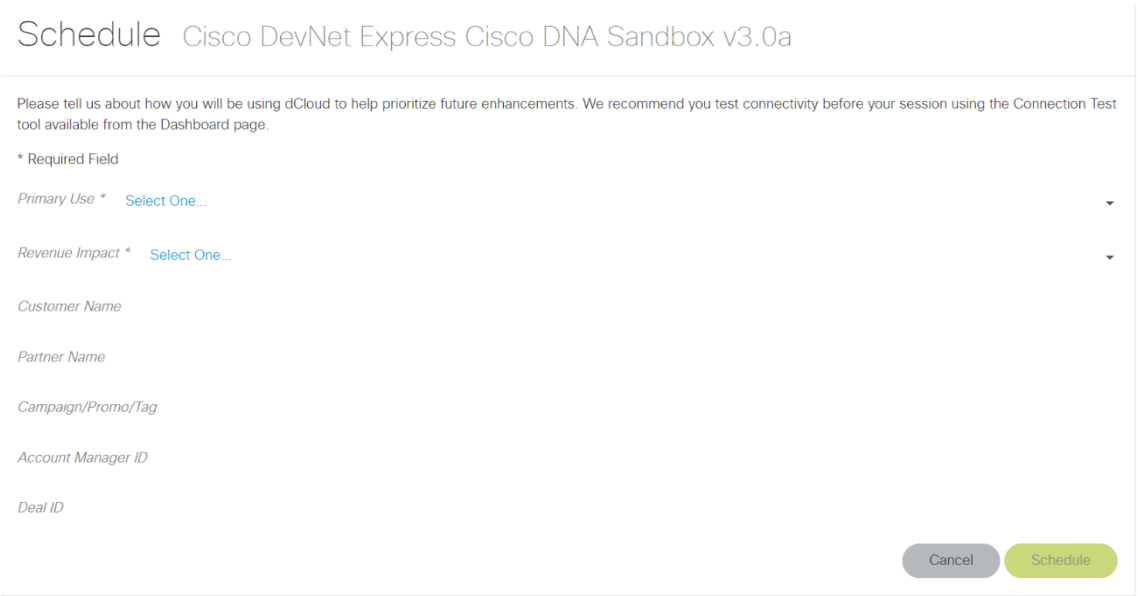


Figura 49. Encuesta de reserva en DCloud.

En caso de visualización de algún demo o plataforma de libre acceso se debe seleccionar el laboratorio para poder visualizar la información sobre el mismo.

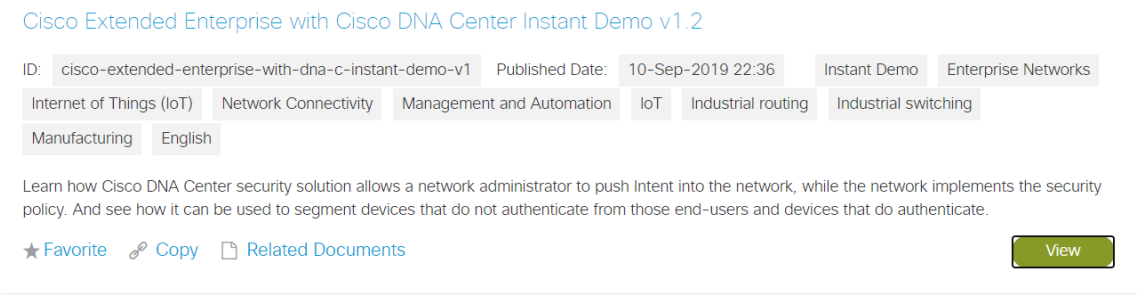


Figura 50. Visualización de demo en DCloud.

Una vez dentro se puede apreciar la información como resumen, escenarios y requisitos para el uso de la demostración. En la pestaña de *Resources* se puede acceder a una guía o ayuda para la exploración del demo.

Por último, para ingresar a la plataforma demostrativa se debe seleccionar *View* e inmediatamente se redirecciona a una nueva pestaña.

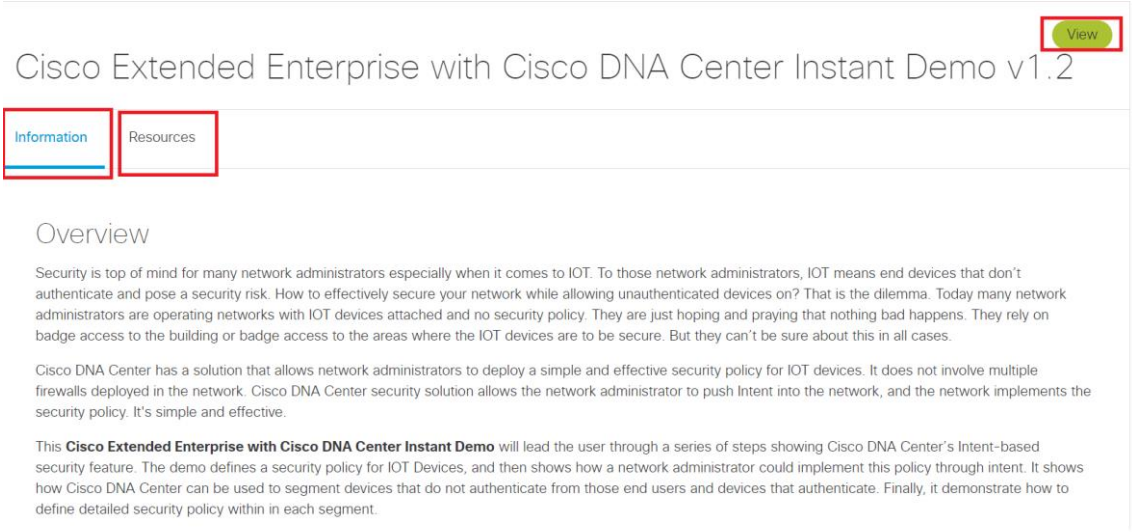


Figura 51. Información sobre la demo en DCloud.

3.7 Panel informativo de Cisco DNA.

Una vez dentro de la plataforma con las credenciales indicadas en la práctica de laboratorio se puede apreciar un *dashboard* con toda la información resumida de una red. Esta información puede ser estado de salud o conexión de todos los dispositivos, cantidad de problemas o errores encontrados en la red, políticas de aplicación, sitios de cada red (infraestructuras o topologías), etc.

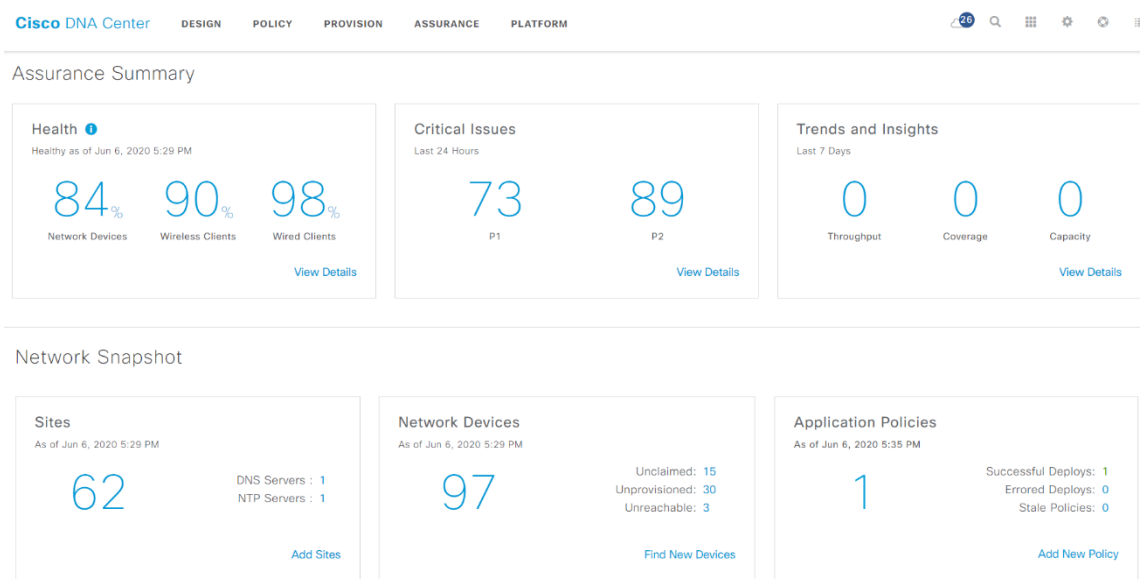


Figura 52. Panel informativo en DNA.

En la pestaña de *Design* se accede a toda la administración en cuanto a topología de las redes. Se puede administrar tanto credenciales de red, credenciales de dispositivos, perfiles de red, plantillas de autenticación, etc.

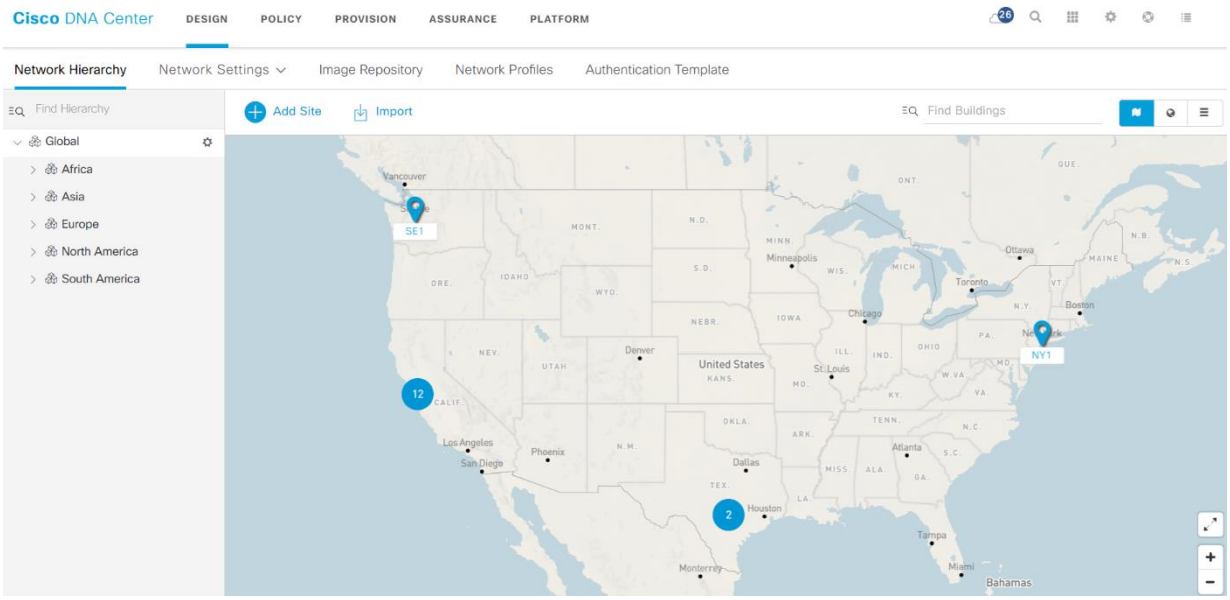


Figura 52. Pestaña Design en DNA

En la pestaña de *Policy* se administra todos los perfiles, políticas o restricciones en aplicaciones de la red. Esto ayuda a crear grupos para políticas basados en perfiles de red, grupo de direcciones IP o incluso por aplicación.

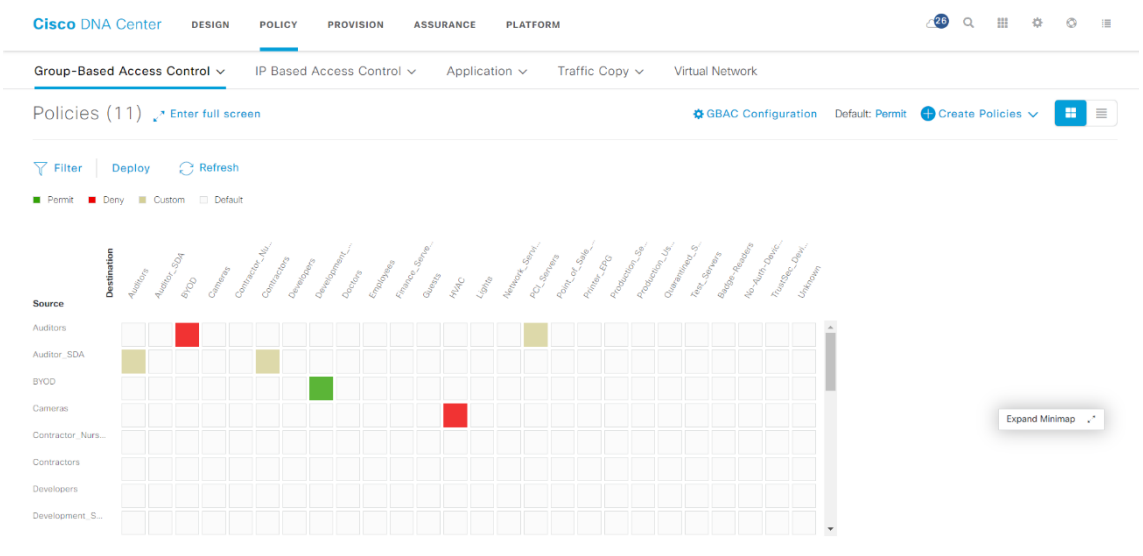


Figura 53. Pestaña Policy en DNA

Finalmente, en la pestaña de *Assurance* se logra visualizar la información sobre estado de conexión y problemas que la red pueda presentar en ese momento. En esta pestaña se puede apreciar la información de toda la red clasificada en capas, tipo de red o tipo de dispositivo, lo cual ayuda a la identificación y administración.

Dentro de esta pestaña existen varios *dashboards* los cuales brindan una información más detallada de los componentes o dispositivos dentro de la red, incluso llegando a ubicar problemas o errores dentro de cada topología u arquitectura de red desplegada.

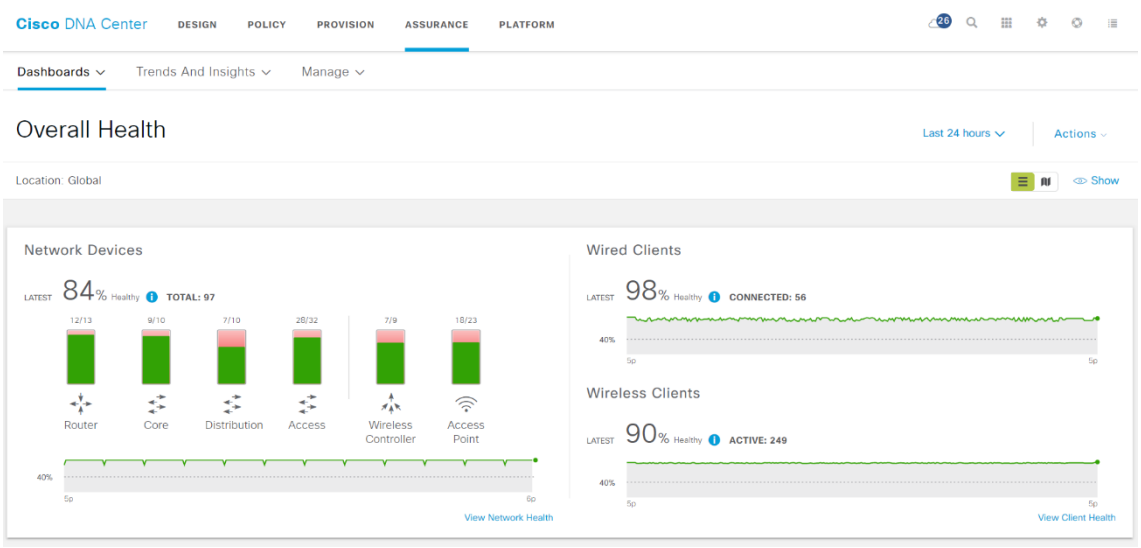


Figura 54. Pestaña Assurance en DNA.

4. **Conclusiones y Recomendaciones.**

4.1 Conclusiones:

- La plataforma Cisco *DevNet* permite una exploración hacia nuevos esquemas en cuanto a interacción con las redes, permitiendo simular entornos virtuales orientados a cada área y así lograr una mayor instrucción hacia estos esquemas.
- La programación es un requisito fundamental para la interacción o personalización de las plataformas dentro del catálogo de *Sandbox*, permitiendo una facilidad en visualización, administración y configuración de las redes.
- La integración de las API con la programación en Python es un requerimiento esencial para el desarrollo y optimización de las plataformas para administración de redes.
- Se obtuvo un mayor conocimiento en cuanto a temas de IoT el cual es fundamental para la formación en el área de redes. Las redes continúan evolucionando en esta área y por lo tanto la implementación del IoT es una realidad en el mundo profesional.
- Se logró aportar una mayor información e introducción en cuanto al uso de la plataforma Cisco *DevNet* dentro de las áreas de *Networking* y Meraki. Estas áreas contienen tecnologías las cuales brindan nuevas funcionalidades dentro del conocimiento de las redes.
- Se completaron guías de laboratorio orientadas a las áreas de IoT, Meraki y *Networking* mediante el uso de *DevNet* y *DCloud*. Esto permitió una mayor información, interacción y cobertura de temas relevantes para las carreras afines a esta temática.
- Al permitir la convergencia de redes y dispositivos se ha obtenido un alcance global permitiendo administrar varias plataformas de manera remota y segura.

4.2 Recomendaciones:

- Al momento de acceder a las diferentes plataformas es recomendable utilizar una cuenta única para que en los futuros proyectos los estudiantes puedan seguir aportando a la comunidad académica.
- Cuando se trata de entornos *Sandbox*, estos tienen un tiempo limitado de uso para lo cual es recomendable que se guarde la información dentro de un repositorio GitHub, por ejemplo.
- Se recomienda revisar los conceptos de programación en Python al igual que su integración con plataformas API.
- Con el incremento de aplicaciones y servicios en una organización el uso e incorporación de redes inteligentes con programabilidad y API se ha convertido en un requisito esencial, por lo tanto, es recomendable revisar el contenido de los laboratorios *Sandbox*.
- En la actualidad Meraki se encuentra en el despliegue en fase beta de la versión V1 del *Dashboard* de API, por lo cual es necesario actualizar las diferentes solicitudes a los métodos HTTP.

Referencias.

Cisco DNA Center. (2020). *Cisco DNA Center Platform At-a-Glance*. Recuperado el 13 Mayo 2020, Obtenido de *https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-cent-platf-aag-cte-en.html?oid=aagen016868*

Cisco DevNet (2020). APIs, SDKs, Sandbox, and Community for Cisco Developers. Recuperado el 14 Mayo 2020, Obtenido de *https://developer.cisco.com/docs/dna-center/api/1-3-3-x/#!intent-api-v1-3-3-x*

Cisco DNA Center (2020). Descripción general de la plataforma Cisco DNA Center. Recuperado el 13 Mayo 2020, Obtenido de *https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/cisco-dna-center-platform-overview*

Cisco DNA Center. (2020). - Cisco DNA Center Platform At-a-Glance. Recuperado el 9 Abril 2020, Obtenido de *https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-cent-platf-aag-cte-en.html?oid=aagen016868*

Cisco (2020). Cisco DevNet: APIs, SDKs, Sandbox, and Community for Cisco Developers. Recuperado el 10 de Abril de 2020, Obtenido de Cisco DevNet: *https://developer.cisco.com/*

Cisco DNA (2020). Cisco Devnet. Obtenido de Cisco Devnet. Recuperado el 09 de Abril de 2020, Obtenido de *https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/cisco-dna-center-platform-overview*

Cisco Meraki (2020). Create with the Meraki Platform. Recuperado el 09 de Abril de 2020, Obtenido de Cisco DevNet: *https://developer.cisco.com/meraki/*

IoT Developer Center (2020). Cisco Devnet. Recuperado el 09 de Abril de 2020, Obtenido de Cisco DevNet: *https://developer.cisco.com/iot/*

Cisco DNA Center (2020). Cloud Systems Management. Recuperado el 13 de Mayo de 2020, Obtenido de Cisco DNA Center: *https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-cent-platf-aag-cte-en.html?oid=aagen016868*

JSON (2020), Introducing JSON, Recuperado el 10 de Abril de 2020, Obtenido de *JSON: https://www.json.org/json-es.html*

PowerShell Scripting (2020). PowerShell Microsoft Docs. Recuperado el 10 de Mayo de 2020, Obtenido de PowerShell*: https://docs.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7*

Read the Cisco DevNet case study (2020). Postman. Recuperado el 25 de Abril de 2020, Obtenido de Postman: *https://www.postman.com/resources/case-studies/cisco-devnet/*

Hack, P. J. (2019). Learn Python Programming [Kindle]. Recuperado de *https://www.amazon.com/-/es/Phil-J-Hack-ebook/dp/B081GCPWWH*

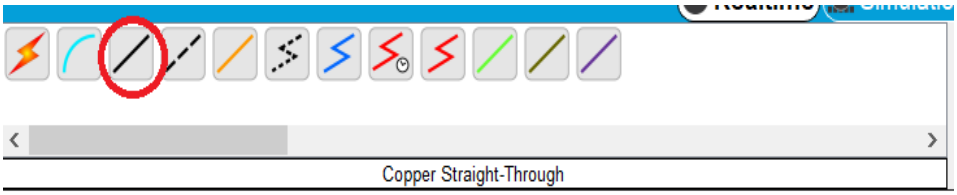
Cisco Meraki Blog (2020). Cisco Meraki. Recuperado el 26 de Marzo de 2020, Obtenido de Cisco Meraki: https://meraki.cisco.com/blog/2020/03/powering-the-remote-workforce/

Anexos.

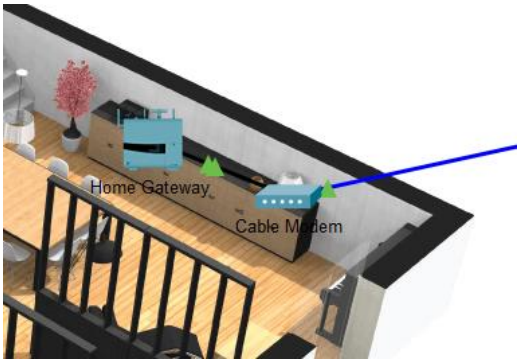
Guía de laboratorio – Introducción a IoT y sus componentes.

Parte 1: Conectando un Home Gateway a la red.

a) Conecte el dispositivo “Home Gateway” al cable módem.
   - Haga clic en el icono de conector y seleccione el cable de cobre de conexión directa. Luego haga clic sobre “Home Gateway” y seleccione el puerto “Internet”. A continuación, haga clic en el cable módem y seleccione ”Port 1” para interconectar estos dos dispositivos.



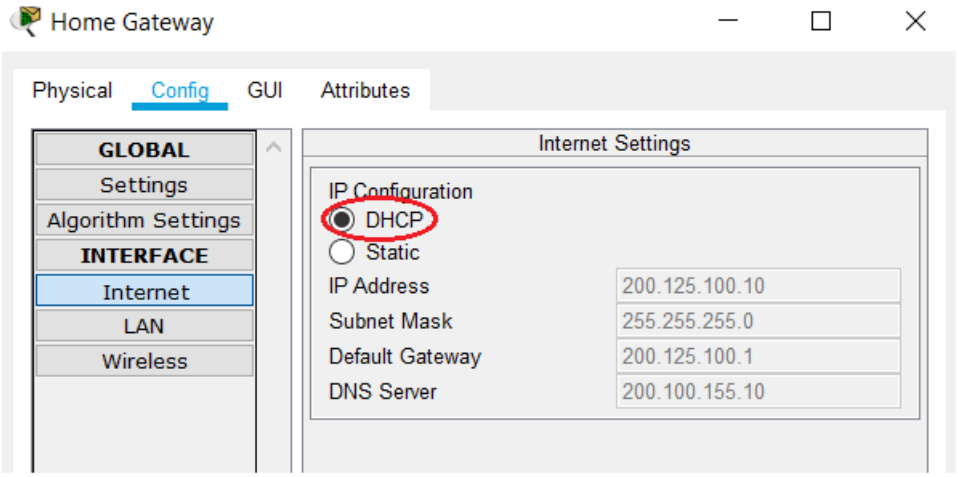
b) Después de unos segundos ambos extremos del cable deben estar en color verde, esto indica que ya se encuentran conectados y comunicados.



Parte 2: Configurando un Home Gateway.

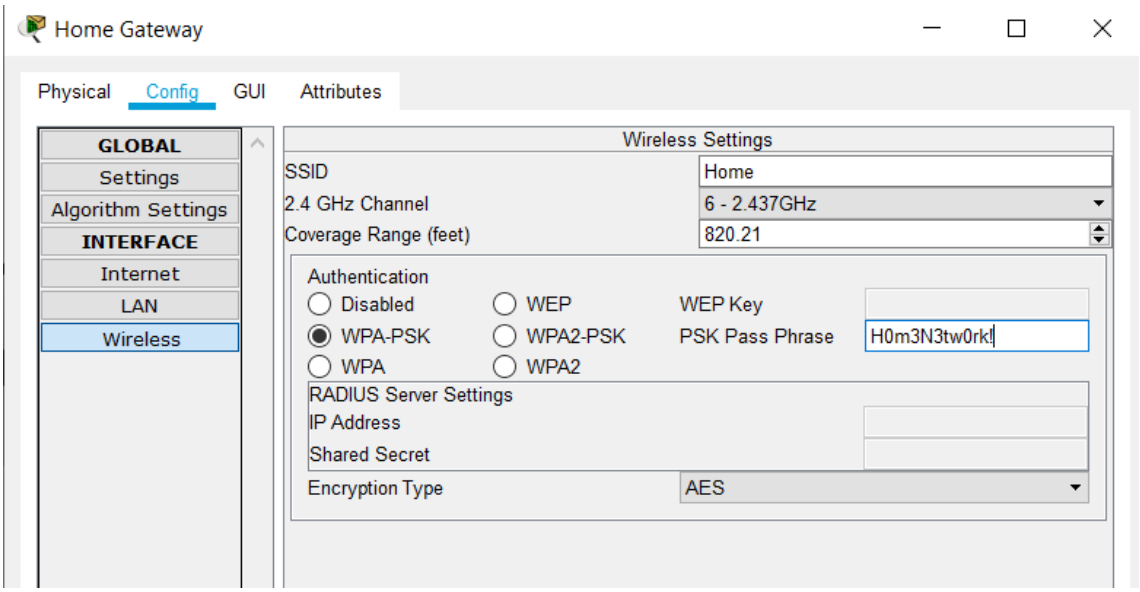
a) Seleccione el dispositivo “Home Gateway” para abrir las propiedades del dispositivo.
b) Seleccione la pestaña de configuración.

c) Seleccione la pestaña de configuración de “Internet” y active el direccionamiento por “DHCP”.



- **Nota:** El direccionamiento mostrado simula a una dirección IP Pública proporcionada por un ISP.

d) Seleccione en la misma ventana la pestaña de configuración “Wireless”.
e) Cambie el nombre de red a “Home”.
f) Seleccione como autenticación la opción “WPA-PSK”.
g) Ingrese la siguiente contraseña: **H0m3N3tw0rk!**



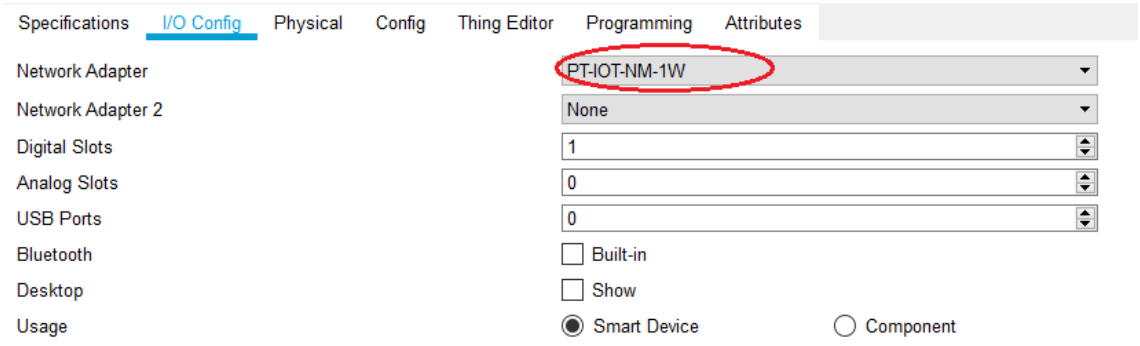
Parte 3: Conectando dispositivos IoT a la red inalámbrica.

a) Haga clic en el icono de “Dispositivos”, posteriormente seleccione “Hogar” y agregue la puerta, la ventana y la lámpara en el plano de la casa.

- **Nota:** Cambie el nombre de los dispositivos en la parte de configuraciones “Display Name”, esto ayudara a ubicar los dispositivos en las actividades posteriores.

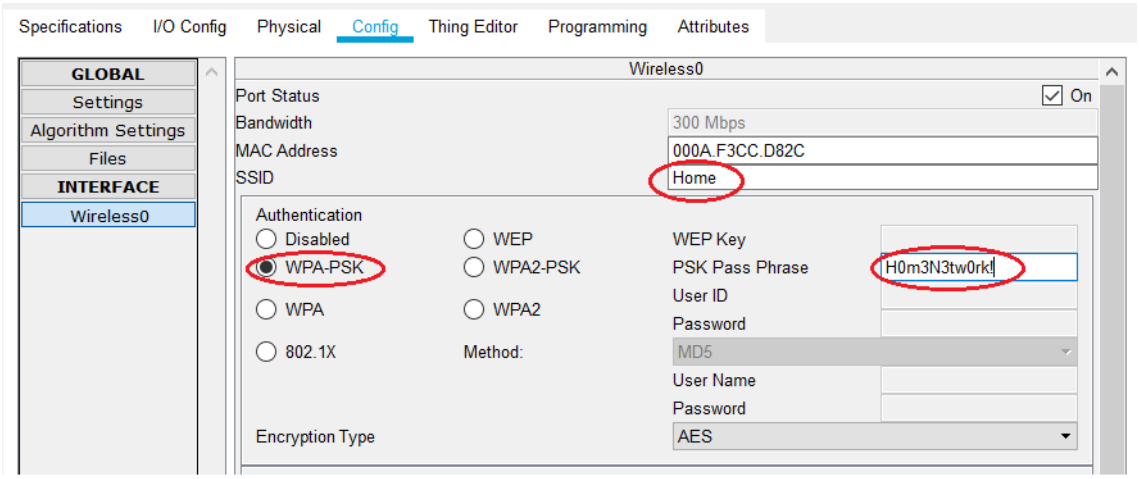
b) Haga clic en la puerta para abrir la ventana de “Especificaciones”, posteriormente clic en el botón “Advanced” ubicado en la parte inferior derecha.

c) Seleccione la pestaña de “I/O Config”, en “Network Adapter” seleccione “PT-IOT-NM-1W”. Esto agrega un adaptador inalámbrico al dispositivo.



d) Seleccione la pestaña de “Configuración”. Posteriormente seleccione la pestaña de configuración “Wireless”.

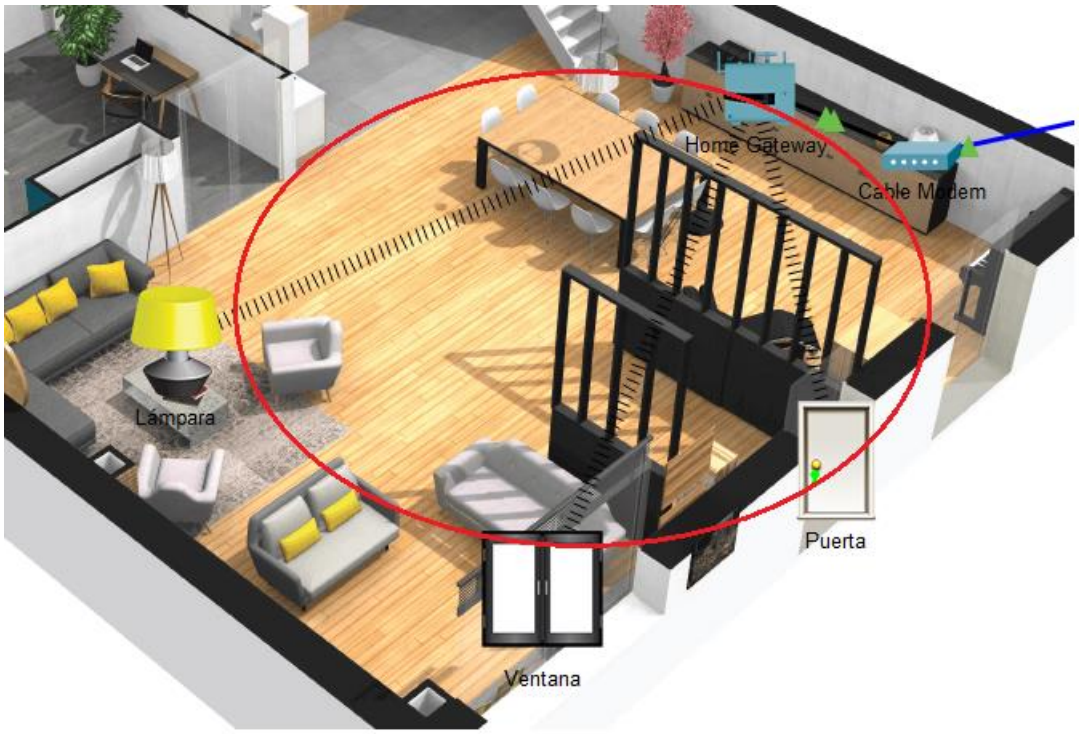
e) Ingrese los datos de la red inalámbrica creada anteriormente en el dispositivo “Home Gateway” en la parte 2 de la guía.



f) Verifique la conexión inalámbrica entre el dispositivo y el “Home Gateway”.

Parte 3.1: Actividad de conexión de dispositivos IoT.

a) Conecte los demás dispositivos a la red inalámbrica del “Home Gateway”.

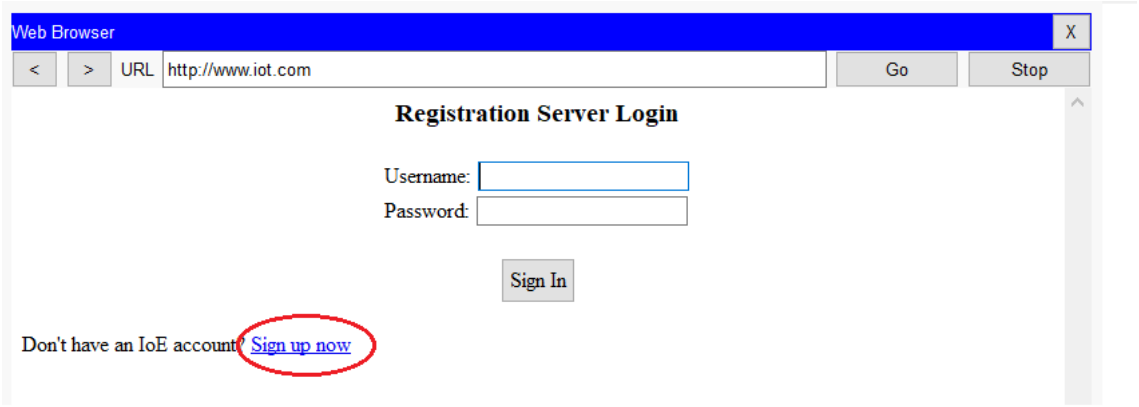


Parte 4: Visualización y control dispositivos IoT.

a) Agregue un celular o “Smartphone” a la red inalámbrica.
b) Haga clic en la parte de configuraciones y seleccione la parte de configuración “Wireless”.
c) Conecte con los datos de la red inalámbrica creada anteriormente en el “Home Gateway”.
d) Verifique la conexión inalámbrica entre el celular y el “Home Gateway”.

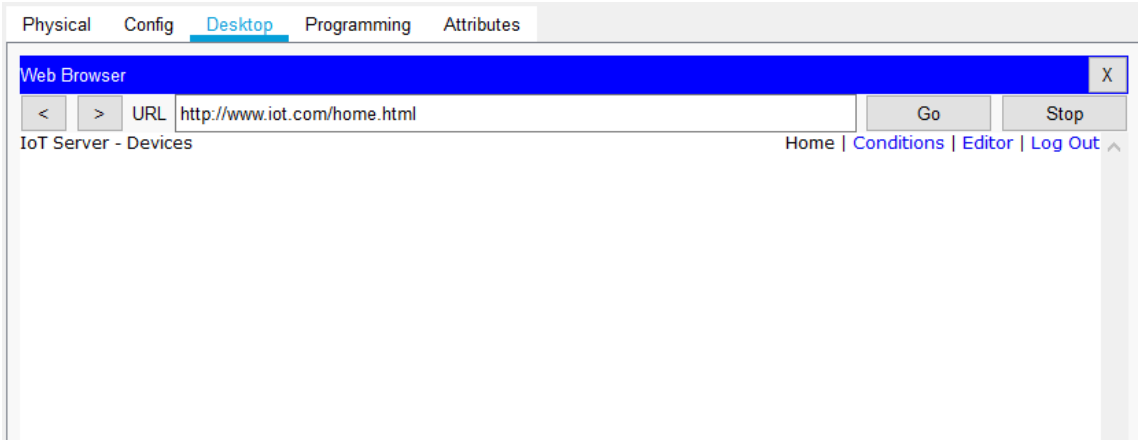
e) Haga clic en el celular e ingrese a la pestaña de “Desktop”. Seleccione “Web Browser” e ingrese a www.iot.com.

f) Seleccione “Sign up now” para crear las credenciales de acceso.



g) En la página de registro ingrese los siguientes datos:
- Username: **admin**
- Password: **admin**

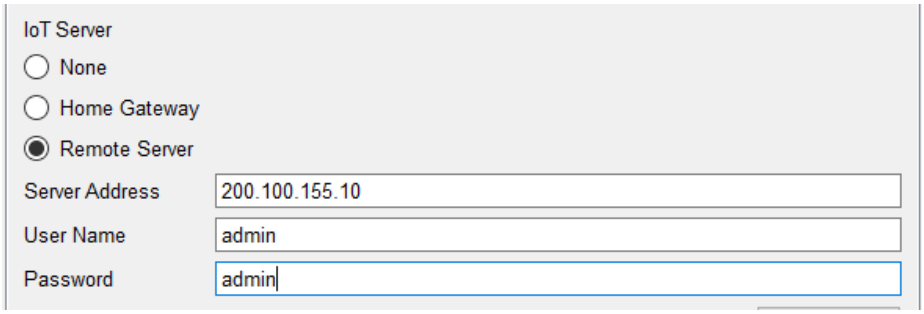
h) Haga clic en el botón “Create”.
i) Verifique el acceso a la página de inicio.



- **Nota:** Para que se pueda visualizar los dispositivos conectados se debe configurar la conexión al servidor en los dispositivos IoT.

j) Abra la pestaña de configuración de cualquier dispositivo y ubicar la configuración de “IoT Server” dentro de “Settings”.
k) Seleccione “Remote Server”.

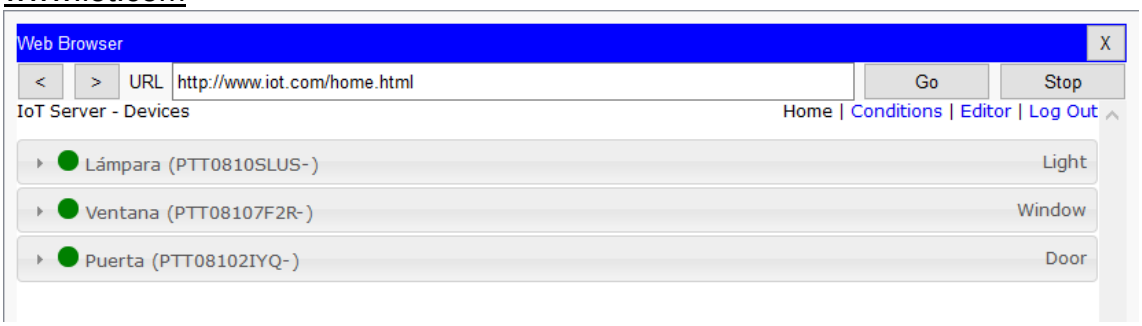
l) Ingrese los siguientes datos:
- Server Address: **200.100.155.10**
- User Name: **admin**
- Password: **admin**



m) Haga clic en el botón “Connect”.

Parte 4.1: Actividad visualización e interacción de dispositivos IoT.

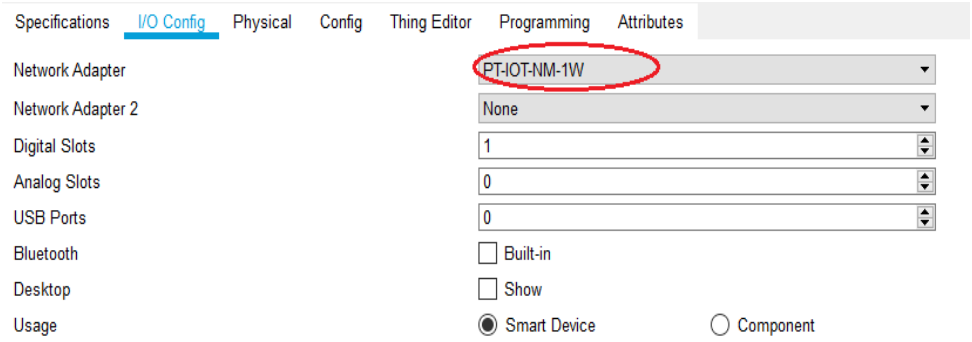
a) Conecte los demás dispositivos al servidor IoT repitiendo los pasos anteriores.
b) Verifique que los dispositivos se vean reflejados en la página web www.iot.com



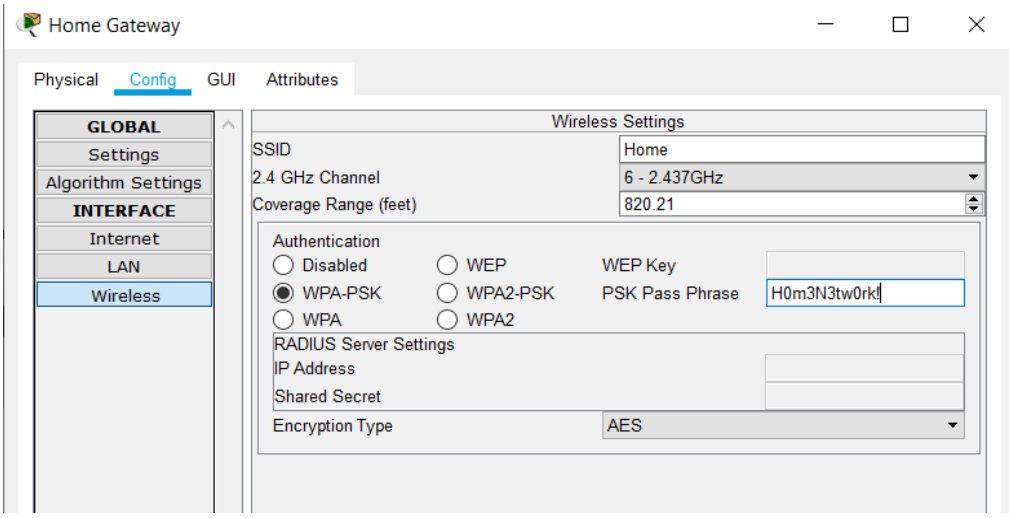
c) Interacción con los dispositivos.
- ¿Qué acciones tiene el dispositivo “Lámpara”?
- ¿Qué sucede al dispositivo “Puerta” cuando se selecciona “Lock”?
- ¿Cuántos controles tiene “Ventana” y qué hace cada uno de ellos?

Parte 3.1 Resolución: Actividad de conexión de dispositivos IoT.

b) Conecte los demás dispositivos a la red inalámbrica del “Home Gateway”.
   a. Haga clic en el dispositivo para abrir la ventana de Especificaciones, posteriormente clic en el botón “Advanced” ubicado en la parte inferior derecha.
   b. Seleccione la pestaña de “I/O Config”, en “Network Adapter” seleccione “PT-IOT-NM-1W”. Esto agrega un adaptador inalámbrico al dispositivo.



   c. Seleccione la pestaña de “Configuración”. Posteriormente seleccione la pestaña de configuración “Wireless”.
   d. Ingrese los datos de la red inalámbrica creada anteriormente en el dispositivo “Home Gateway”:
      i. SSID: **Home**
      ii. Autenticación: **WPA-PSK**
      iii. Contraseña: **H0m3N3tw0rk!**



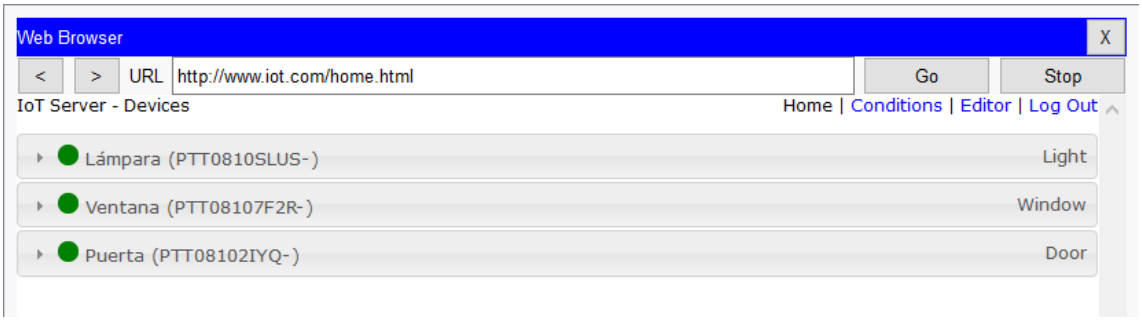
e. En la pestaña “Settings”, cambie el nombre del dispositivo para poder identificarlo fácilmente.

Parte 4.1 Resolución: Actividad visualización e interacción de dispositivos IoT.

d) Conecte los demás dispositivos al servidor IoT repitiendo los pasos anteriores.
   - Abra la pestaña de configuración del dispositivo y ubicar la configuración de IoT Server dentro de “Settings”.
   - Seleccione “Remote Server”.
   - Ingrese los siguientes datos:
     i. Server Address: **200.100.155.10**
     ii. User Name: **admin**
     iii. Password: **admin**

   - Haga clic en el botón “Connect”.

e) Verifique que los dispositivos se vean reflejados en la página web www.iot.com
   - Los dispositivos se encuentran conectados y sincronizados con el servidor por esa razón se ven reflejados en la página web.



f) Interacción con los dispositivos.
   - ¿Qué acciones tiene el dispositivo “Lámpara”?
     i. Apagado, Luz media, Luz intensa.
   - ¿Qué sucede al dispositivo “Puerta” cuando se selecciona “Lock”?
     i. Se bloquea la puerta y no se puede abrir.
   - ¿Cuántos controles tiene “Ventana” y qué hace cada uno de ellos?
     i. Uno tanto para abrir y cerrar la ventana.

Guía de laboratorio - Configuración de una red IoT

Prerrequisito: Práctica Introductoria IoT.

Parte 1: Explorando la red Casa

c) Haga clic en Casa para abrir el “Cluster”.
d) Haga clic en “Smarthphone Casa” para abrir el dispositivo.
e) Desde “Smarthphone Casa”, abrir “Desktop”, “Web Browser” e ingresar la siguiente dirección: www.casa.com.
f) Ingrese las siguientes credenciales. Ingresar **admin** como username y **admin** como password para ingresar al servidor remoto.

Nota: En la página “Home” se puede apreciar todos los dispositivos conectados actualmente al dispositivo “HomeGateway”.

g) Finalmente se puede apreciar que tanto “SENSOR” y “GARAJE” no se ven reflejados en la página “Home”. Esto se debe a que no están conectados al dispositivo “HomeGateway”.

Parte 1.1: Actividad de conexión de dispositivos IoT a un Home Gateway.

a) Conecte los dispositivos faltantes al “Home Gateway” y verificar que se encuentran reflejados en la página www.casa.com
Los datos para conexión son los siguientes:

- SSID: **Home**
- WEP Key: **1234567890**
- Remote Server: **192.168.100.10**
- Usuario: **admin**
- Contraseña: **admin**

Parte 2: Automatización de dispositivos IoT.

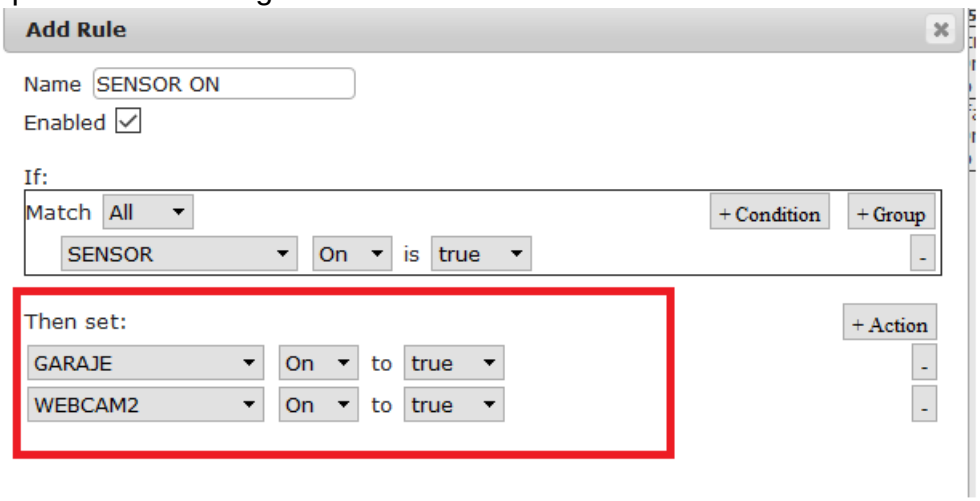
a) En la página www.casa.com, ir a “Conditions”. En esta parte se puede automatizar los dispositivos IoT.
b) Para visualizar el ejemplo, ir a “Home”, abrir la pestaña de “PUERTA ENTRADA” y presionar el botón “Lock”.

c) Se puede apreciar que se ha activado las seguridades de la casa, la puerta está bloqueada, “WEBCAM1” está grabando, la ventana se encuentra cerrada y finalmente se activa la alarma de seguridad.
d) A continuación se automatizará un condicionante para que cuando el sensor detecte movimiento la puerta del garaje se abra y la “WEBCAM2” comience a grabar.
e) Ingrese a “Conditions”, clic en “Add” para agregar un nuevo condicionante.
f) En Nombre ingresar “SENSOR ON”.

g) Ingrese los siguientes datos para el condicionante:

- **Nota:** Se establece el condicionante cuando el sensor se activa o detecta movimiento.

h) Luego se debe especificar las acciones a realizar cuando se cumpla el condicionante. En este caso, seleccione las acciones para que la puerta del garaje se abra y la webcam comience a grabar. Las acciones quedarían de la siguiente manera:



- **Nota:** En caso de ingresar más de una acción, se debe dar clic en el botón “+ Action”.

i) Haga clic en “OK” para guardar el condicionante.

j) Para interactuar con el sensor presionar “ALT” y pasar el cursor por encima del sensor.

Parte 3.1: Actividad de automatización de dispositivos.

a) Complementar el condicionante creado anteriormente con uno nuevo, el cual cierre la puerta del garaje y apague la cámara cuando el sensor deje de detectar movimiento. El condicionante debe llevar el nombre “SENSOR OFF”.

Parte 4: Actividad de configuración red IoT - Oficina.

a) Crear una red inalámbrica en el “Home Gateway” con los siguientes datos:

- SSID: **Office**
- WPA-PSK Key: **0ff1c3N3tw0rk**!

b) Conectar todos los dispositivos IoT y la laptop a la red, crear el usuario en la página www.oficina.com.
   - Remote Server: **192.168.100.20**
   - Usuario: **admin**
   - Contraseña: **admin**

c) Verificar que los dispositivos IoT se reflejen en la página web www.oficina.com

d) Crear condicionantes para que la alarma se encienda cuando la puerta este cerrada o en estado “Lock”.

e) Crear condicionantes para que la cámara se encienda cuando el sensor registre movimiento.

Guía de solución de laboratorio - Configuración de una red IoT

Prerrequisito: Práctica Introductoria IoT.

Parte 1.1: Actividad de conexión de dispositivos IoT a un Home Gateway.

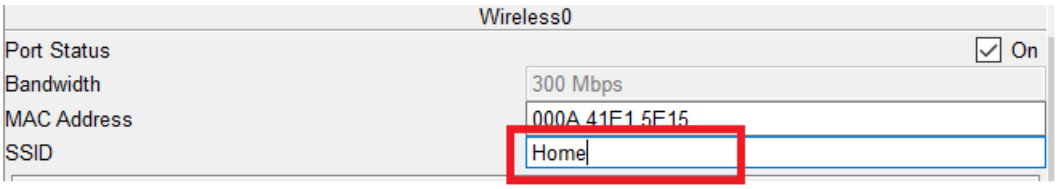
b) Conecte los dispositivos faltantes al “Home Gateway” y verificar que se encuentran reflejados en la página www.casa.com
Los datos para conexión son los siguientes:
   - SSID: **Home**
   - WEP Key: **1234567890**
   - Remote Server: **192.168.100.10**
   - Usuario: **admin**
   - Contraseña: **admin**

Parte 1.1 Resolución: Conexión y configuración de dispositivos IoT.

I. Haga clic en “Sensor” para abrir el menú de configuración. Abra la pestaña de Configuración, posteriormente ingresar a “Wireless0” para configurar la red a la que queremos conectar nuestro dispositivo IoT.

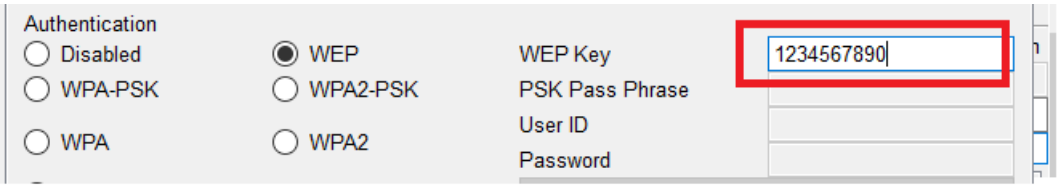
II. La red que está configurada en el dispositivo “HomeGateway” se llama “Home”, por lo tanto, este nombre se debe ingresar en el campo de SSID.

- SSID: **Home**



III. La contraseña de la red está configurada como “WEP”, por lo tanto seleccione en “Authentication” el campo “WEP” y posteriormente ingrese la contraseña.

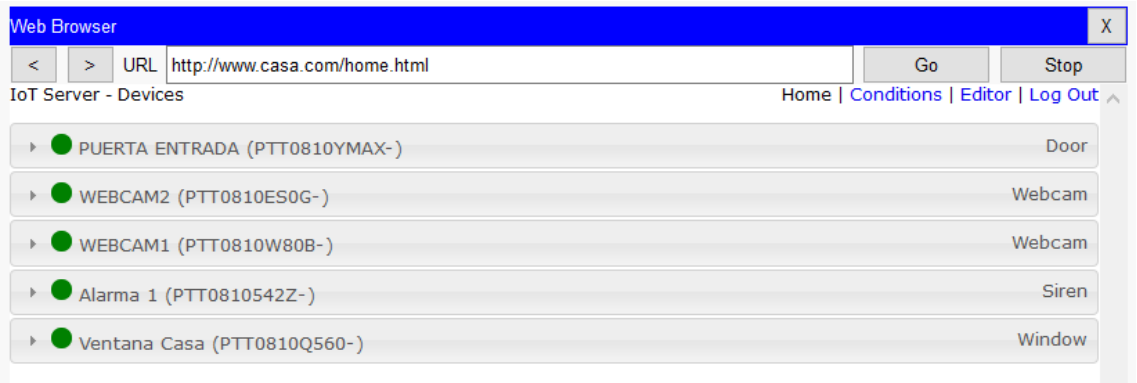
- Contraseña: **1234567890**



IV. Una vez hecho esto, el dispositivo se conecta inalámbricamente al “HomeGateway”.

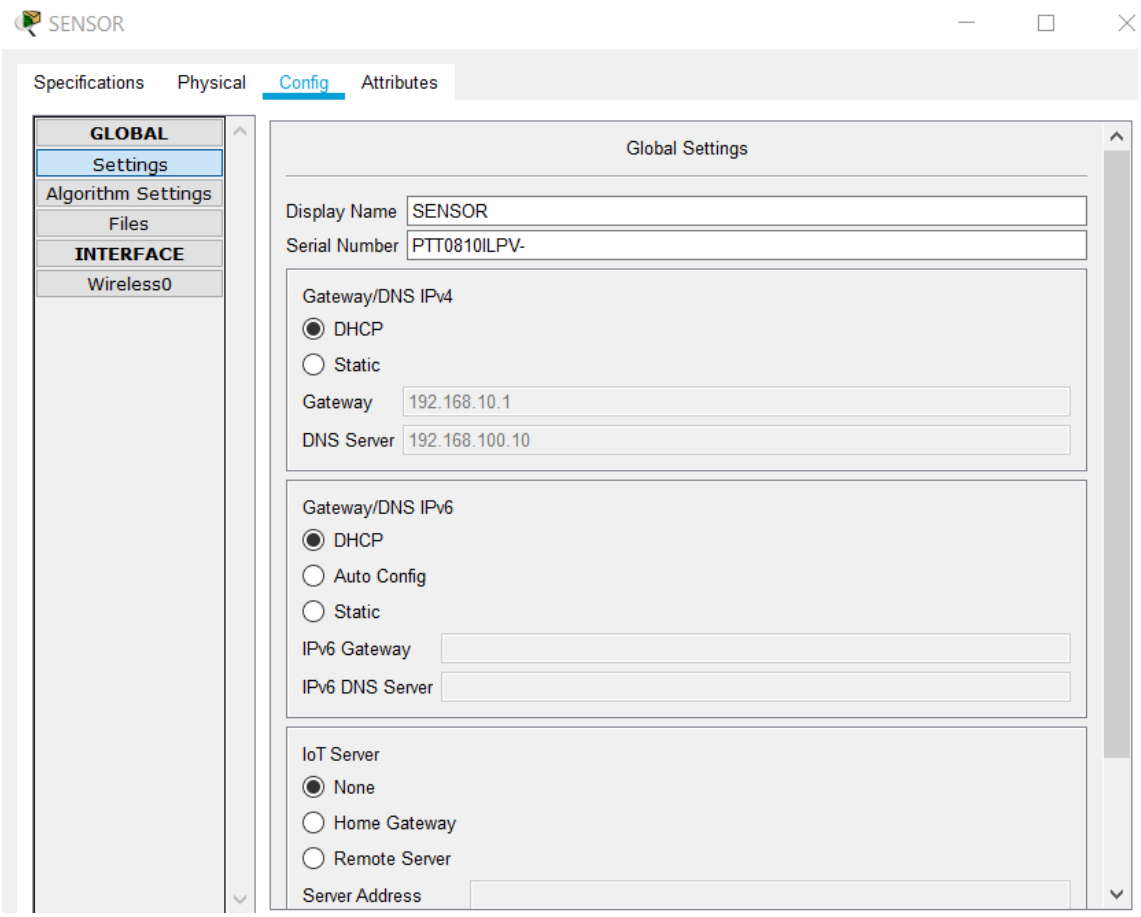
V. Repita estos pasos para conectar el dispositivo IoT “GARAJE”.

VI. Una vez conectados todos los dispositivos, verifique en la página www.casa.com que tanto “SENSOR” y “GARAJE” no se ven reflejados en la página “Home”.

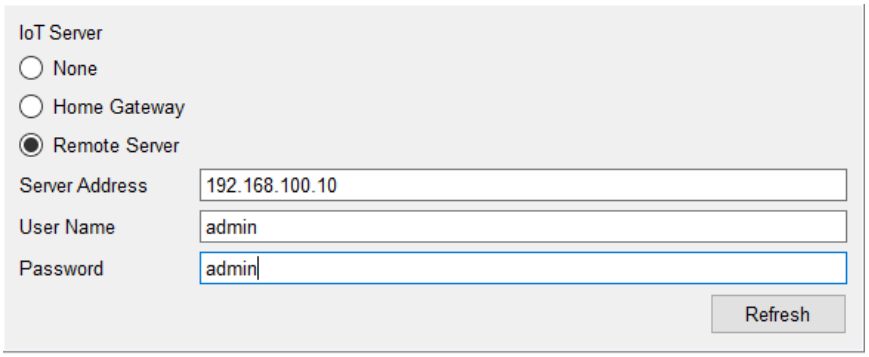


Esto se debe a que los dispositivos no están configurados o apuntando hacia el servidor IoT.

VII. Para la configuración, ingrese a la pestaña de configuración de los dispositivos en “Settings”.

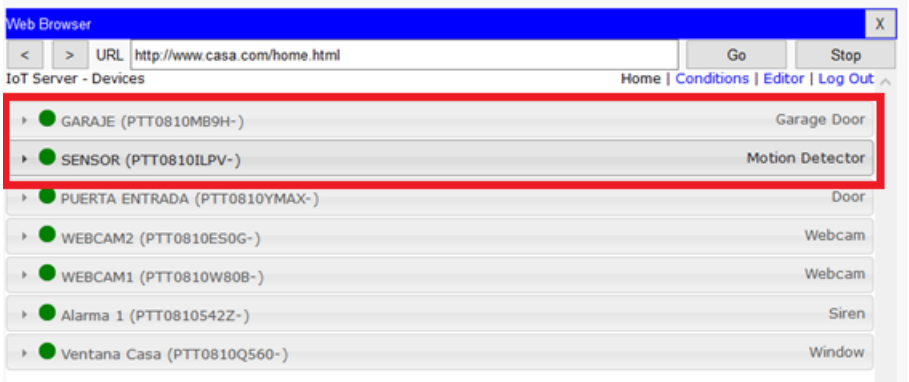


VIII. En la parte de IoT Server seleccione “Remote Server” e ingrese los siguientes datos:



IX. Finalmente haga clic en “Connect”. Los dispositivos estarán sincronizados al servidor enviando datos continuamente.

X. Ingrese a www.casa.com y valide que los dispositivos se encuentran sincronizados. Como se puede apreciar en la siguiente imagen:

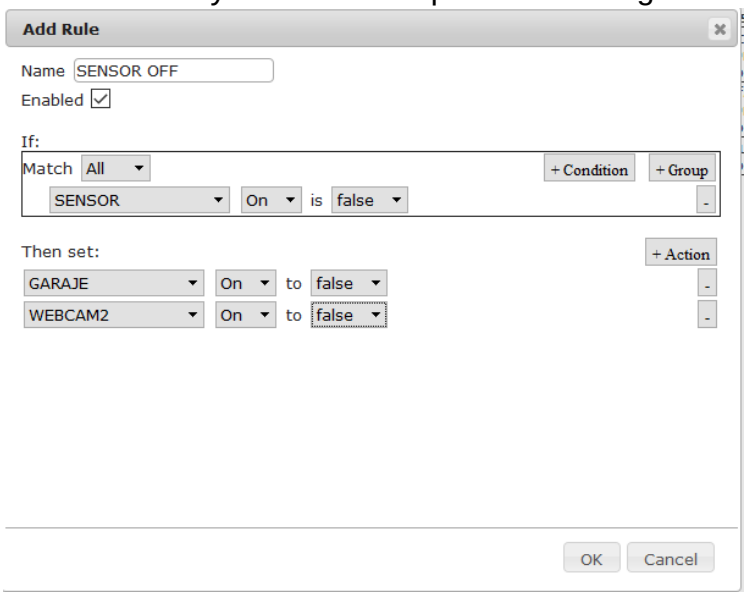


Parte 3.1: Actividad de automatización de dispositivos.

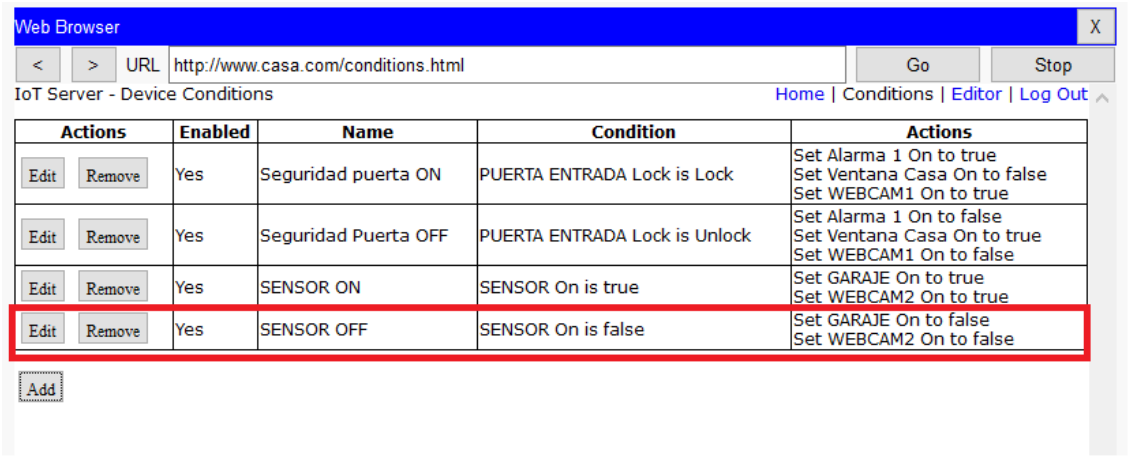
b) Complemente el condicionante creado anteriormente con uno nuevo, el cual cierre la puerta del garaje y apague la cámara cuando el sensor deje de detectar movimiento. El condicionante debe llevar el nombre “SENSOR OFF”.

Parte 3.1 Resolución: Actividad de automatización de dispositivos.

I. Seleccione “Add”, ingrese el nombre “SENSOR OFF”.
II. Seleccione el condicionante de sensor para que en caso de que este apagado cumpla las acciones a ingresar.
III. Ingrese las acciones para que tanto la puerta de garaje y la webcam estén en estado apagado cuando el condicionante se cumpla. El condicionante y las acciones quedan de la siguiente manera:



IV. Clic en “OK” para guardar el condicionante. Una vez guardado se ve reflejado de la siguiente manera:

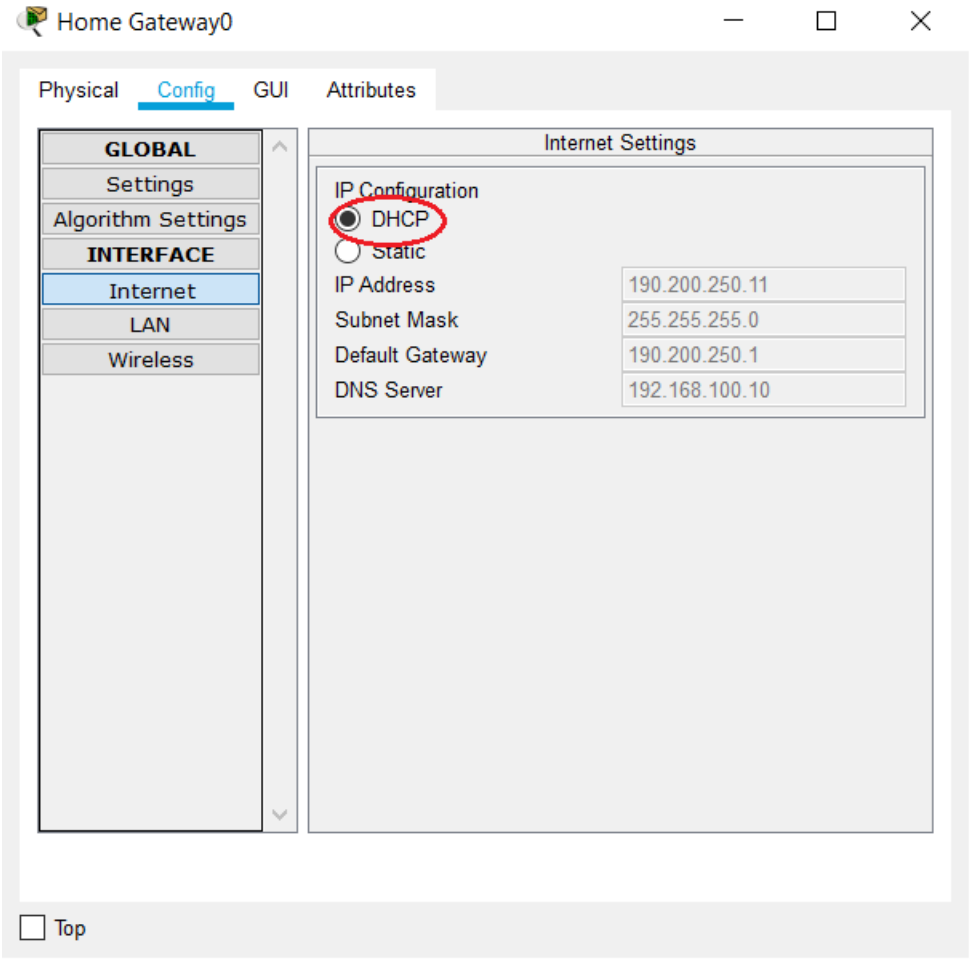


Parte 4 Resolución: Actividad de configuración red IoT - Oficina.

f) Crear una red inalámbrica en el “Home Gateway” con los siguientes datos:
   - SSID: **Office**
   - WPA-PSK Key: **0ff1c3N3tw0rk**!

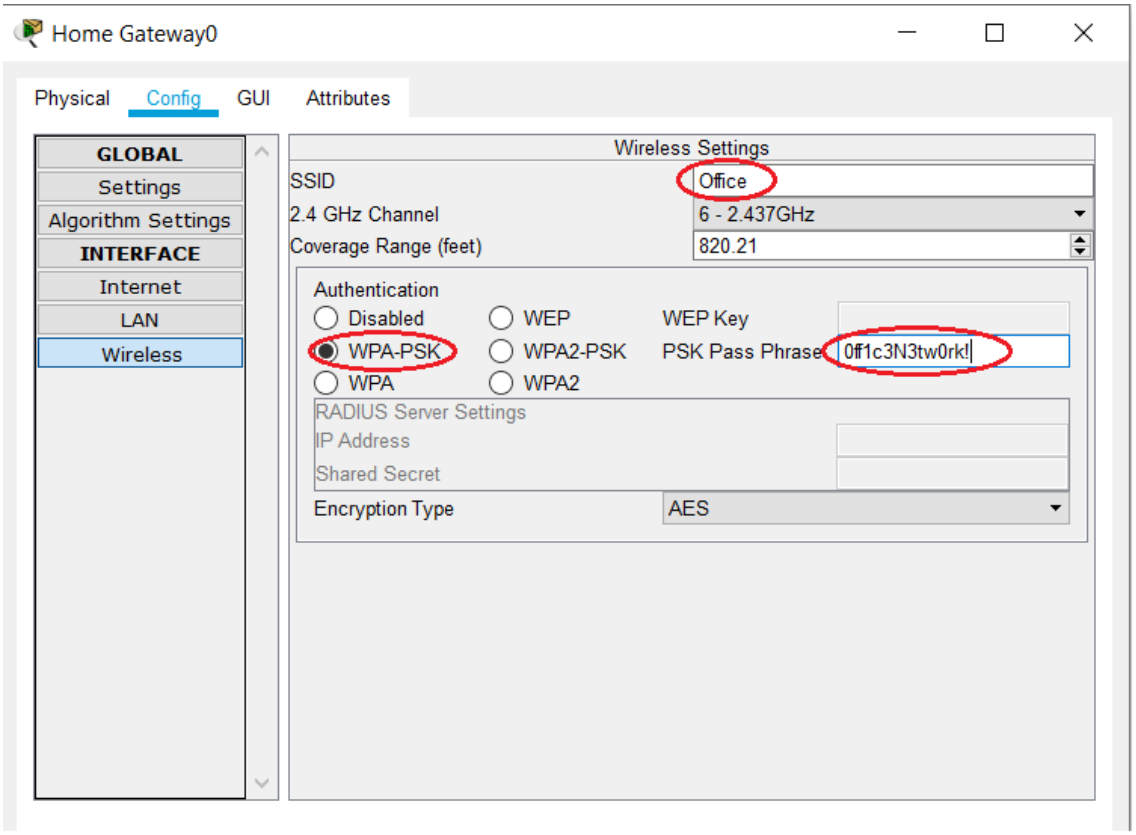
I. Seleccione “HomeGateway” y abra las configuraciones de internet.

II. Seleccione “DHCP”.



III. Seleccione la pestaña de “Wireless”.

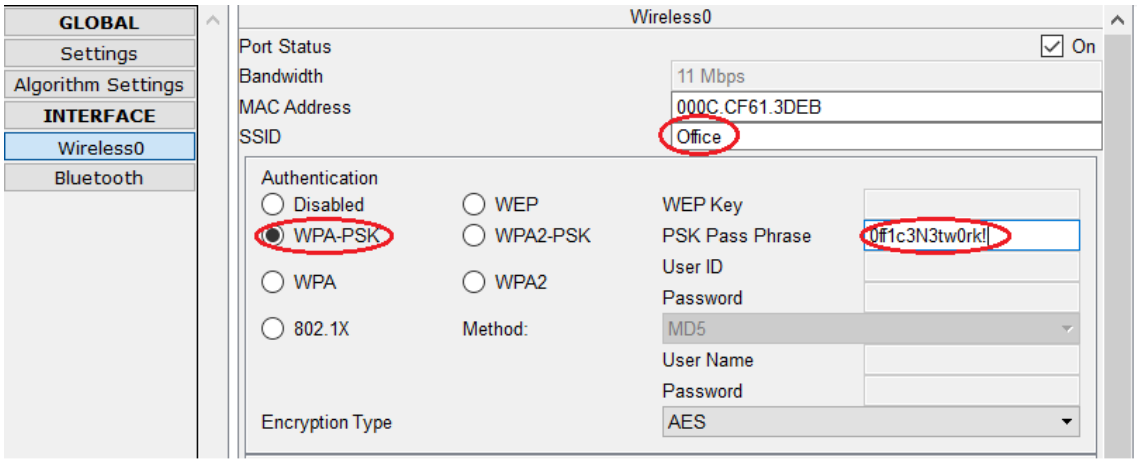
IV. Ingrese los datos proporcionados en el enunciado de la siguiente manera:



g) Conectar todos los dispositivos IoT y la laptop a la red, crear el usuario en la página www.oficina.com.

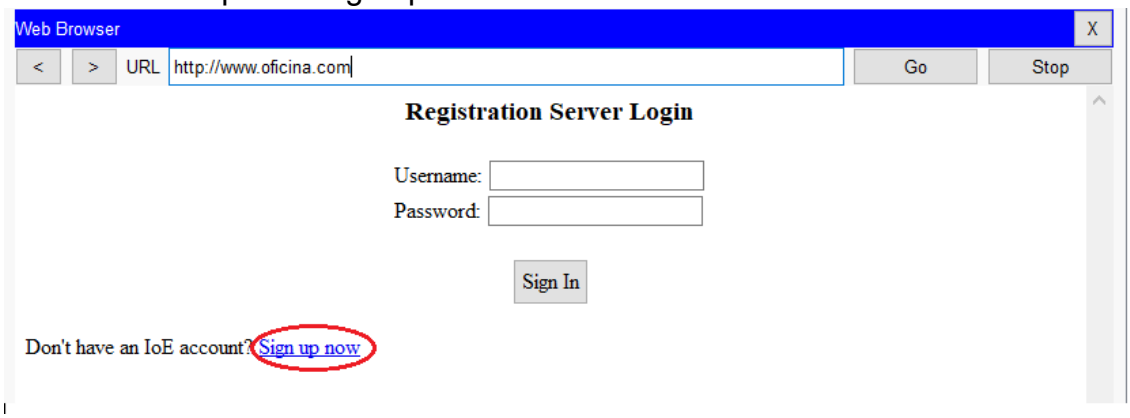
- Remote Server: **192.168.100.20**
- Usuario: **admin**
- Contraseña: **admin**

I. Haga clic en la laptop para abrir las configuraciones.
II. Seleccione la pestaña de configuración, seleccione “Wireless” para conectar a la red inalámbrica.
III. Ingresar los siguientes datos:

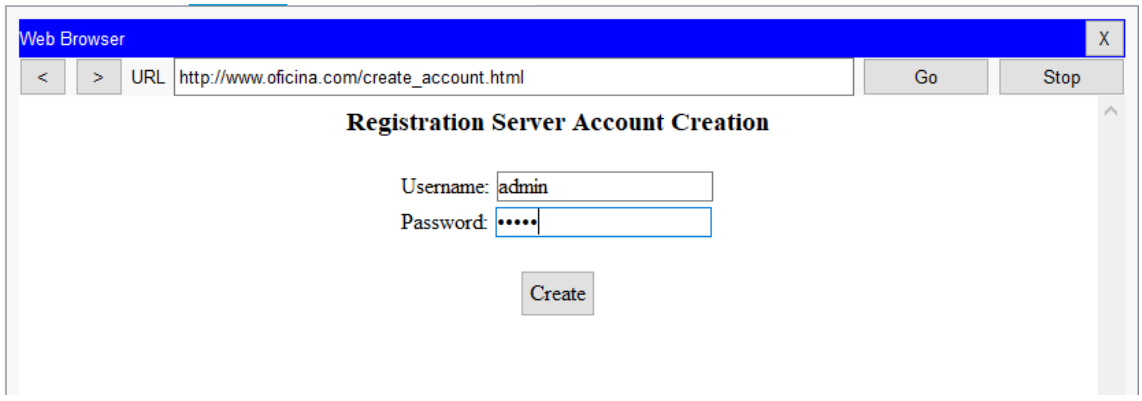


IV. Ingrese al navegador web y digite www.oficina.com

V. Seleccione la opción “Sign up now”

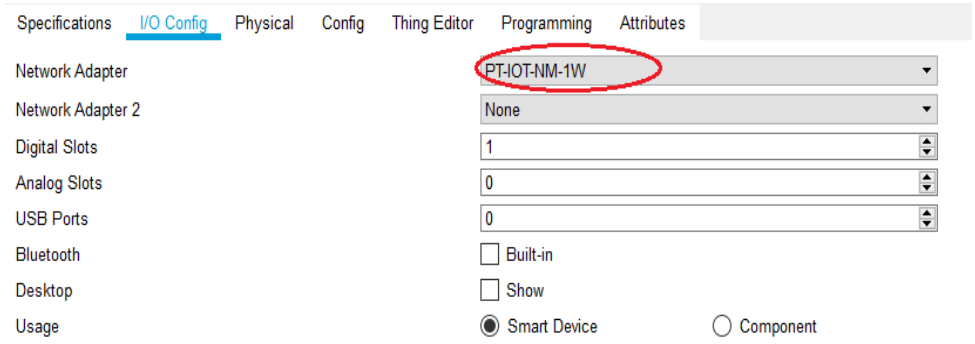


VI. Ingresar las credenciales indicadas en la actividad y de clic en el botón “Create”



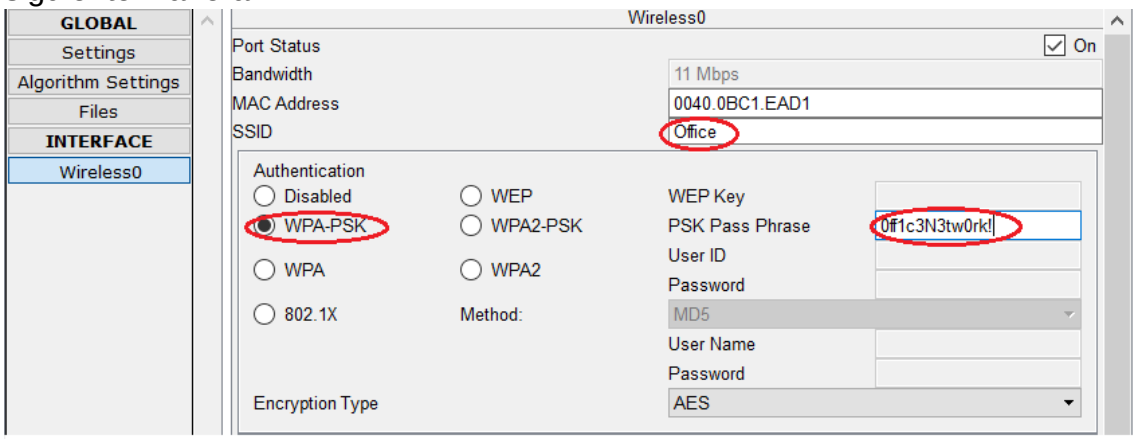
VII. Haga clic en el dispositivo para abrir la ventana de “Especificaciones”, posteriormente clic en el botón “Advanced” ubicado en la parte inferior derecha.

VIII. Seleccione la pestaña de “I/O Config”, en “Network Adapter” seleccione “PT-IOT-NM-1W”. Esto agrega un adaptador inalámbrico al dispositivo.



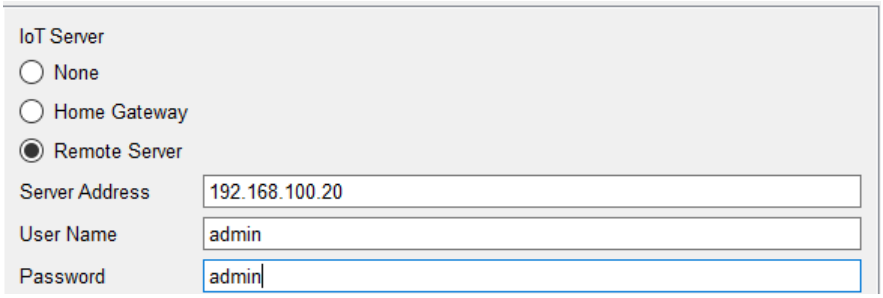
IX. Seleccione la pestaña de configuración. Posteriormente seleccione la pestaña de configuración “Wireless”.

X. Ingrese los datos de la red inalámbrica indicados en la actividad de la siguiente manera:

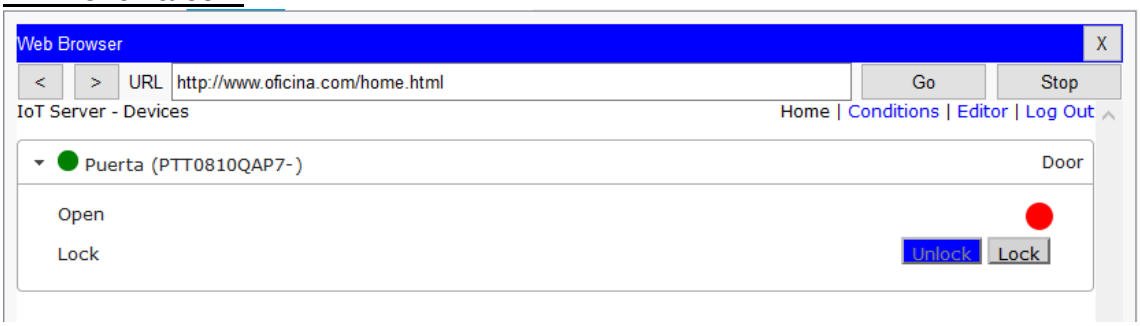


XI. Abra la pestaña de configuración y en la parte de “IoT Server”, seleccione “Remote Server”.

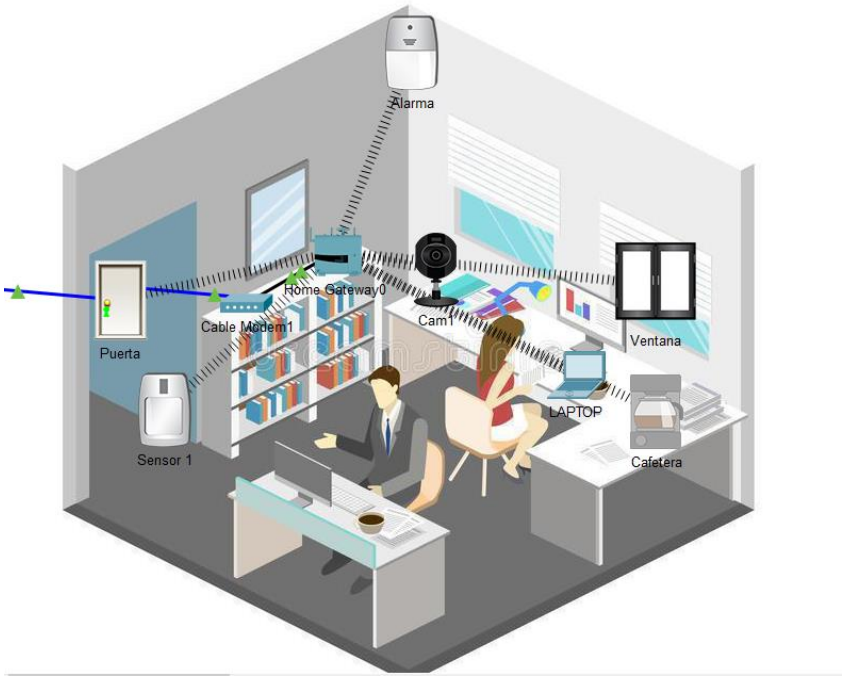
XII. Ingrese los siguientes datos:



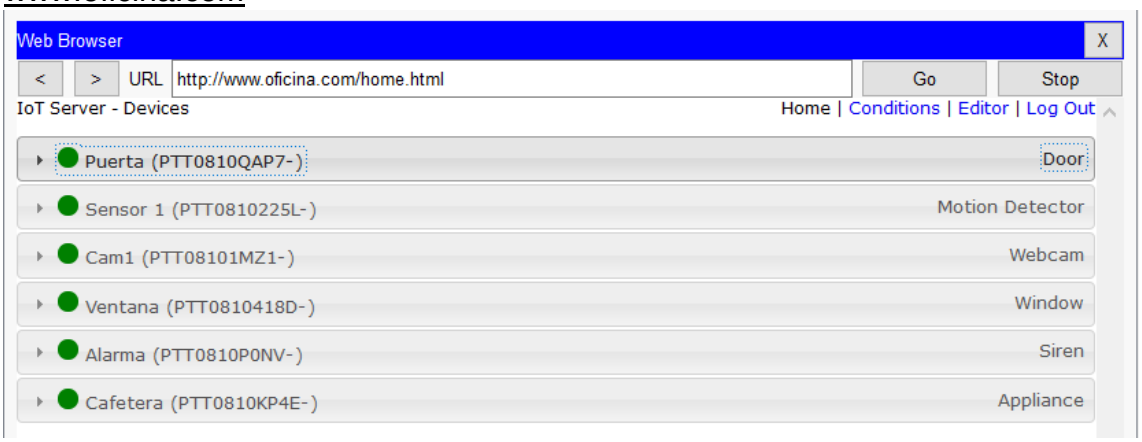
XIII. Verifique que el dispositivo este reflejado en la página web www.oficina.com



XIV. Repita los pasos 7 – 12 para los demás dispositivos.



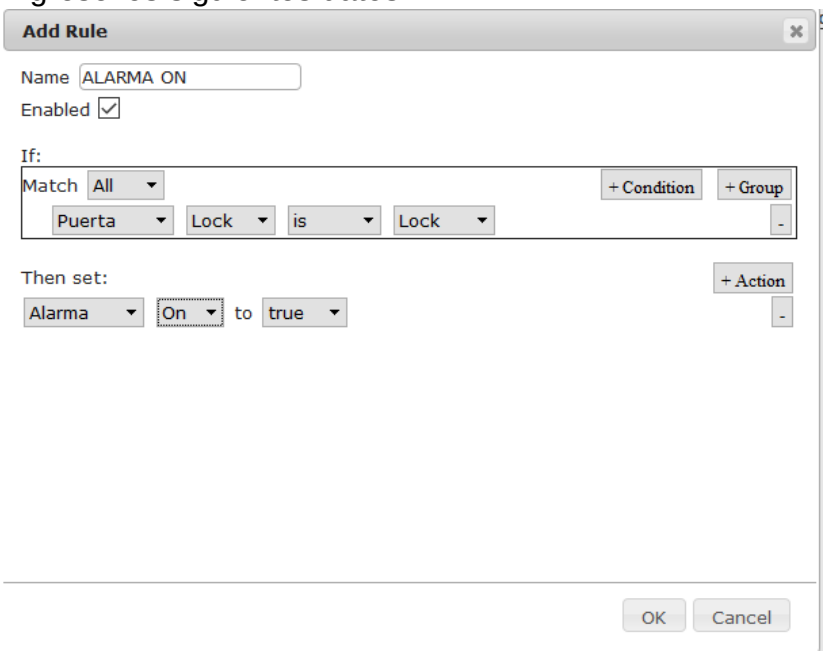
h) Verificar que los dispositivos IoT se reflejen en la página web www.oficina.com



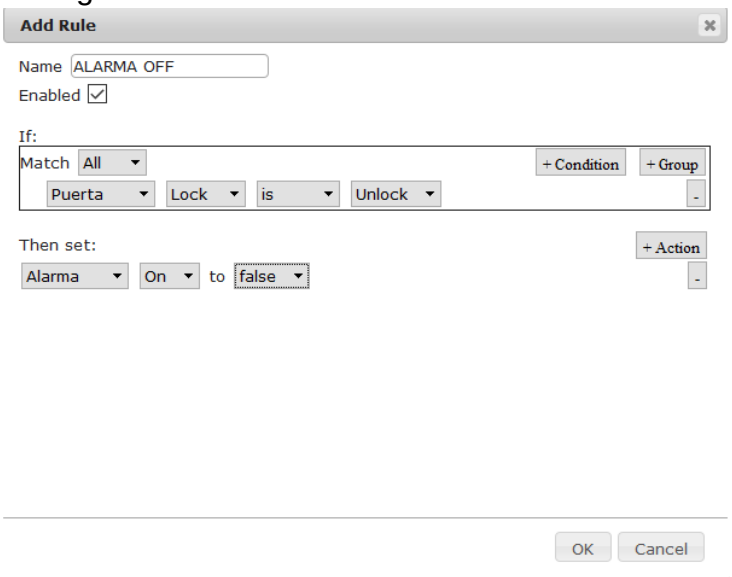
i) Crear condicionantes para que la alarma se encienda cuando la puerta este cerrada o en estado “Lock”.

- Seleccione “Add”, ingrese el nombre “ALARMA ON”.

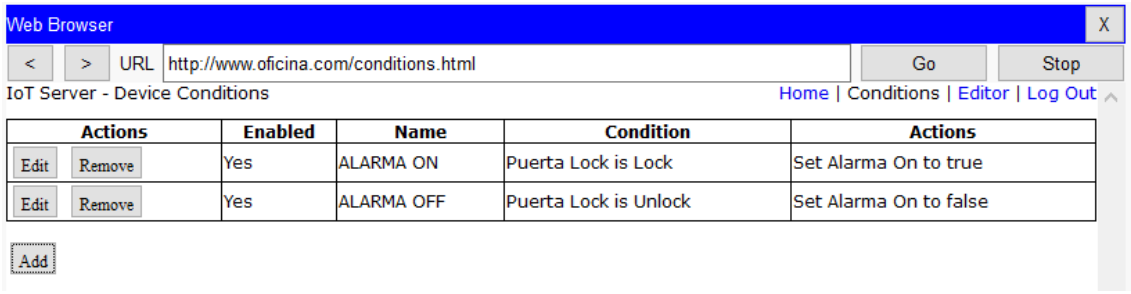
- Ingrese los siguientes datos:

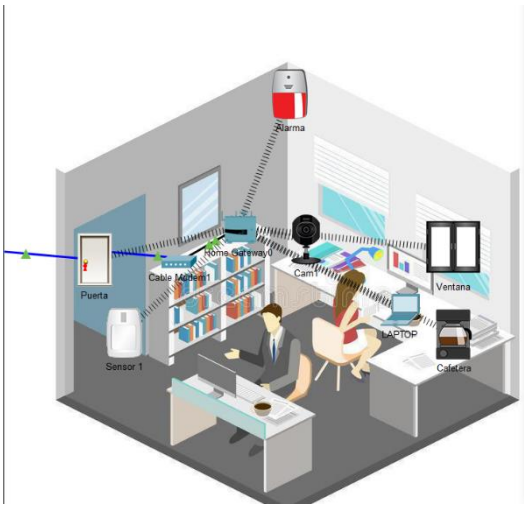


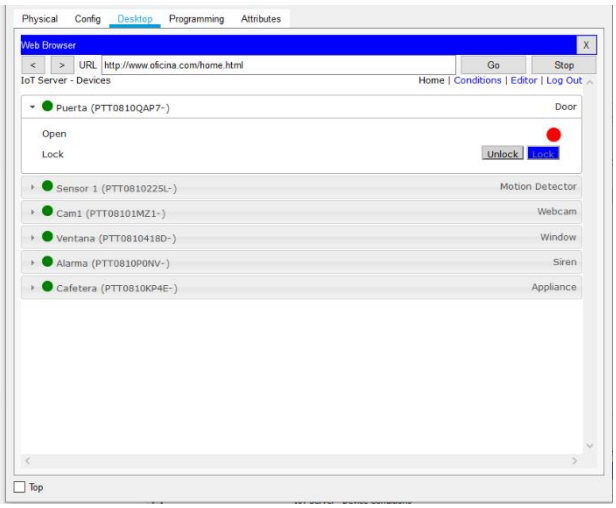
- Haga clic en “OK” para guardar.
- Repetir los pasos 1-3 para crear el condicionante de apagado con los siguientes datos:



- Las dos condiciones se deben visualizar de la siguiente manera:

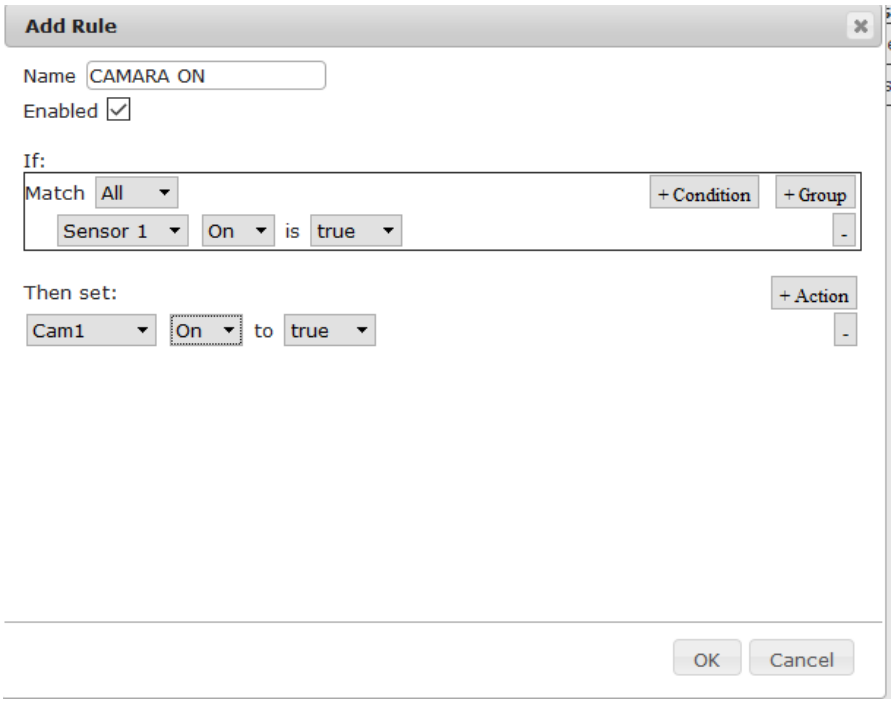






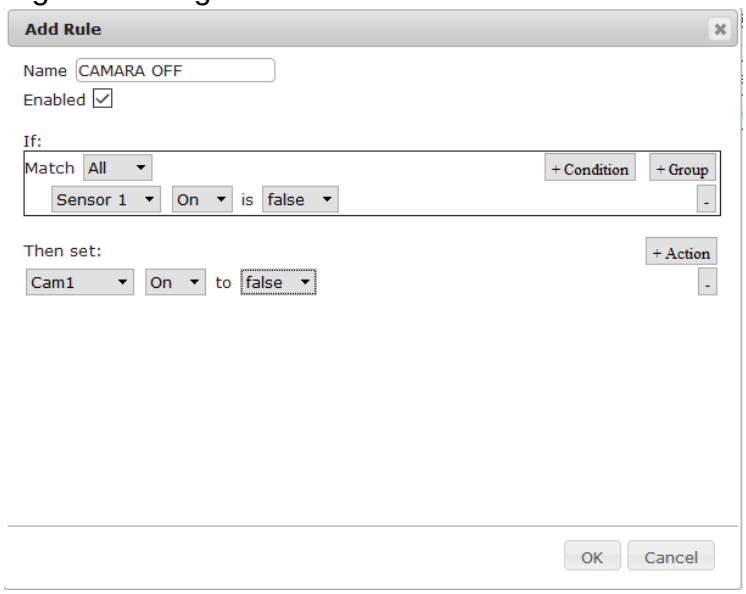
j) Crear condicionantes para que la cámara se encienda cuando el sensor registre movimiento.

- Seleccione “Add”, ingrese el nombre “CAMARA ON”.
- Ingrese los siguientes datos:

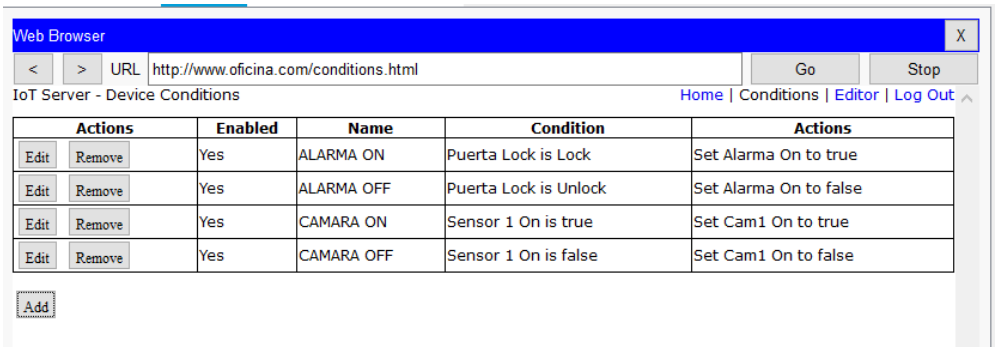


- Haga clic en “OK” para guardar.
- Seleccione “Add”, ingrese el nombre “CAMARA OFF”.

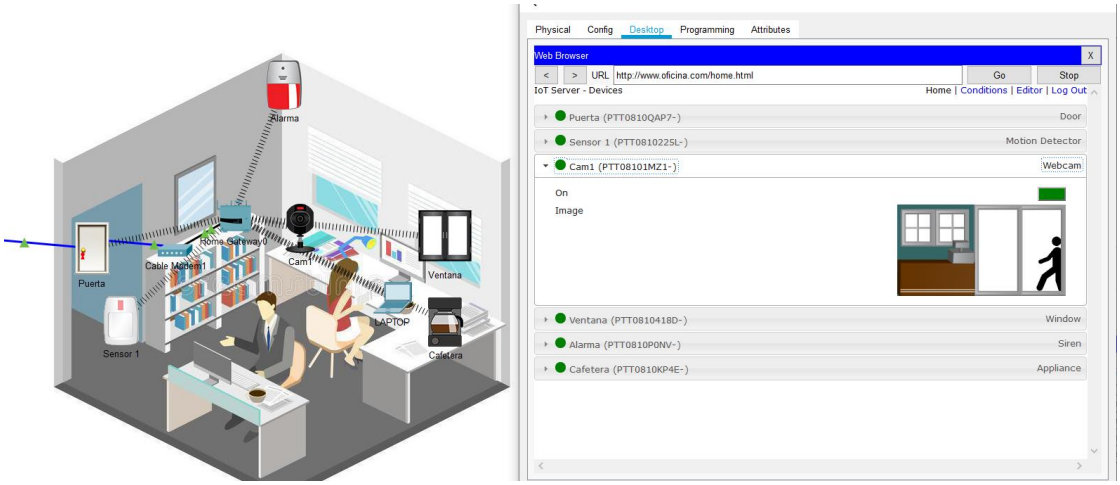
- Ingrese los siguientes datos:



- Haga clic en “OK” para guardar.
- Verificar que los condicionantes estén creados de la siguiente manera:



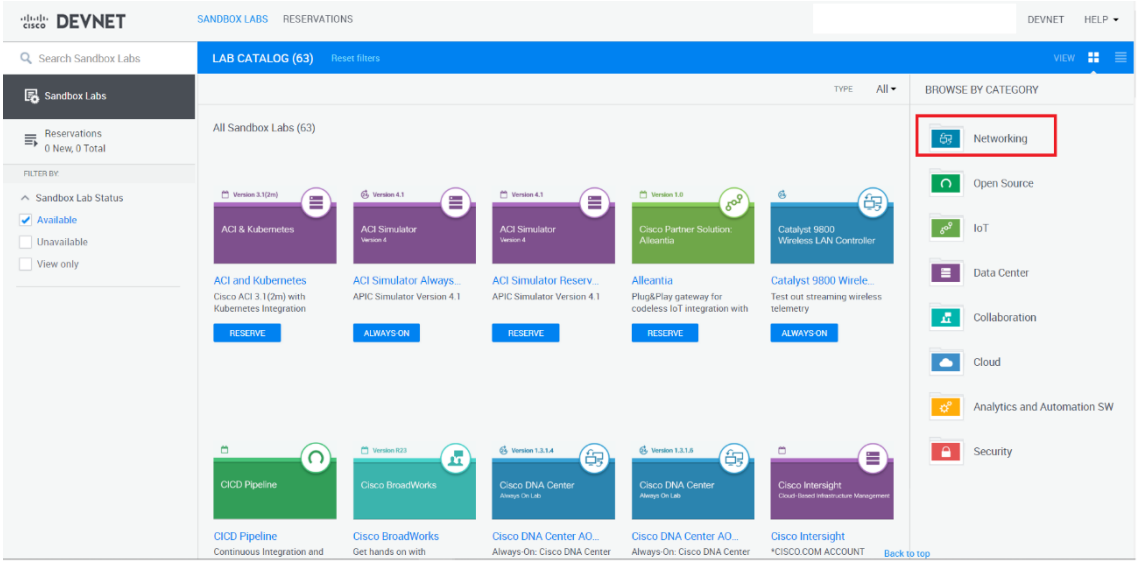
- Abra el panel de “CAM1”.
- Presione “ALT” y pase el cursor por el sensor para interactuar con el mismo y verifique que el condicionante esté funcionando. Este proceso se puede apreciar en la siguiente imagen:



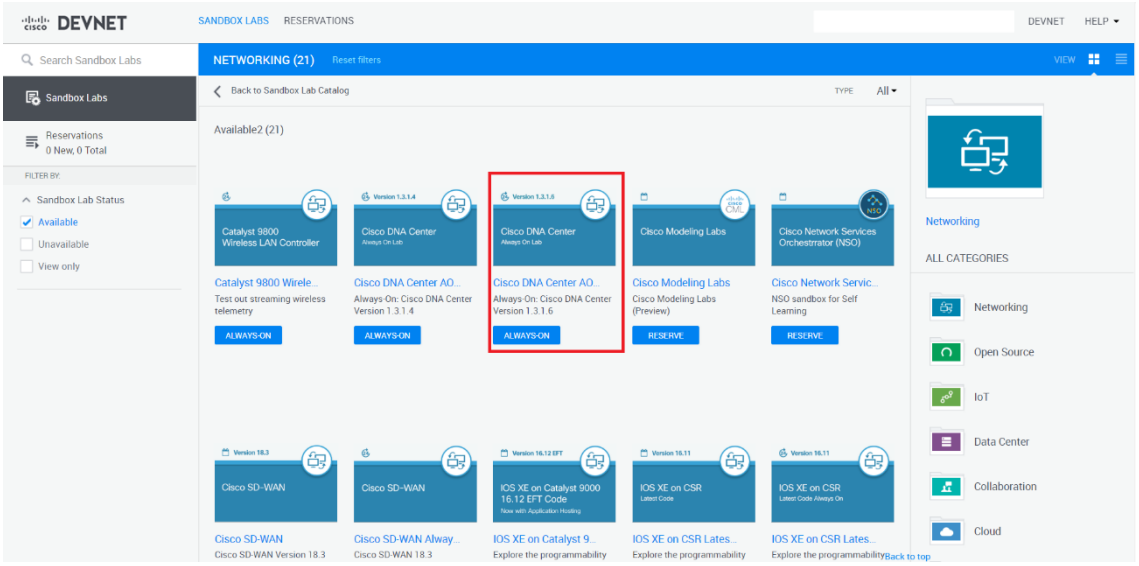
Guía de laboratorio – Introducción a DNA y sus componentes.

Parte 1: Ingreso a Laboratorio de Sandbox.

h) Ingrese al catálogo de laboratorios de “Sandbox” indicados en el manual de uso de Devnet.
i) Seleccione el área de “Networking”.

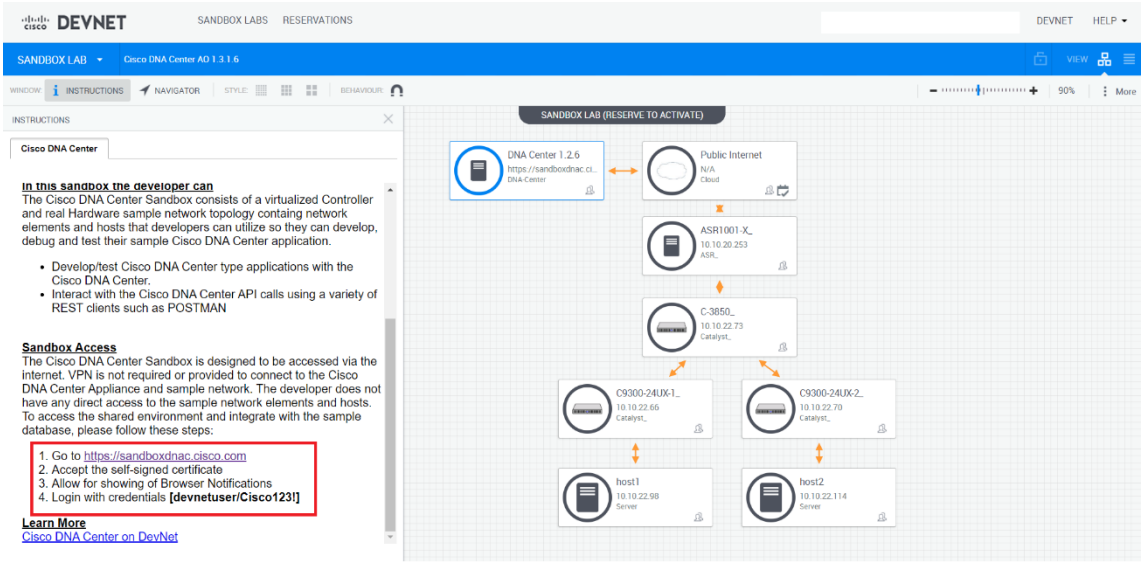


j) Seleccione “ALWAYS-ON” para abrir el laboratorio “Cisco DNA AO 1.3.1.6”.



Parte 2: Exploración DNA Center.

h) Desplace el mouse hacia la parte de las instrucciones del laboratorio.

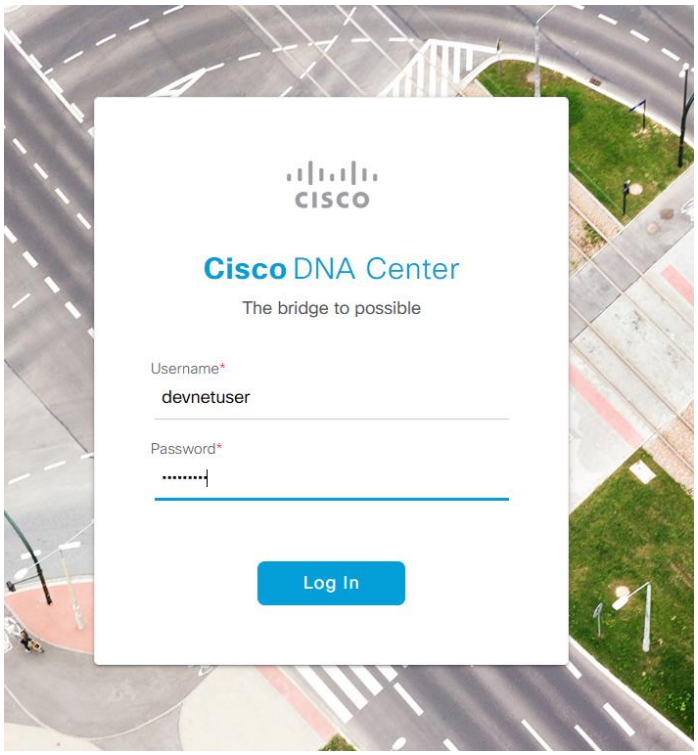


i) Seleccione o de clic en el link **https://sandboxdnac.cisco.com**

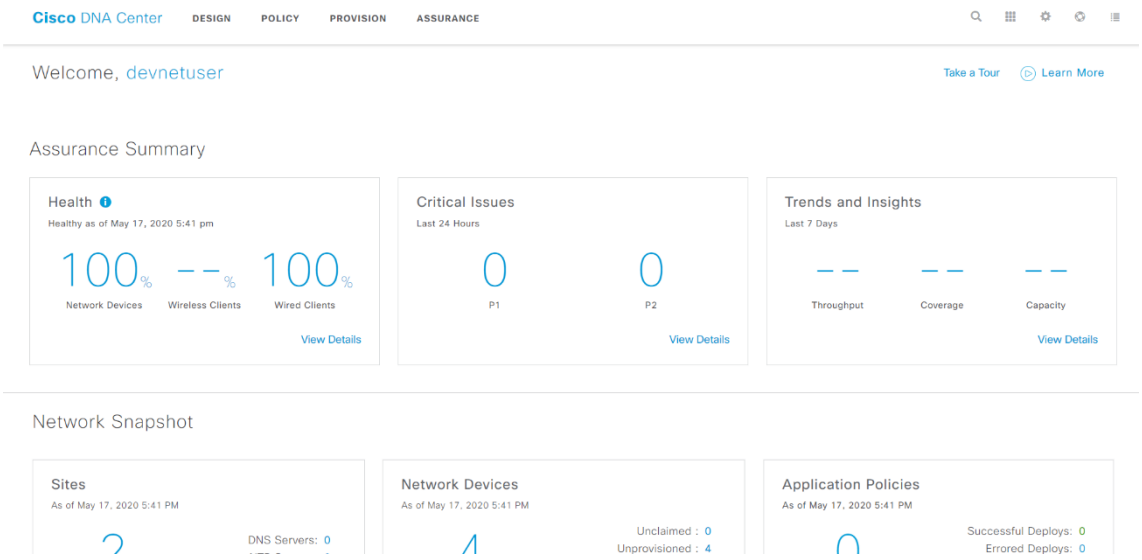
j) Ingrese las siguientes credenciales de acceso:

   a. Usuario: **devnetuser**

b. Contraseña: **Cisco123!**

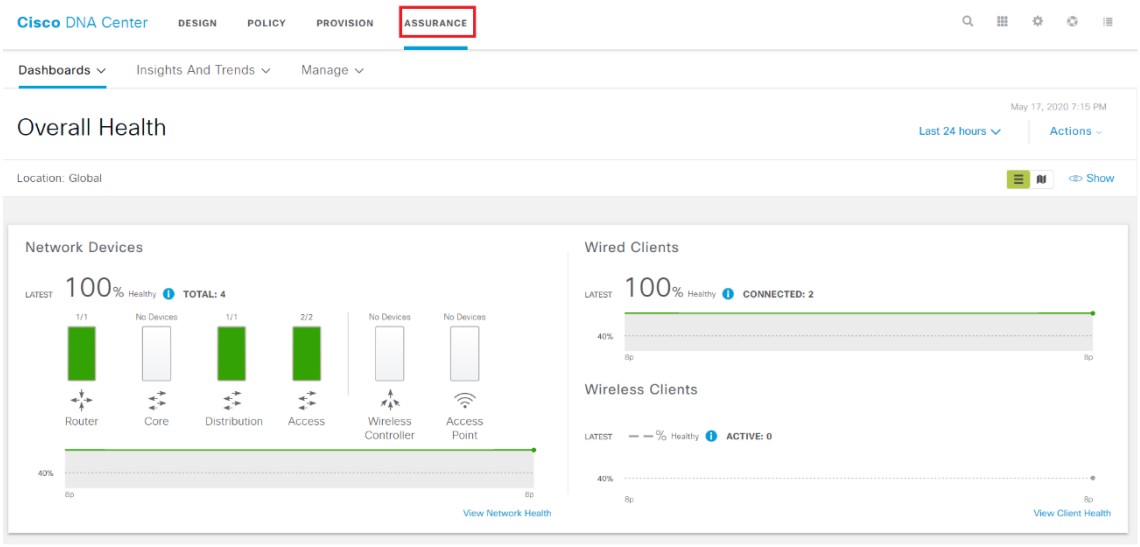


k) Seleccione “Log In”.
l) Se desplegara una página de inicio o “Dashboard” de Cisco DNA Center.



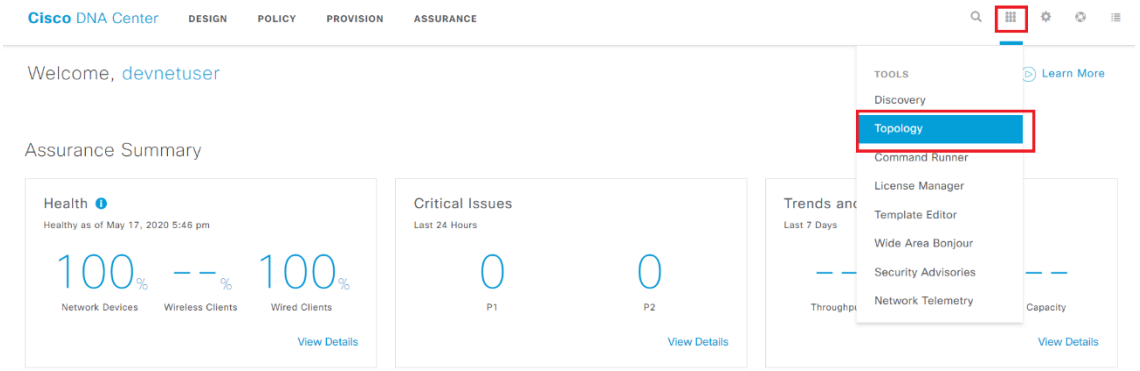
- **Nota:** En esta página de inicio se puede apreciar un breve resumen sobre el estado de los dispositivos en la red al igual que los problemas críticos que presente la red en este momento.

m) Seleccionar “Assurance”.

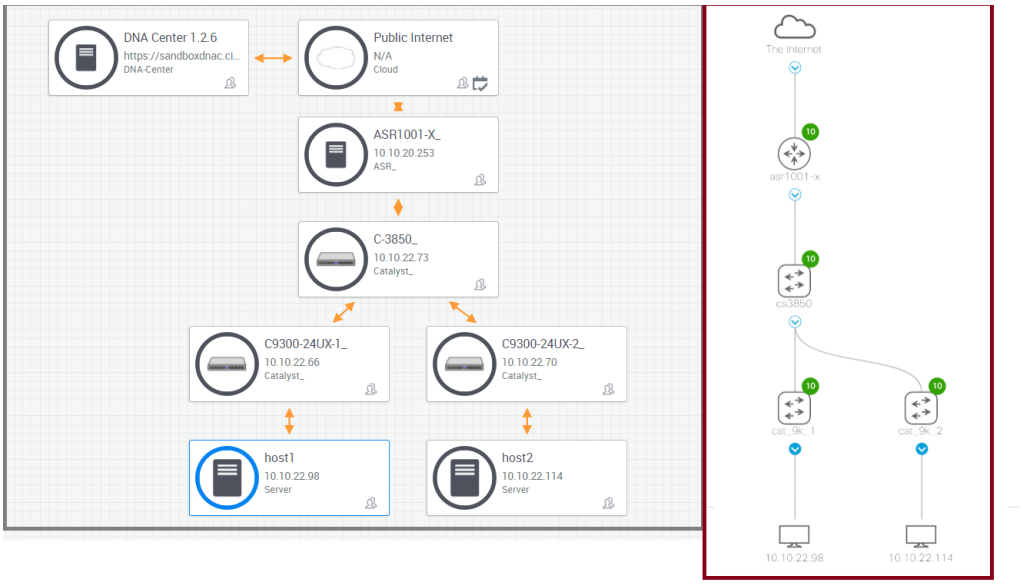


- **Nota:** En el panel se puede apreciar el estado de salud de todos los dispositivos conectados a la red. DNA Center reconoce las redes alámbricas e inalámbricas.

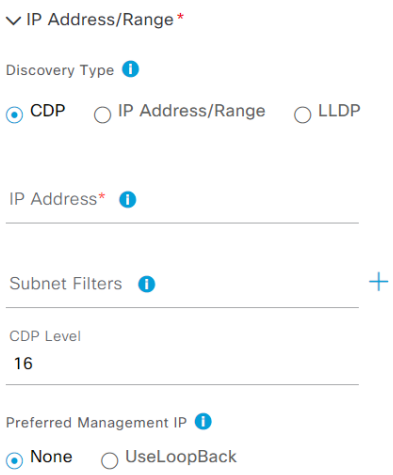
n) Seleccione “Tools” y posteriormente seleccione “Topology”.



o) En la nueva ventana desplegada seleccione “Global”.
p) En la topología desplegada seleccione las dos flechas azules debajo de los “switch catalyst” para desplegar los dispositivos conectados a los mismos.
q) La topología desplegada debe ser igual a la mostrada en el laboratorio de “Sandbox”.

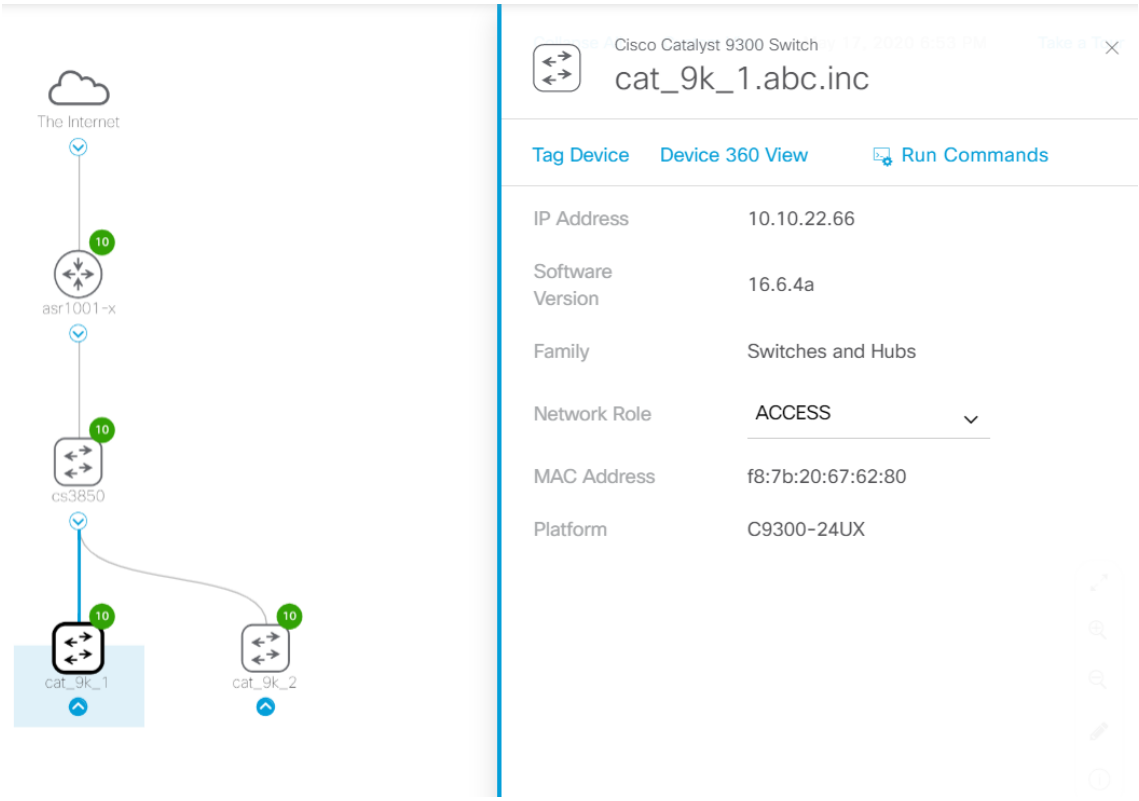


- **Nota:** Cisco DNA Center realiza un descubrimiento de una red indicada ya sea por IP, CDP, LLDP. Esto se puede apreciar en la siguiente imagen.

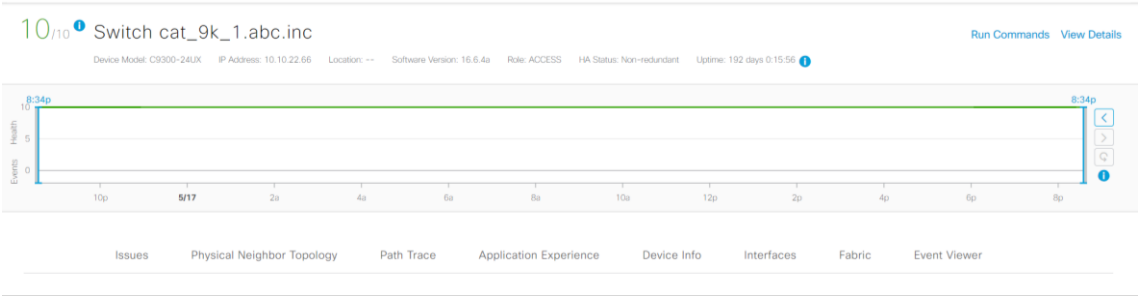


Parte 3: Interacción con dispositivos de DNA Center.

a) Seleccione el switch “cat_9k_1”.

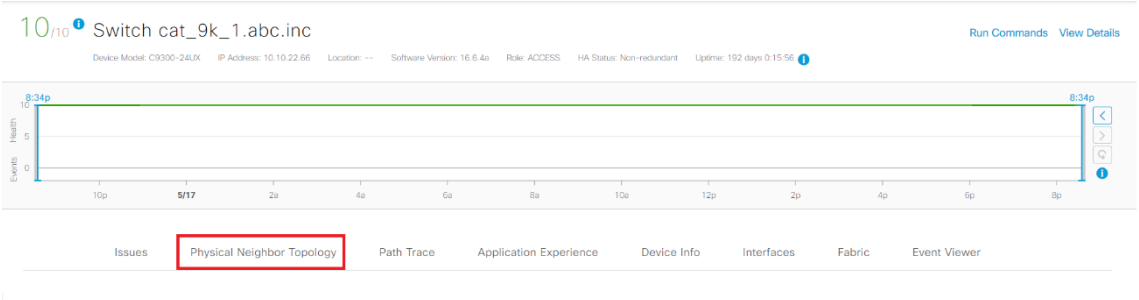


b) Seleccione en la misma ventana la pestaña de “Device 360 View”

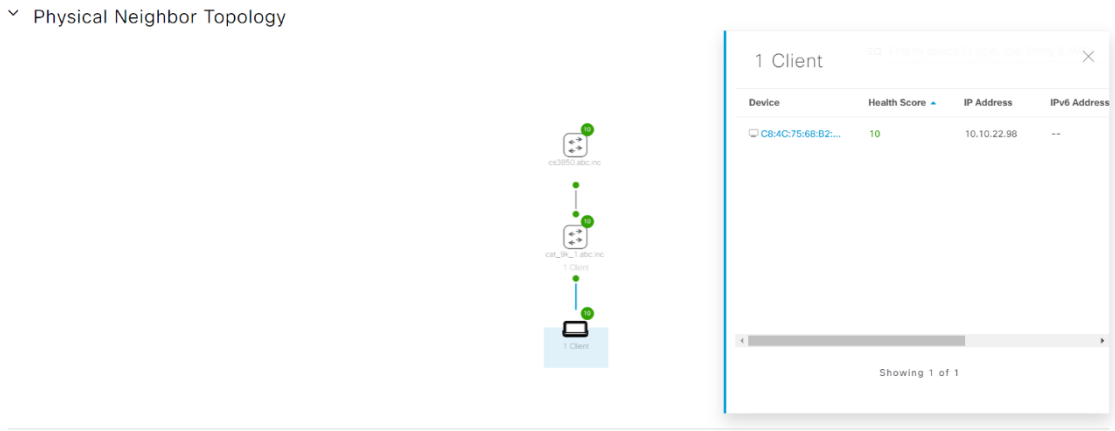


- **Nota:** La vista 360 permite visualizar todos los datos posibles del dispositivo. Tales como: estado de conexión, modelo del equipo, dirección IP, versión de software, etc.

c) Seleccione “Physical Neighbor Topology”.

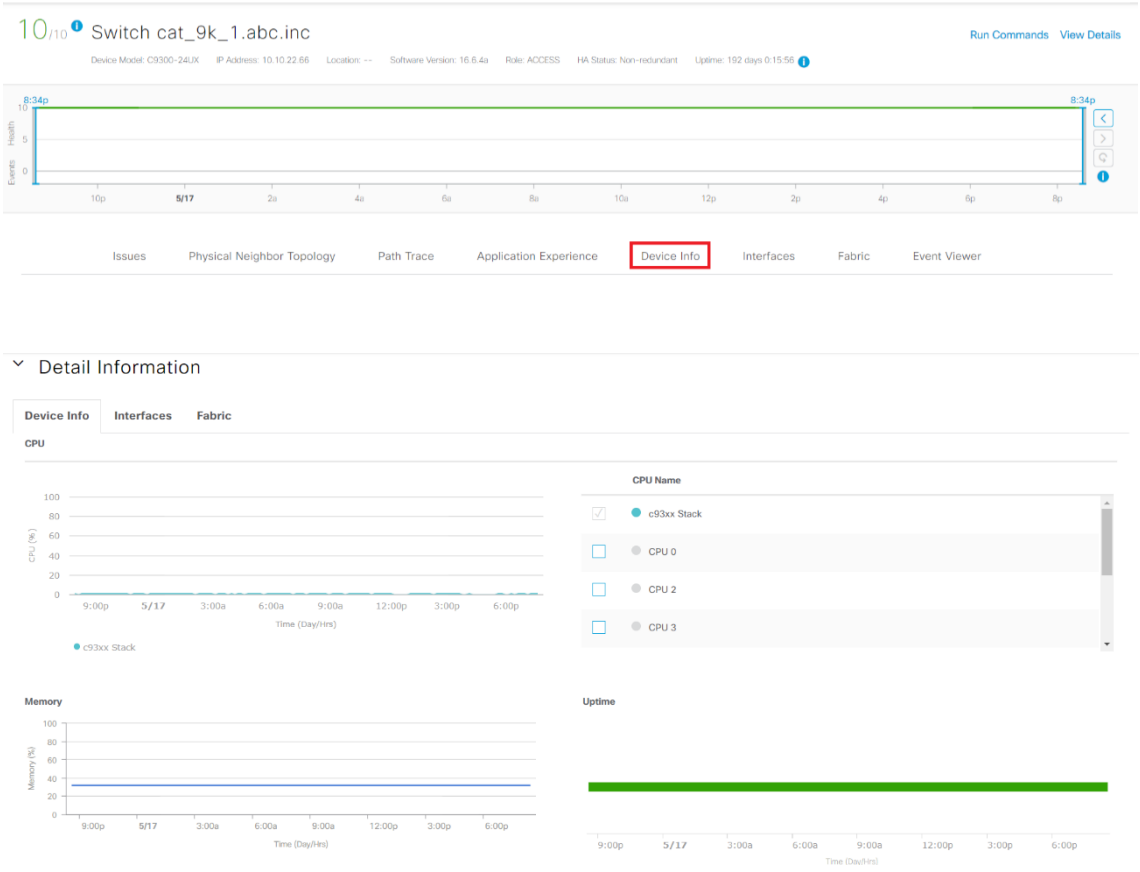


d) Esta funcionalidad permite la visualización de los dispositivos conectados al equipo.



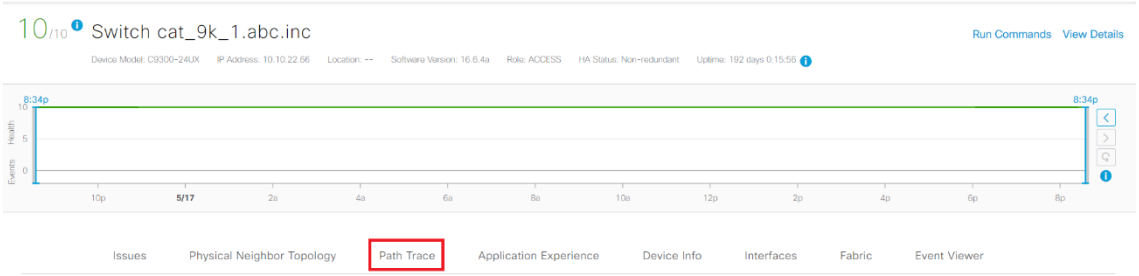
- **Nota:** Al dar clic sobre cliente se despliega la lista de dispositivos conectados al switch.

e) Seleccione “Device Info”.

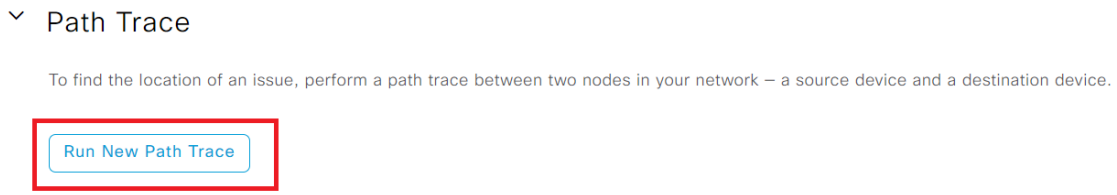


- **Nota:** Esta ventana despliega toda la información o estado del equipo. Tal como: uso del CPU, uso de la memoria y temperatura.

f) Seleccione “Path Trace”.

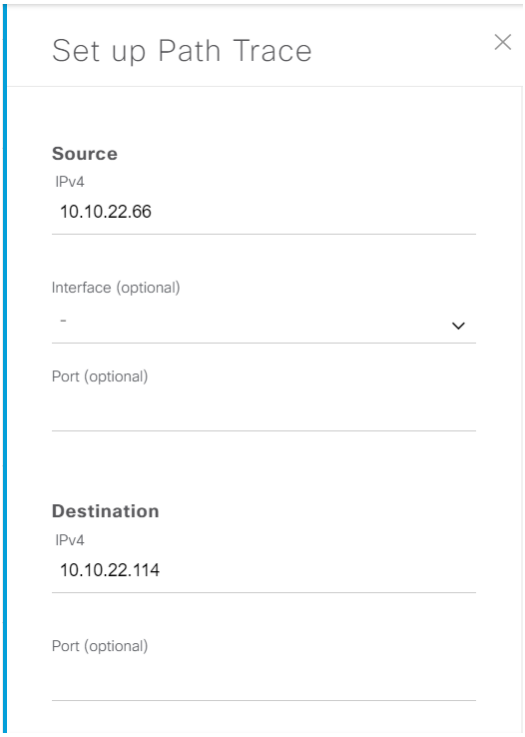


g) Seleccione “Run New Path Trace”.

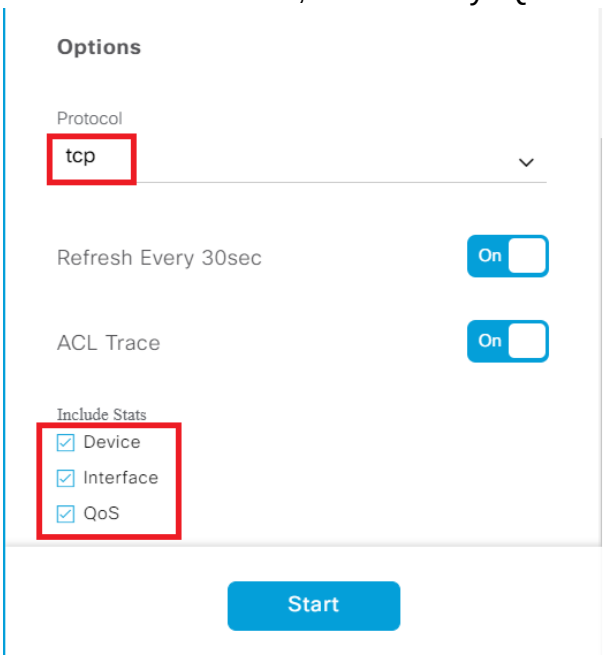


- **Nota:** Con “Path Trace” se logra un reconocimiento de todo el recorrido que realizan los paquetes desde una IP de origen (incluidos puertos) a una IP de destino. Los detalles que puede desplegar por ejemplo son: puertos, VLANS, protocolos y estado de salud en el recorrido.

h) En “Destination” seleccione la dirección IP del otro dispositivo host (10.10.22.114).

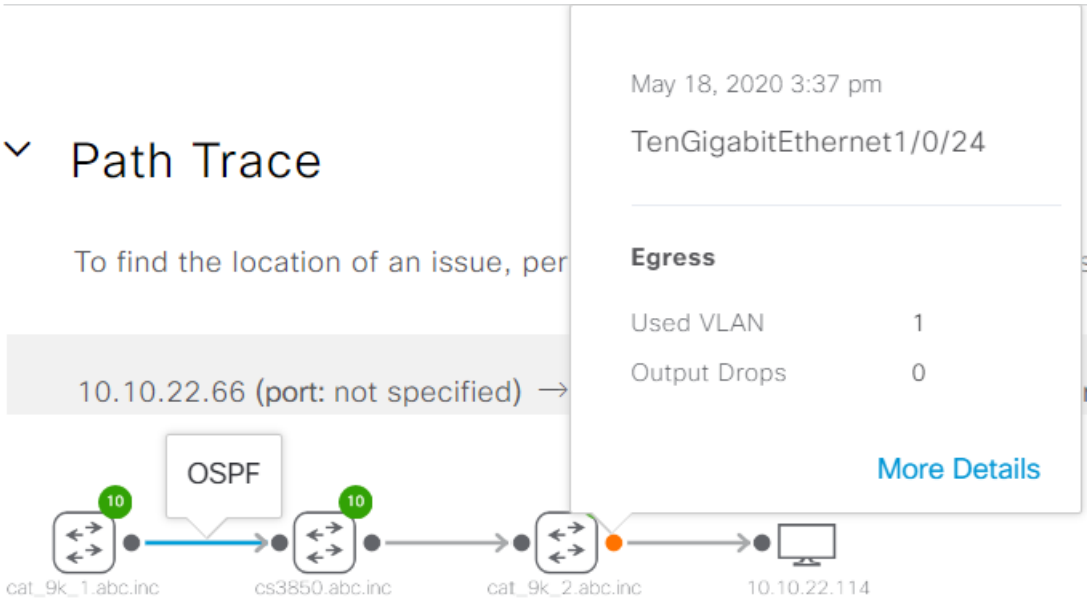


i) Seleccione el protocolo “TCP”.
j) Seleccione las casillas de: “Device”, “Interface” y “QoS”.



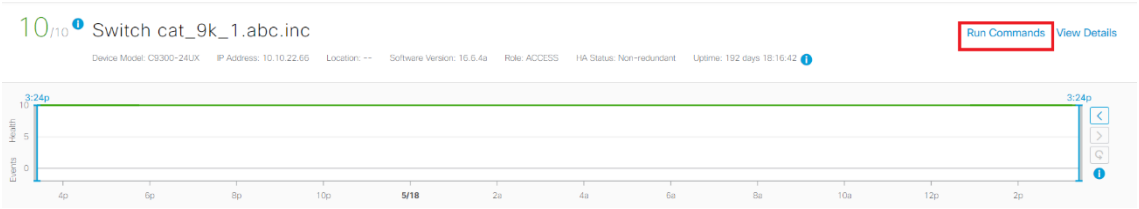
- **Nota:** Las estadísticas incluyen datos de los dispositivos, interfaces y calidad de servicio en el trayecto.

k) Seleccione “Start” para realizar el escaneo.



- **Nota:** Permite la visualización del tipo de enrutamiento utilizado, puertos por los cuales se comunican los dispositivos y la VLAN usada para comunicación con el destino, etc.

l) Seleccione “Run Commands”



- **Nota:** Esto permite la interacción con el dispositivo mediante comandos CLI.

m) Ingrese “show ver” para ver los datos del dispositivo tales como: número de serie, dirección MAC, etc.

```
cat_9k_1.abc.inc@10.10.22.66

Welcome to Cisco DNA Center command runner.

You can access this window from anywhere using the key combination Q+T.
You can access recently viewed devices using the key combination Q+D.


Note: You can enter "man" anytime to get the list of currently supported commands and shortcuts.

cat_9k_1.abc.inc # show ver
cisco C9300-24UX (X86) processor with 1392681K/6147K bytes of memory.
Processor board ID FCW2136L0AK
1 Virtual Ethernet interface
4 Gigabit Ethernet interfaces
32 Ten Gigabit Ethernet interfaces
2 Forty Gigabit Ethernet interfaces
2048K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
1638400K bytes of Crash Files at crashinfo:.
11264000K bytes of Flash at flash:.
0K bytes of WebUI ODM Files at webui:.

Base Ethernet MAC Address          : f8:7b:20:67:62:80
Motherboard Assembly Number        : 73-17958-06
Motherboard Serial Number          : FOC21316VXP
Model Revision Number              : A0
Motherboard Revision Number        : A0
Model Number                       : C9300-24UX
System Serial Number               : FCW2136L0AK


Switch Ports Model              SW Version        SW Image              Mode
------ ----- -----              ----------        ----------            ----
*    1 38    C9300-24UX         16.6.4a           CAT9K_IOSXE           INSTALL
```

Parte 4: Actividad autónoma con DNA Center.

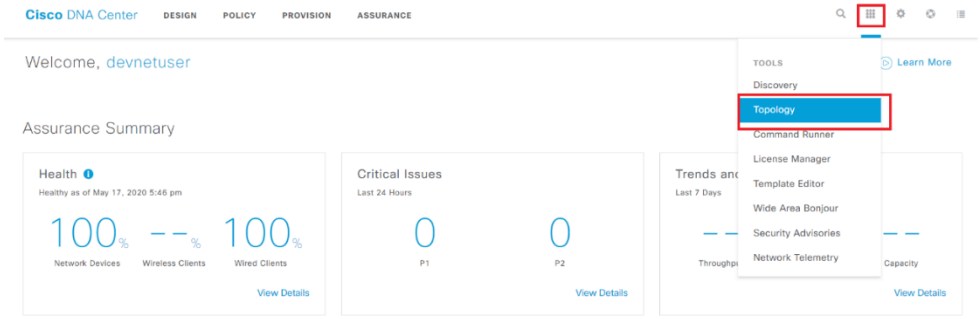
g) Ubique el router de borde “asr1001-x” y utilice CDP mediante CLI para visualizar los dispositivos conectados al router.
h) Verifique que los dispositivos conectados sean los mismos que se reflejan en la topología de red.
i) Realice un “Path Trace” desde el router “asr1001-x” hasta el puerto de conexión HTTPS en la dirección 10.10.22.98. Utilice el protocolo TCP.
j) ¿Por cuál VLAN se conecta al host 10.10.22.98?

Guía de solución de laboratorio - Introducción a DNA y sus componentes.

Parte 4 Resolución: Actividad autónoma con DNA Center.

k) Ubique el router de borde “asr1001-x” y utilice CDP mediante CLI para visualizar los dispositivos conectados al router.

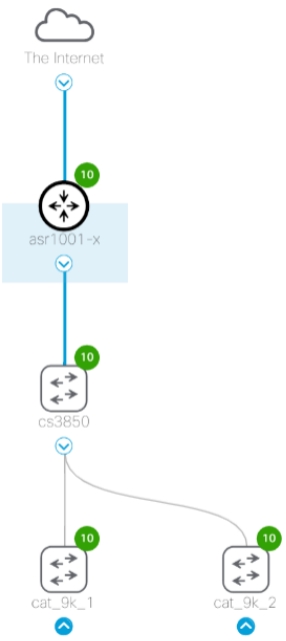
a. Seleccione “Tools” y posteriormente seleccione “Topology”.

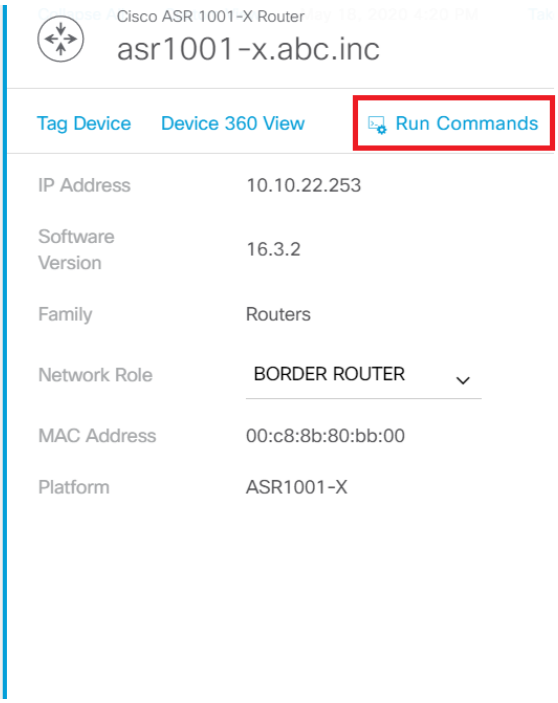


b. Seleccione “Global”.

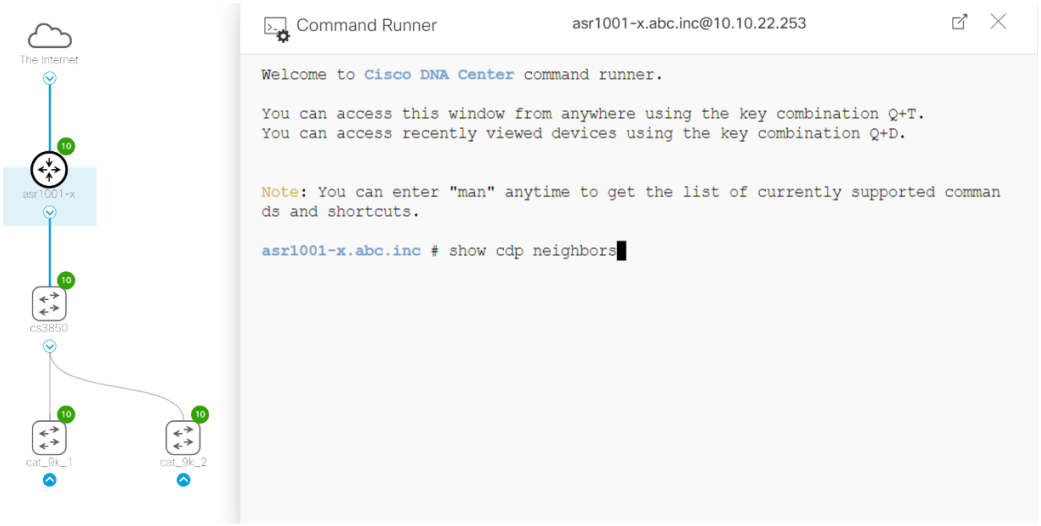
c. Haga clic en “asr1001-x”.

d. Seleccione “Run Commands”

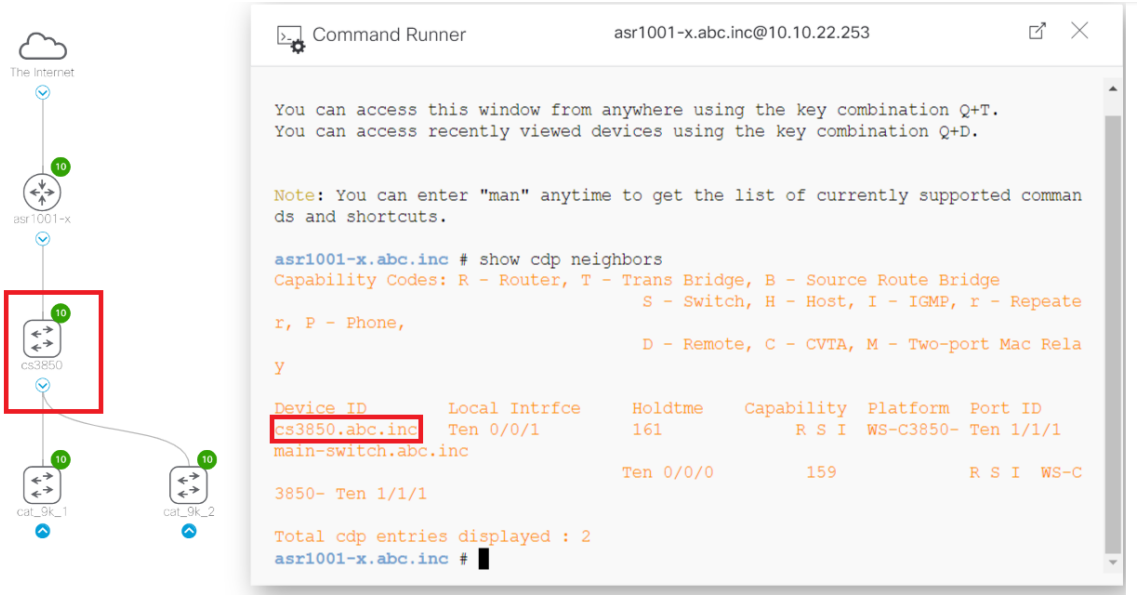




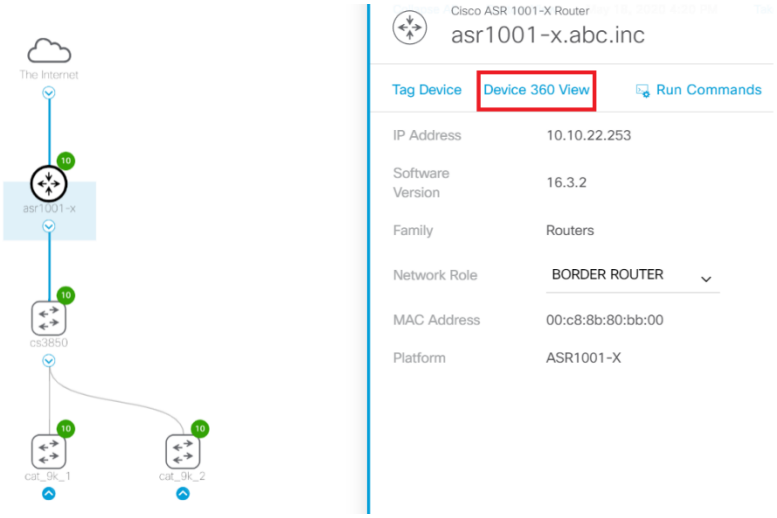
e. Ingrese “show cdp neighbors”



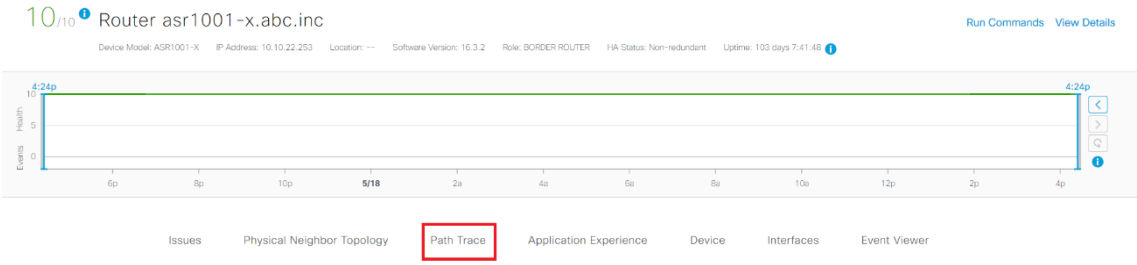
l) Verifique que los dispositivos conectados sean los mismos que se reflejan en la topología de red.



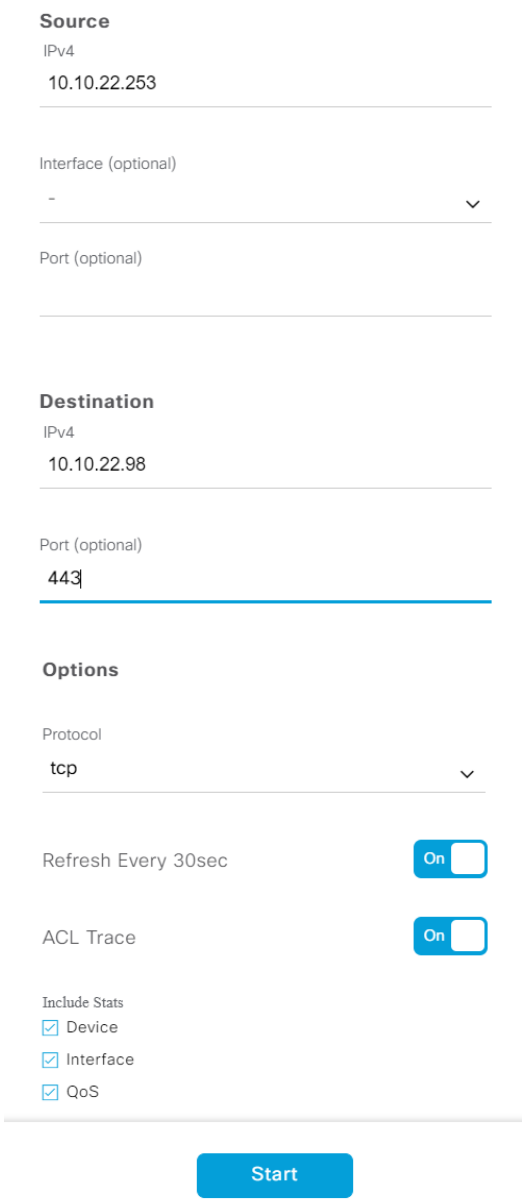
m) Realice un “Path Trace” desde el router “asr1001-x” hasta el puerto de conexión HTTPS en la dirección 10.10.22.98. Utilice el protocolo TCP.
   a. Seleccione la pestaña “Device 360 View”



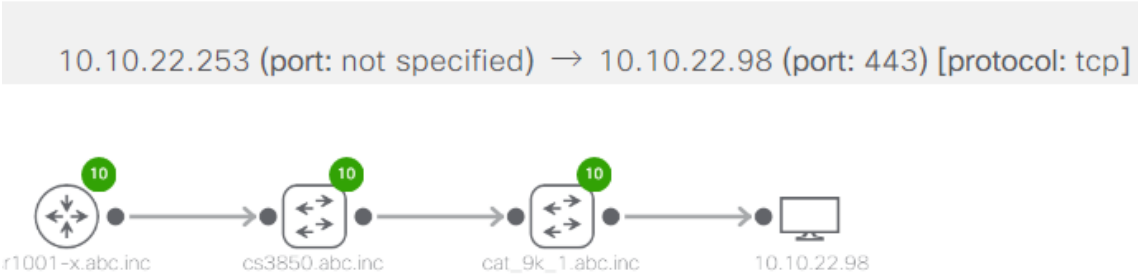
b. Haga clic en la pestaña “Path Trace”.



c. Seleccione “Run New Path Trace”
d. Ingrese los siguientes datos:

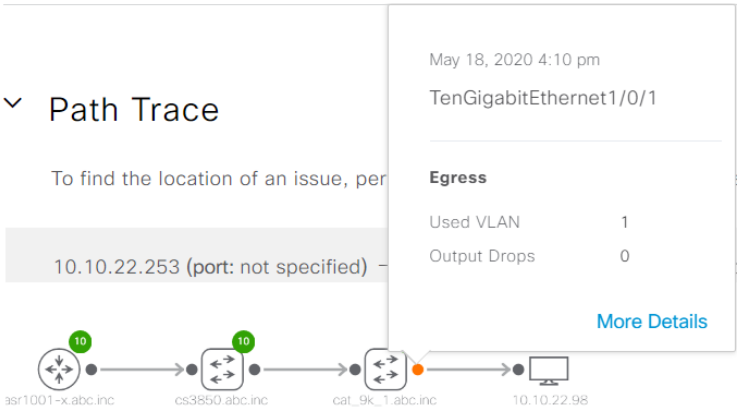


e. Verifique la conexión de toda la ruta.



n) ¿Por cuál VLAN se conecta al host 10.10.22.98?

a. Para visualizar los datos de conexión al host posicione el mouse sobre el puerto de conexión con el switch.



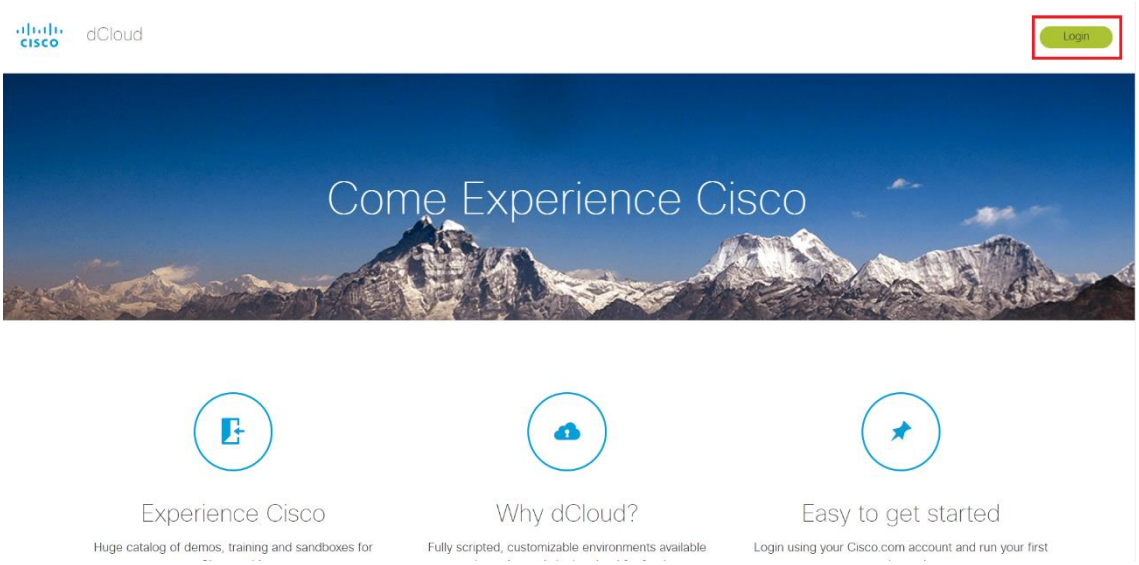
- **Respuesta: VLAN 1**

Guía de laboratorio – DNA y sus funcionalidades.

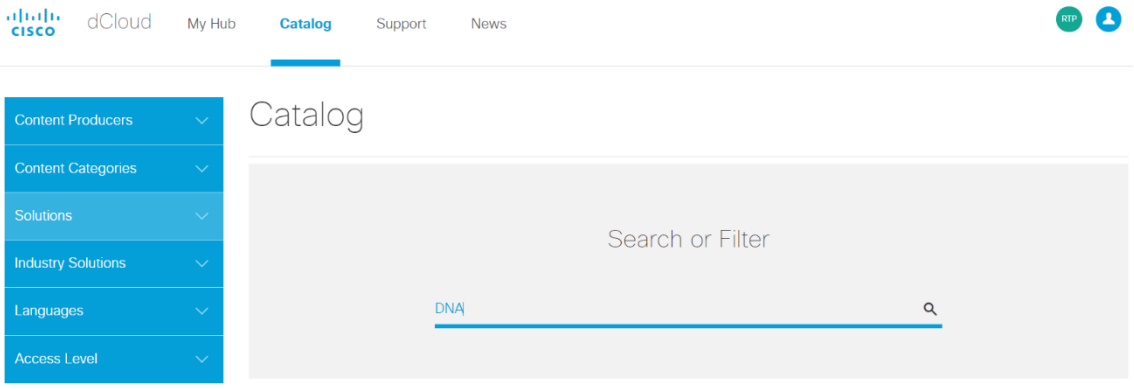
Prerrequisito: Guía de laboratorio - Introducción a DNA y sus componentes.

Parte 1: Ingreso a Laboratorio de DNA en DCloud.

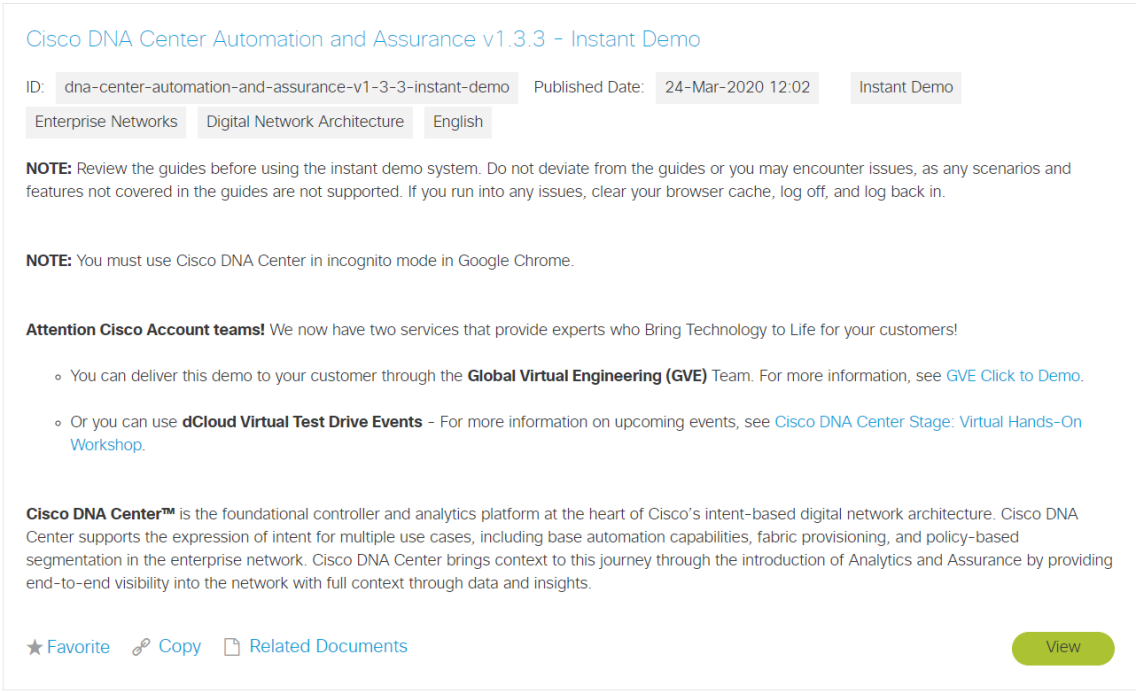
k) Ingrese al siguiente link https://dcloud.cisco.com/ mediante el navegador Google Chrome de incognito.
l) Seleccione “Login”.
m) Ingrese con las credenciales de la Universidad.



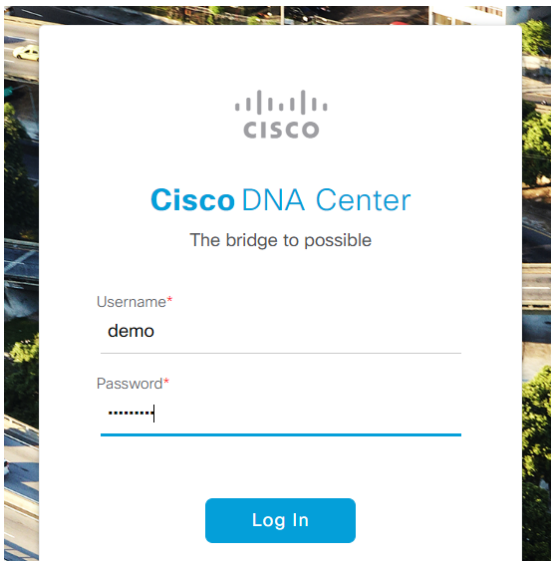
n) En la barra de búsqueda ingrese “DNA”.



o) Seleccione “View” para abrir el laboratorio “Cisco DNA Center Automation and Assurance v1.3.3”.

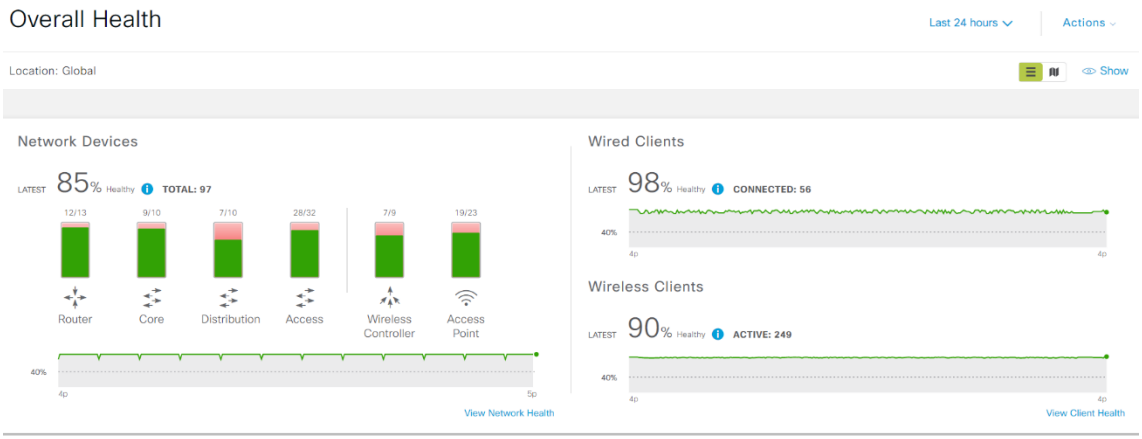


p) Ingrese las siguientes credenciales:
   a. Usuario: **demo**
   b. Contraseña: **demo1234!**



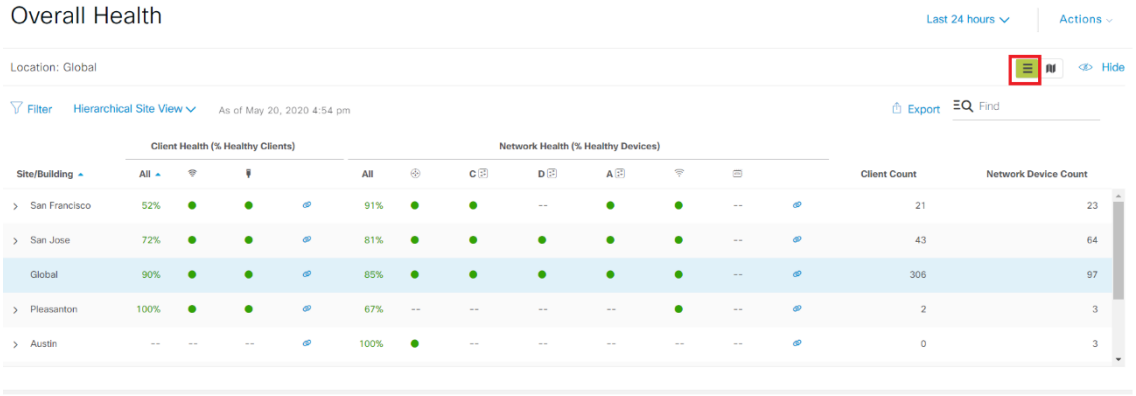
Parte 2: Exploración e identificación de problemas de red.

r) Seleccione la pestaña “Assurance”, posteriormente “Dashboards” > “Health” > “Overall Health”.



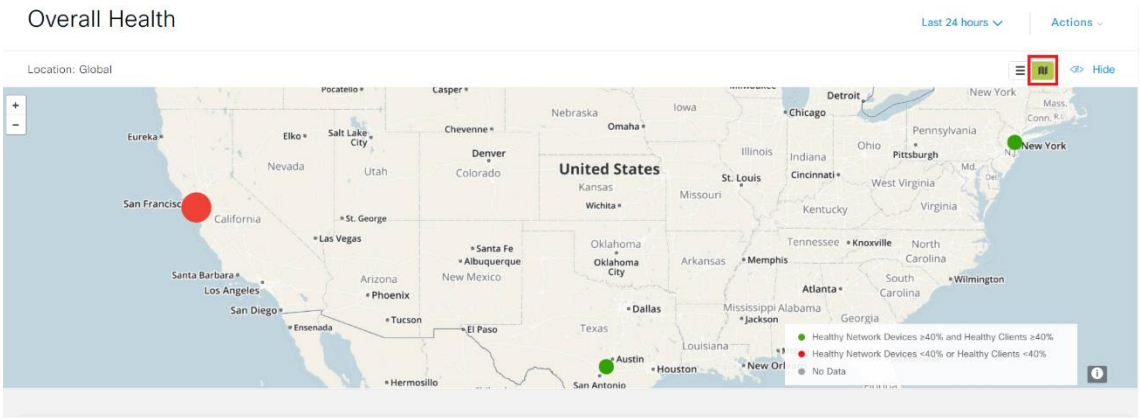
- **Nota:** En esta ventana se puede apreciar la salud o estado de todos los dispositivos de la red. Sean routers, switch, access points, etc.

s) Seleccione el botón “Hierarchical View”.



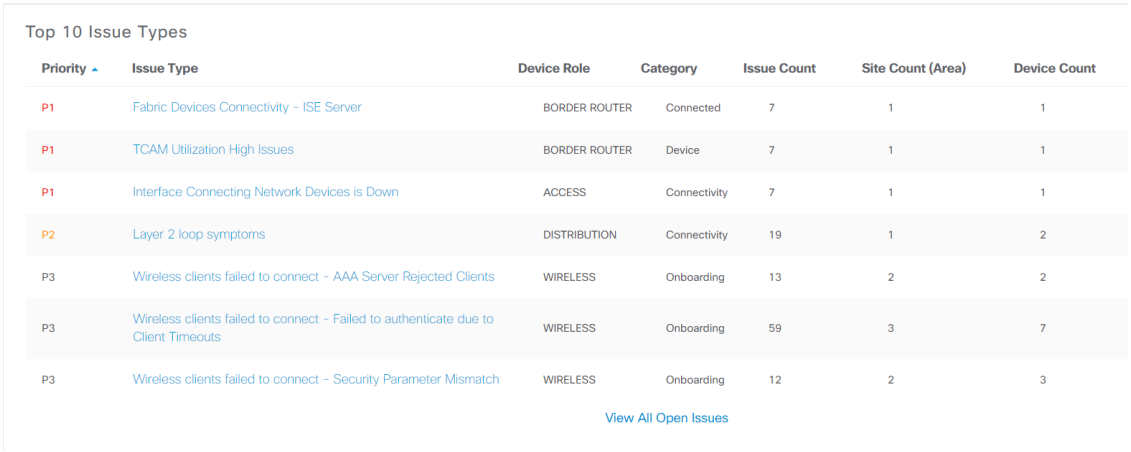
- **Nota:** En esta vista se puede apreciar el estado de la red por ubicación.

t) Seleccione “Map View”.



- **Nota:** En esta vista se puede apreciar las ubicaciones de las redes en un mapa. El punto rojo indica problemas en la red.

u) Desplace el mouse hacia la parte inferior para apreciar una tabla donde indica los 10 mayores problemas de la red.

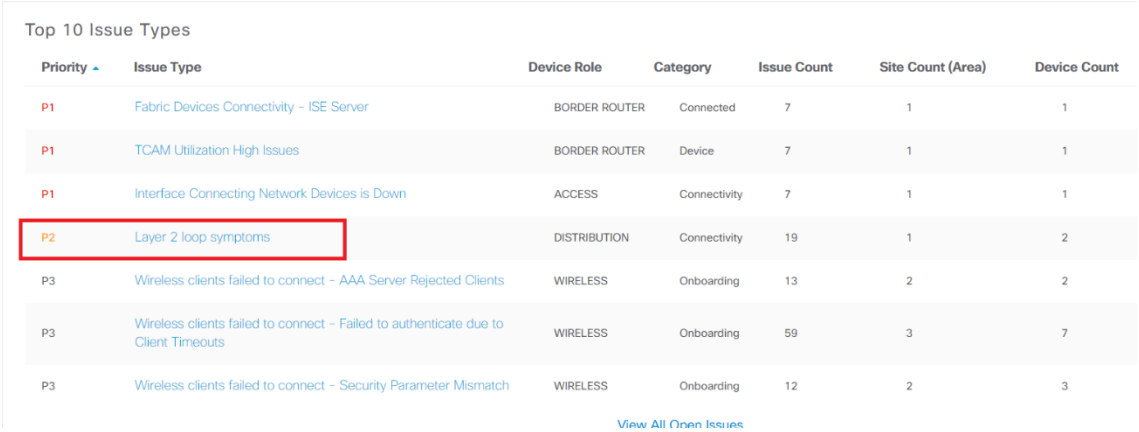


Top 10 Issue Types

Priority	Issue Type	Device Role	Category	Issue Count	Site Count (Area)	Device Count
P1	Fabric Devices Connectivity – ISE Server	BORDER ROUTER	Connected	7	1	1
P1	TCAM Utilization High Issues	BORDER ROUTER	Device	7	1	1
P1	Interface Connecting Network Devices is Down	ACCESS	Connectivity	7	1	1
P2	Layer 2 loop symptoms	DISTRIBUTION	Connectivity	19	1	2
P3	Wireless clients failed to connect – AAA Server Rejected Clients	WIRELESS	Onboarding	13	2	2
P3	Wireless clients failed to connect – Failed to authenticate due to Client Timeouts	WIRELESS	Onboarding	59	3	7
P3	Wireless clients failed to connect – Security Parameter Mismatch	WIRELESS	Onboarding	12	2	3

View All Open Issues

v) Seleccione el problema de “Loop de capa 2”.

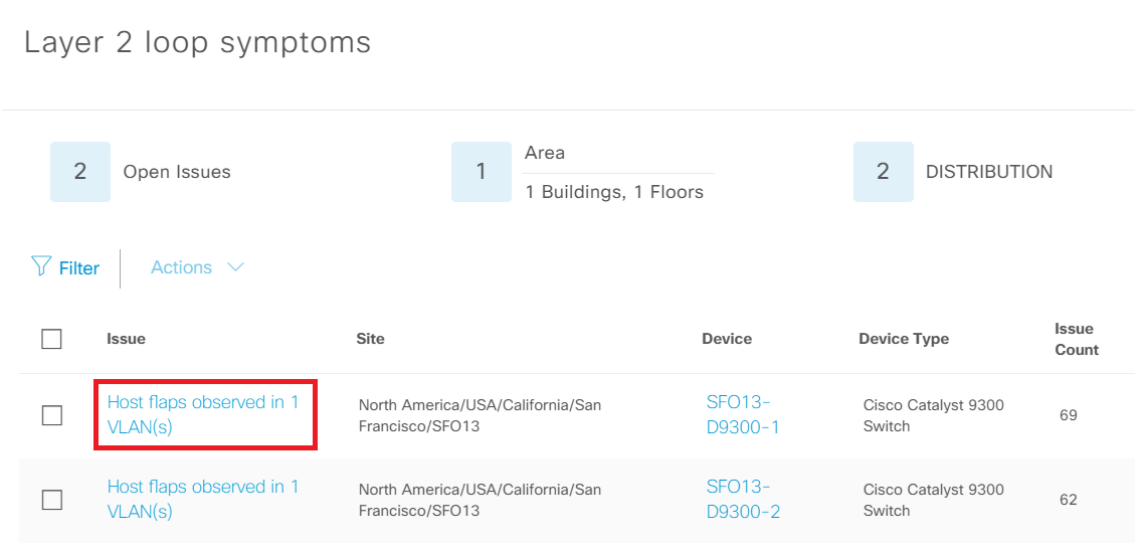


Top 10 Issue Types

Priority	Issue Type	Device Role	Category	Issue Count	Site Count (Area)	Device Count
P1	Fabric Devices Connectivity - ISE Server	BORDER ROUTER	Connected	7	1	1
P1	TCAM Utilization High Issues	BORDER ROUTER	Device	7	1	1
P1	Interface Connecting Network Devices is Down	ACCESS	Connectivity	7	1	1
P2	Layer 2 loop symptoms	DISTRIBUTION	Connectivity	19	1	2
P3	Wireless clients failed to connect - AAA Server Rejected Clients	WIRELESS	Onboarding	13	2	2
P3	Wireless clients failed to connect - Failed to authenticate due to Client Timeouts	WIRELESS	Onboarding	59	3	7
P3	Wireless clients failed to connect - Security Parameter Mismatch	WIRELESS	Onboarding	12	2	3

View All Open Issues

w) Seleccione la primera opción el siguiente recuadro.



Layer 2 loop symptoms

2 Open Issues

1 Area

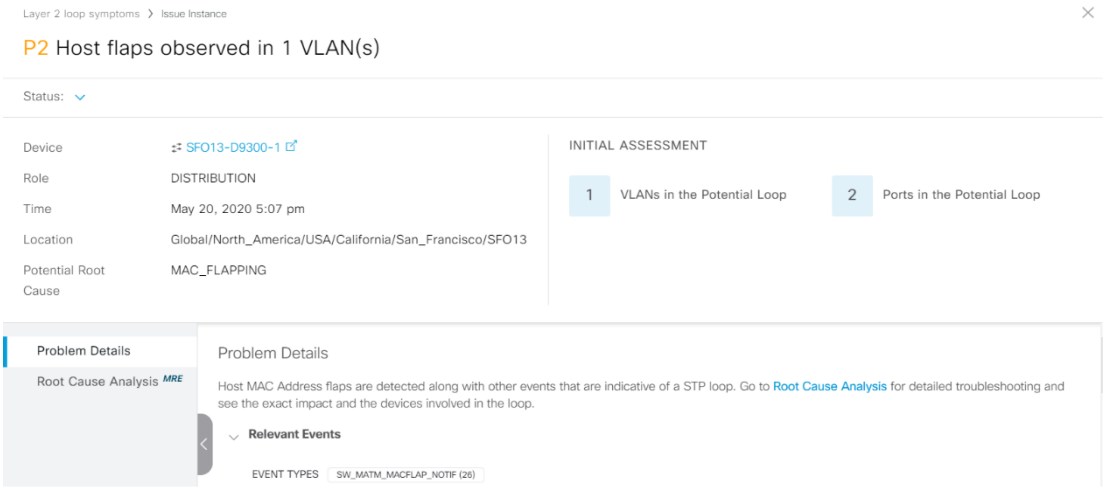
1 Buildings, 1 Floors

2 DISTRIBUTION

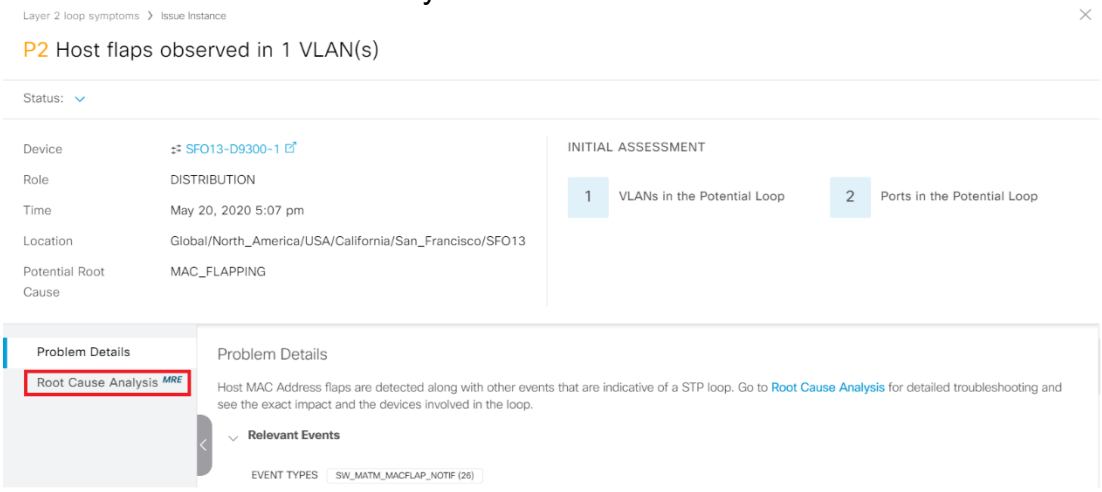
Filter | Actions

Issue	Site	Device	Device Type	Issue Count
Host flaps observed in 1 VLAN(s)	North America/USA/California/San Francisco/SFO13	SFO13-D9300-1	Cisco Catalyst 9300 Switch	69
Host flaps observed in 1 VLAN(s)	North America/USA/California/San Francisco/SFO13	SFO13-D9300-2	Cisco Catalyst 9300 Switch	62

x) En el siguiente recuerdo se detalla una breve descripción del problema que presenta el switch.

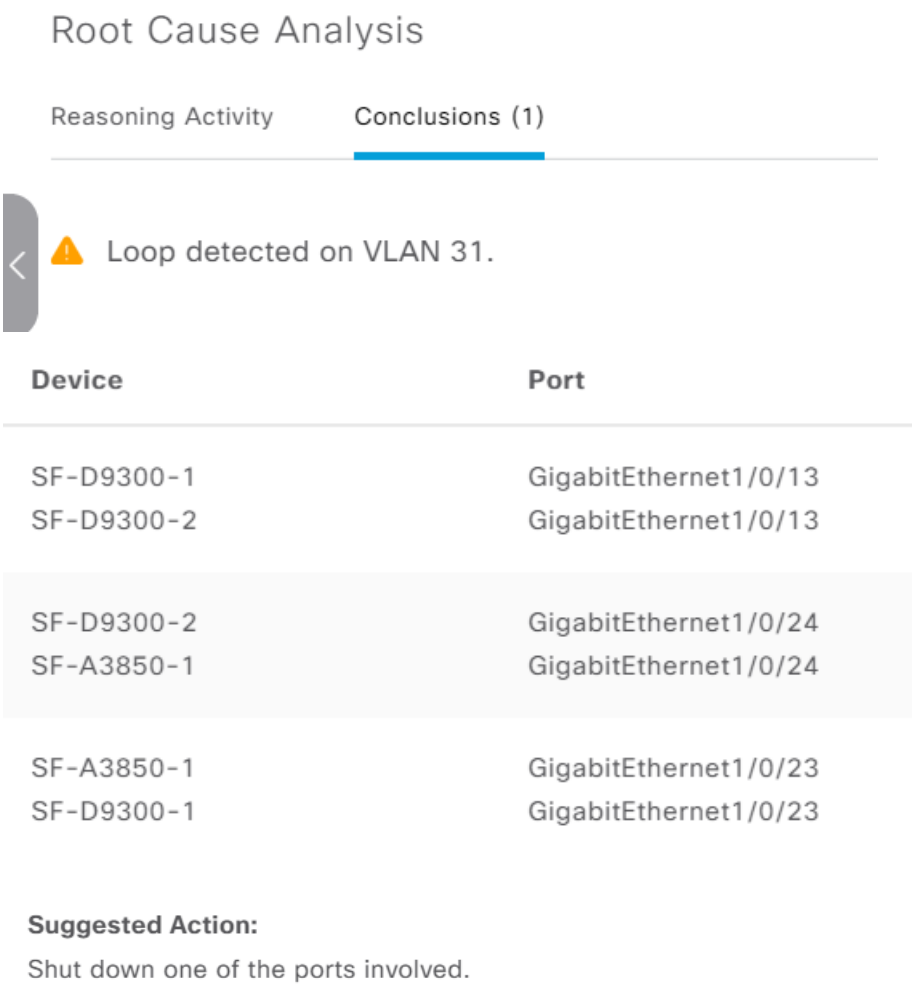


y) Seleccione “Root Cause Analysis”.



- **Nota:** Esta herramienta realiza un análisis rápido con inteligencia artificial y así ubicar de manera más rápida las posibles causas y soluciones a los problemas de red.

z) Seleccione “Run Machine Reasosing”.



- **Nota:** En “Tools” > “Topology” > “Global” se obtiene una Figura del diagrama de red de las conexiones de la red.

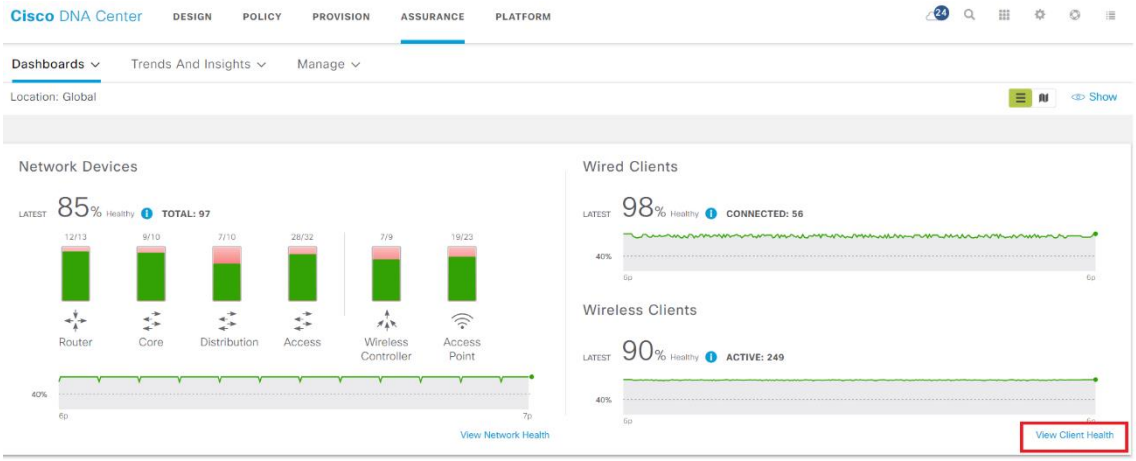
Parte 2.1: Preguntas sobre la actividad.

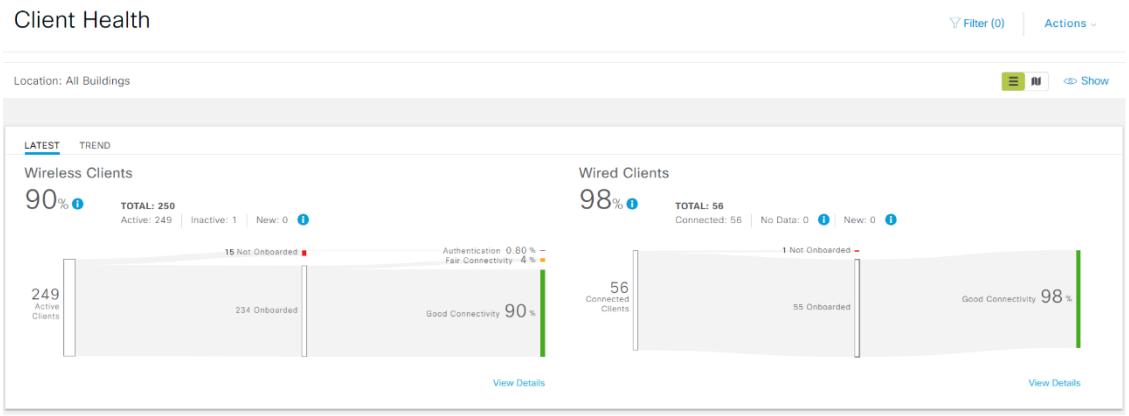
a) ¿Cuál es el problema que identifico DNA con “Root Cause Analysis”?
b) ¿Qué dispositivos son los que causan el lazo?
c) ¿Cuál es la solución al problema?

Parte 3: Exploración de una red inalámbrica en DNA.

a) Seleccione la pestaña “Assurance”, posteriormente “Dashboards” > “Health” > “Overall Health”.

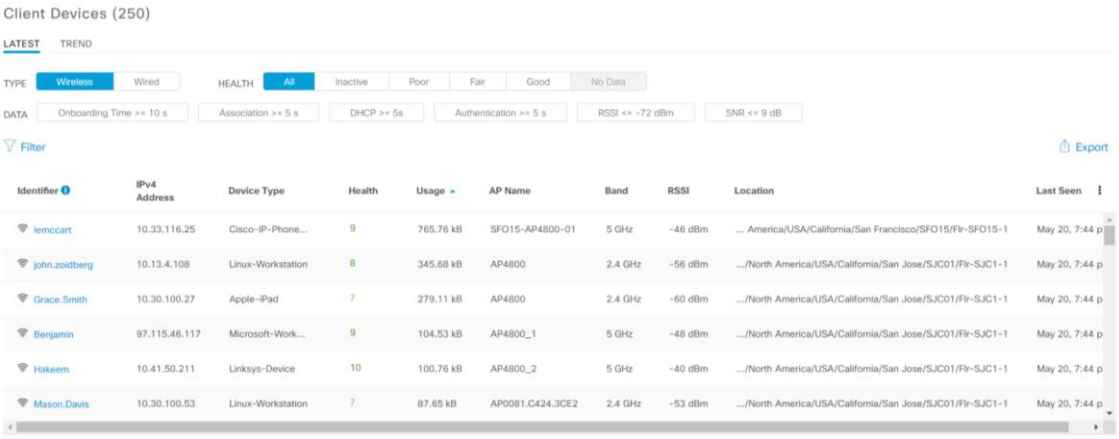
b) Seleccione “View Client Health”





- **Nota:** En estas graficas se pueden obtener datos tales como: usuarios conectados, porcentaje de conectividad, lugares con más clientes conectados, access points con más usuarios conectados, etc.

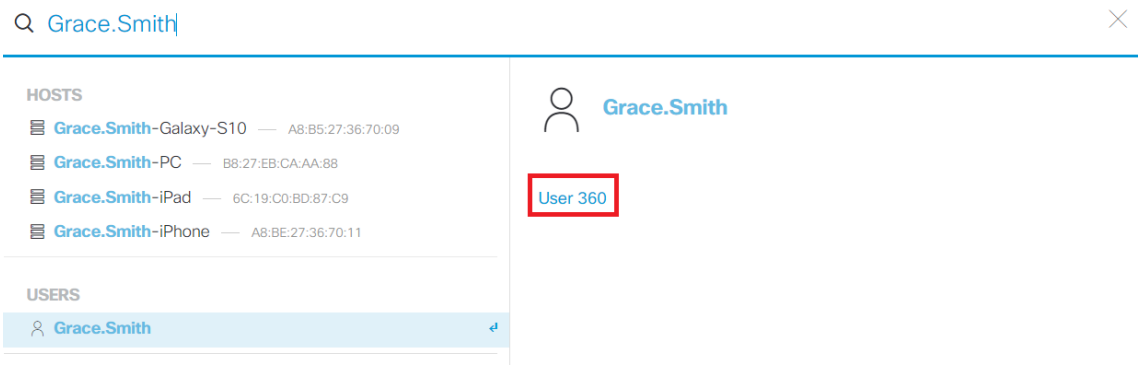
c) Desplace el mouse hacia la parte inferior para ver los dispositivos conectados a las redes inalámbricas.



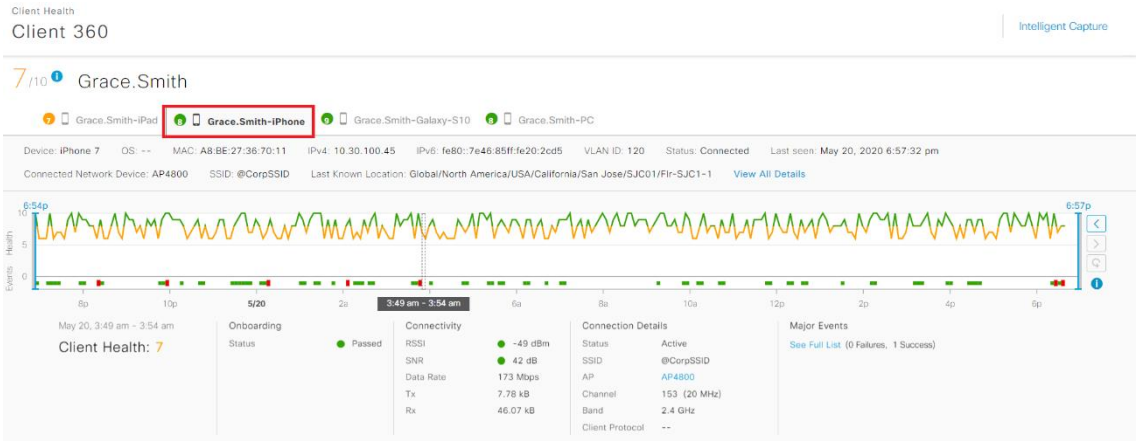
- **Nota:** Aquí se puede apreciar que dispositivos están conectados y a donde están conectados. Todos los datos que generar tales como: estado de salud, estado de señal, tipo de dispositivo, IP, etc.

d) Ingrese “Grace.Smith” en la barra de búsqueda.

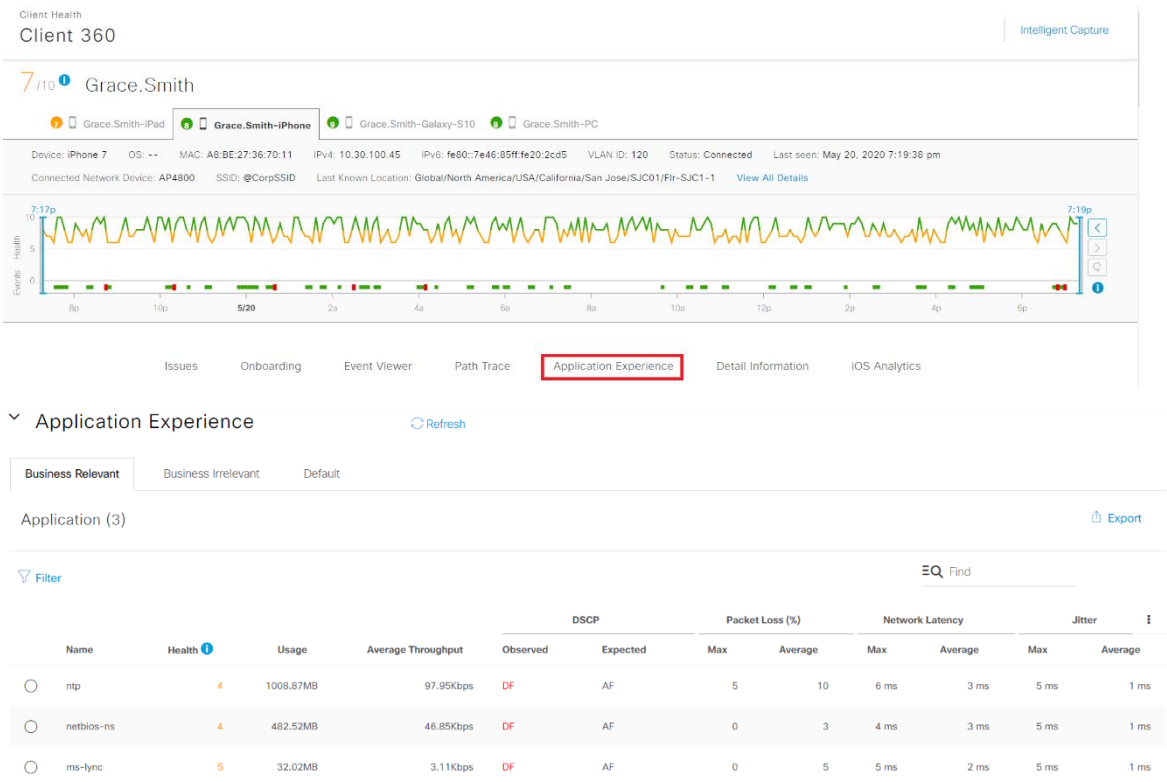
e) Seleccione “User 360”.



f) Seleccione la pestaña de “iPhone”.

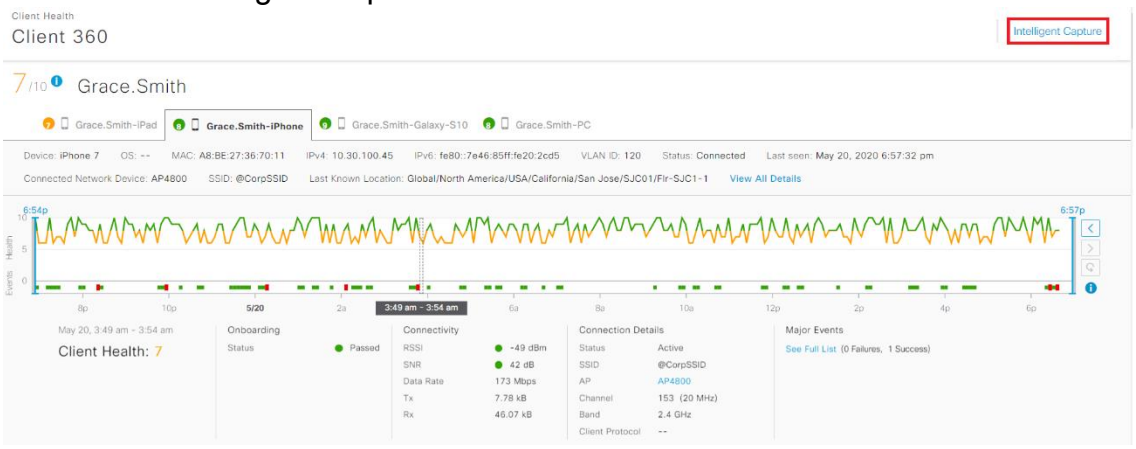


g) Seleccione “Application Experience”.



- **Nota:** En esta ventana se puede apreciar las aplicaciones utilizadas por el dispositivo, al igual que los datos que generan estas aplicaciones.

h) Seleccione “Intelligent Capture”.



- **Nota:** “Intelligent Capture” permite analizar los paquetes enviados por el dispositivo a la red. Permite la ubicación en tiempo real del dispositivo mediante el indicador de fuerza de la señal recibida (dBm).

Parte 4: Actividad autónoma con DNA Center.

o) Se necesita ubicar el iPad de Charles (Charles-iPad) y por motivos de auditoria se le solicita los siguientes datos:
   a. Dirección IP.
   b. AP al que se encuentra conectado.
   c. Banda de frecuencia.
   d. Indicador de fuerza de la señal recibida o RSSI (dBm).
   e. Ubicación geográfica.

p) Busque el computador de Roger (Roger-PC) e indique que aplicaciones se encuentra usando.

q) El administrador de red solicita a su persona un reporte de la aplicación más utilizada dentro de la red, esta aplicación debe constar en el ámbito de “Relevante para el negocio”. Los datos solicitados son:
   a. Nombre de la aplicación.
   b. Uso.
   c. Latencia de conexión.

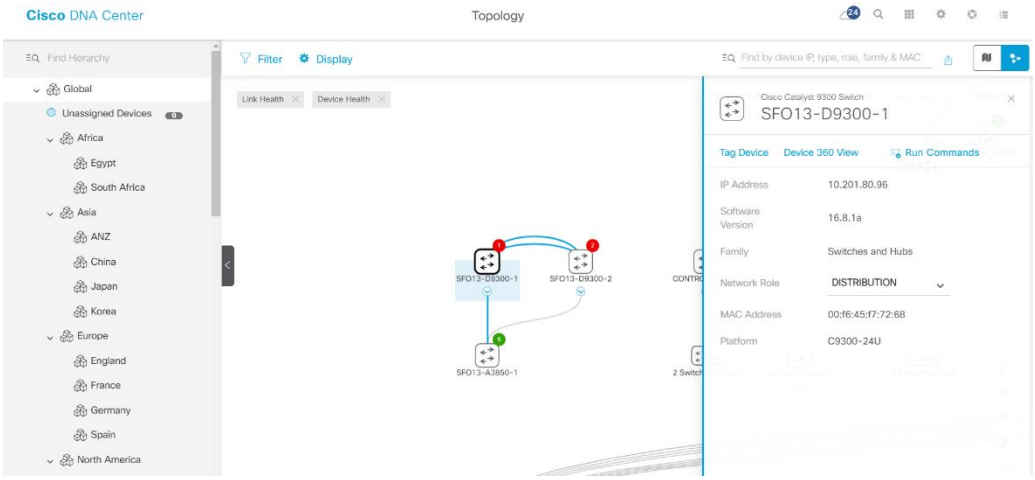
Nota: Para la última actividad los datos a buscar se pueden obtener en “Assurance” > “Dashboards” > “Health” > “Application Health”.

Guía de solución de laboratorio - DNA y sus funcionalidades.

Parte 2.1 Resolución: Preguntas sobre la actividad.

d) ¿Cuál es el problema que identifico DNA con “Root Cause Analysis”?
   - Hay un loop en la VLAN 31 el cual causa un Host MAC flap.

e) ¿Qué dispositivos son los que causan el lazo?
   - Seleccione “Tools” > “Topology” > “Global”.
   - En la barra de búsqueda ingrese uno de los dispositivos. Por ejemplo: “SFO13-D9300-1”



- Respuesta: Los dispositivos que causan el lazo son “SFO13-D9300-1” y “SFO13-D9300-2”

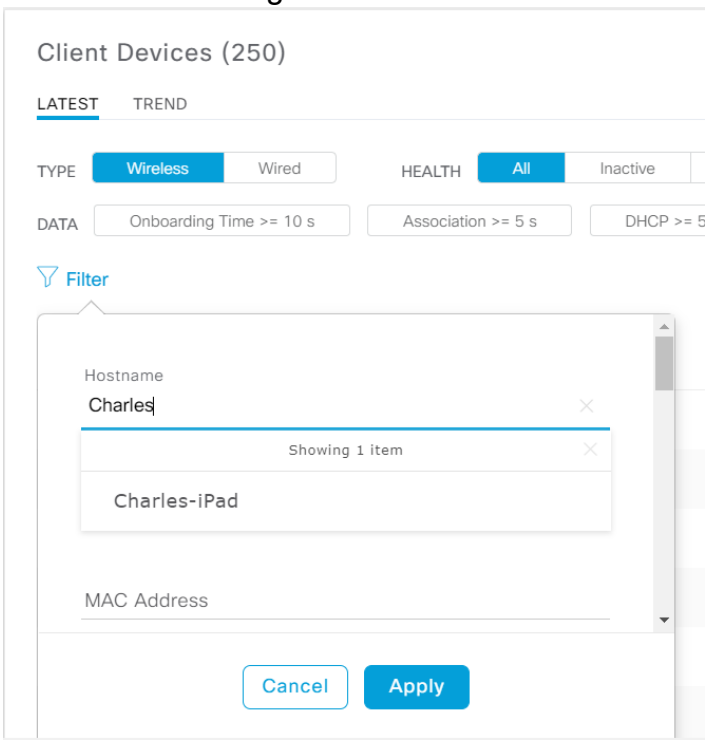
f) ¿Cuál es la solución al problema?

- Apagar uno de los puertos.

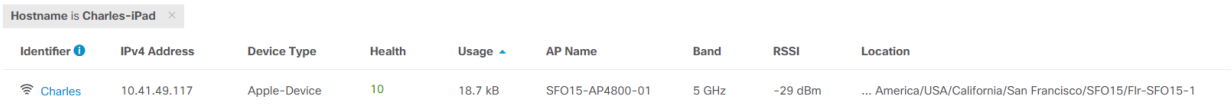
Parte 4 Resolución: Actividad autónoma con DNA Center.

r) Se necesita ubicar el iPad de Charles (Charles-iPad) y por motivos de auditoria se le solicita los siguientes datos:

I. Seleccione “Assurance” > “Dashboards” > “Health” > “Client Health”.
II. Desplace el mouse hasta la tabla de “Client Devices”.
III. Seleccione “Filter”.
IV. En “Hostname” ingrese “Charles-iPad”.

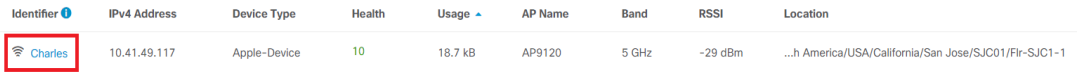


V. Seleccione “Apply”.



a. Dirección IP: **10.41.49.117**
b. AP al que se encuentra conectado: **SFO15-AP4800-01**
c. Banda de frecuencia: **5 GHz**
d. Indicador de fuerza de la señal recibida o RSSI (dBm): **-29 dBm**

VI. Seleccione el identificador “Charles”.



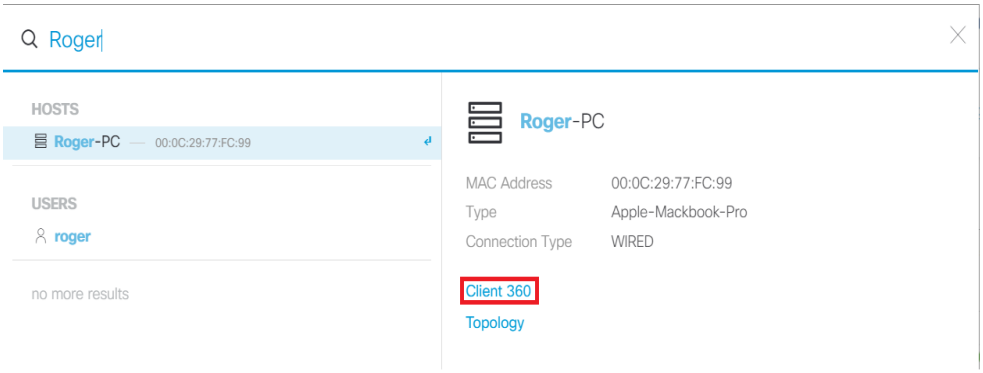
VII. Seleccione “Intelligent Capture” en la parte superior derecha.

e. Ubicación geográfica: **San Jose/SJC01**

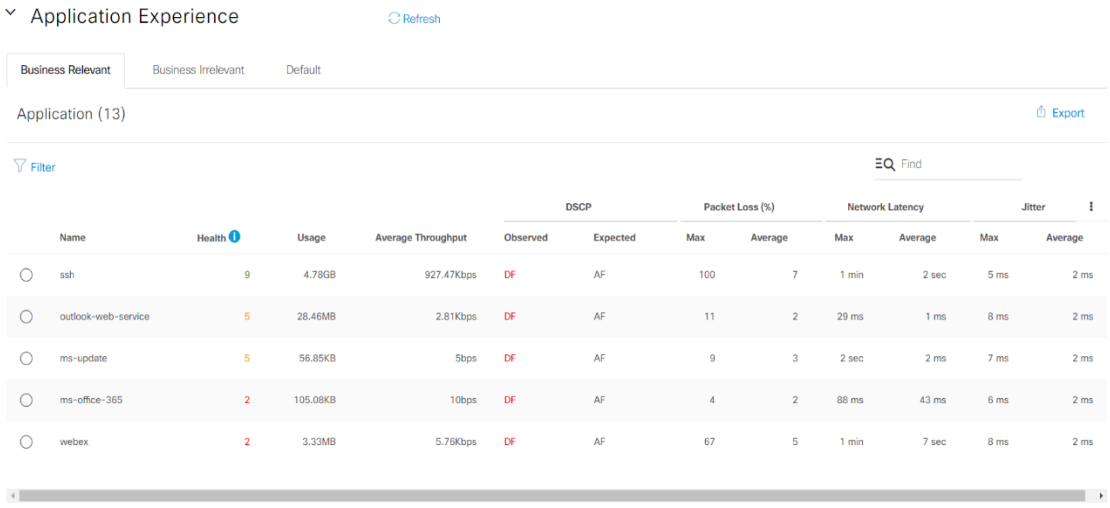
s) Busque el computador de Roger (Roger-PC) e indique que aplicaciones se encuentra usando.

I. En búsqueda (ubicada en la parte superior derecha).

II. Ingrese “Roger-PC”.
III. Seleccione “Client 360”



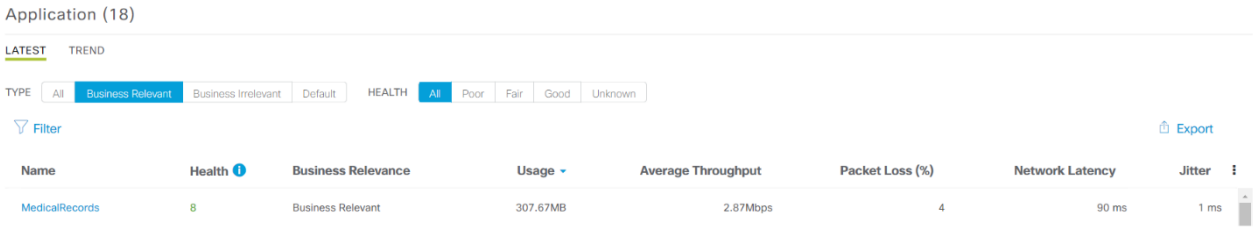
IV. Desplace el mouse hasta la tabla de “Application Experience”



a. Respuesta: **SSH, Outlook, ms-update, ms-office-365, Webex**.

t) El administrador de red solicita a su persona un reporte de la aplicación más utilizada dentro de la red, esta aplicación debe constar en el ámbito de “Relevante para el negocio”. Los datos solicitados son:

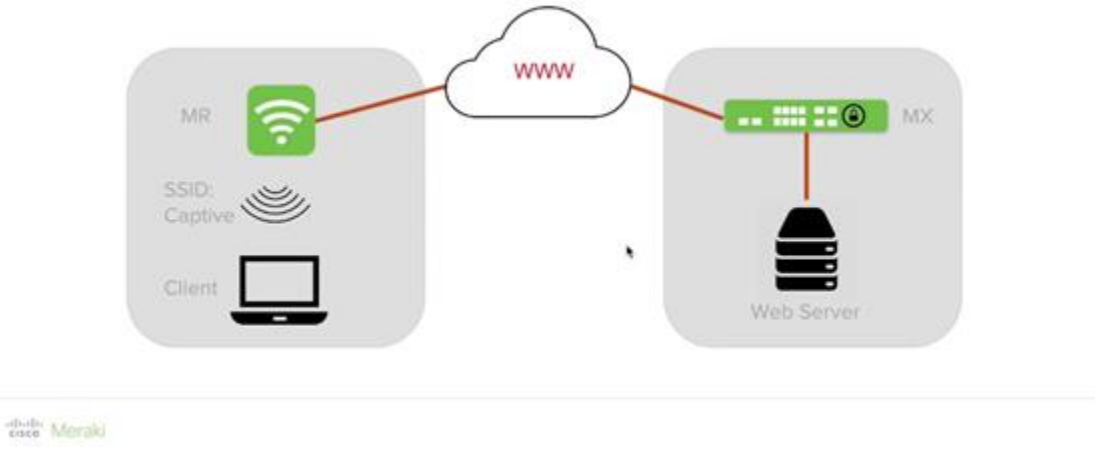
I. Seleccione “Assurance” > “Dashboards” > “Health” > “Application Health”.
II. Desplace el mouse hasta la tabla de “Application”



a. Nombre de la aplicación: **MedicalRecords.**
b. Uso: **307.67 MB.**
c. Latencia de conexión: **90 ms.**

Guía de laboratorio – Portal Cautivo con Meraki y API.

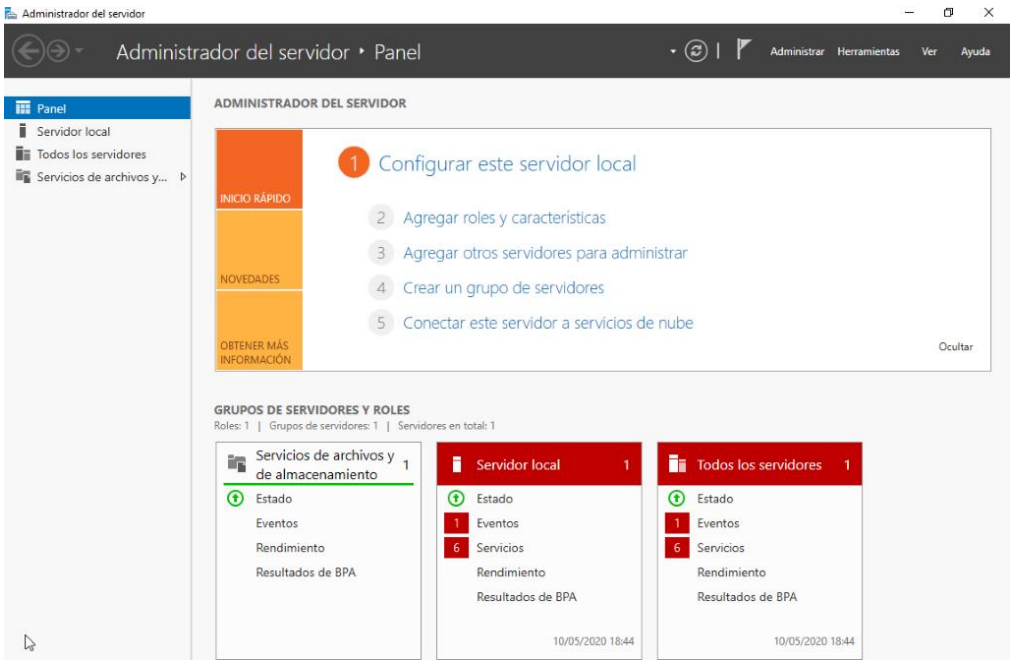
En el diseño de la red se usa los dispositivos Meraki: MX como router para la configuración y MR como Punto de Acceso (AP) para distribuir la red. Ambos equipos pueden estar configurados en un misma LAN, pero aprovechando las ventajas de Meraki van a estar conectados vía WAN y por una IP pública.



Parte 1: Levantar una máquina virtual

Como prerrequisitos se debe tener instalado un virtualizador y una imagen de Windows Server.

a) Dar clic en el virtualizador y montar la imagen de Windows Server.
b) Configurar la interfaz de internet y colocar en modo puente (bridge) para usar el mismo segmento de red local.
c) Correr la máquina virtual e instalar la imagen.

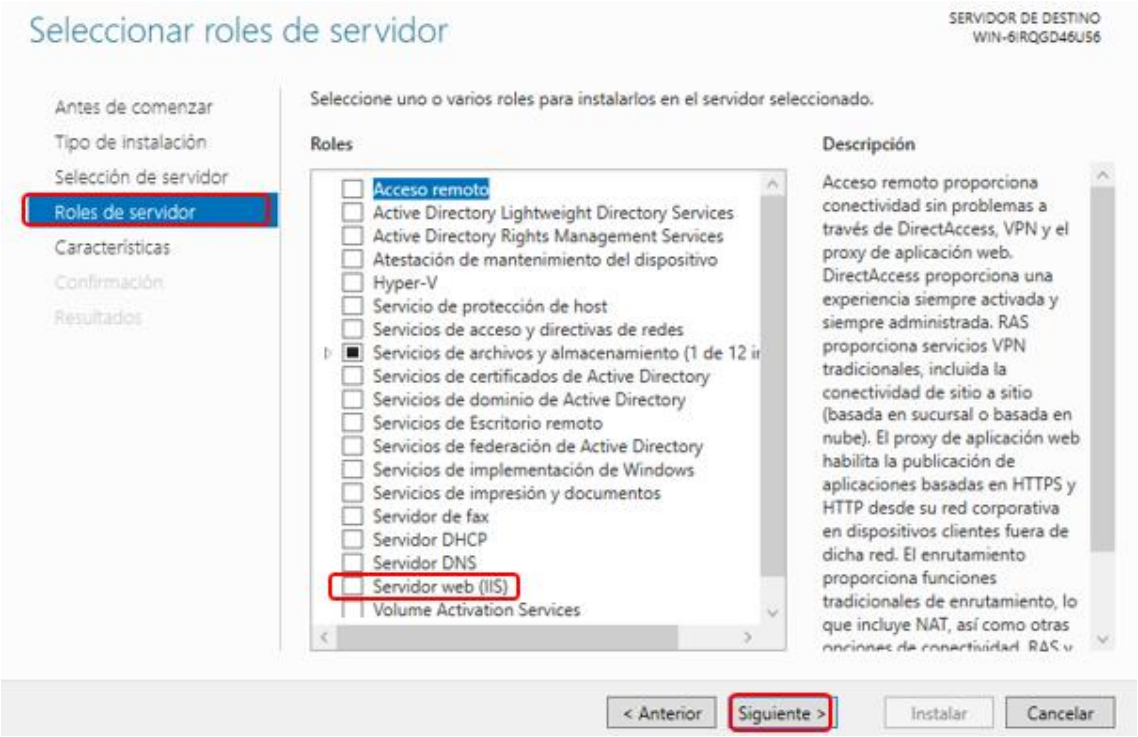


Parte 2: Levantar un web server y el servicio IIS

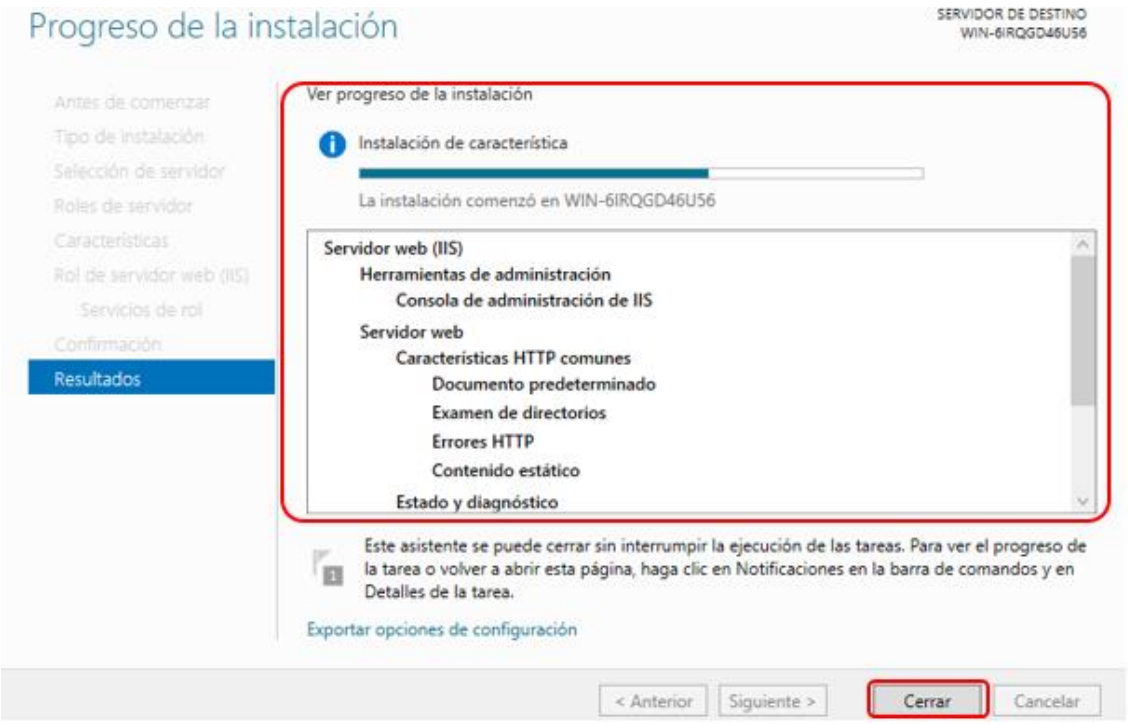
Con la maquina corriendo procedemos a levantar el servicio IIS de Windows

a) Se da clic en Administrar, luego en Agregar roles y características; o en la guía de inicio rápido.

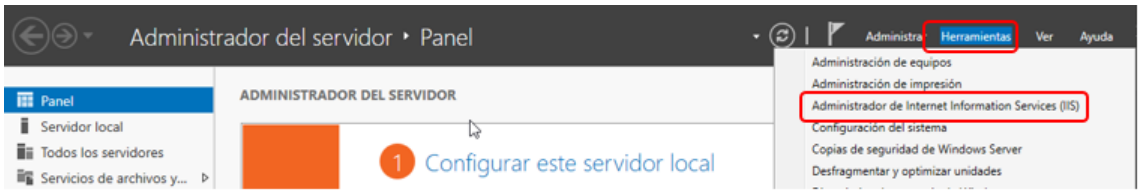
b) Continuando con el proceso se llega a Roles del servidor y se selecciona la casilla Servidor web (IIS) y finaliza con el clic en Siguiente.



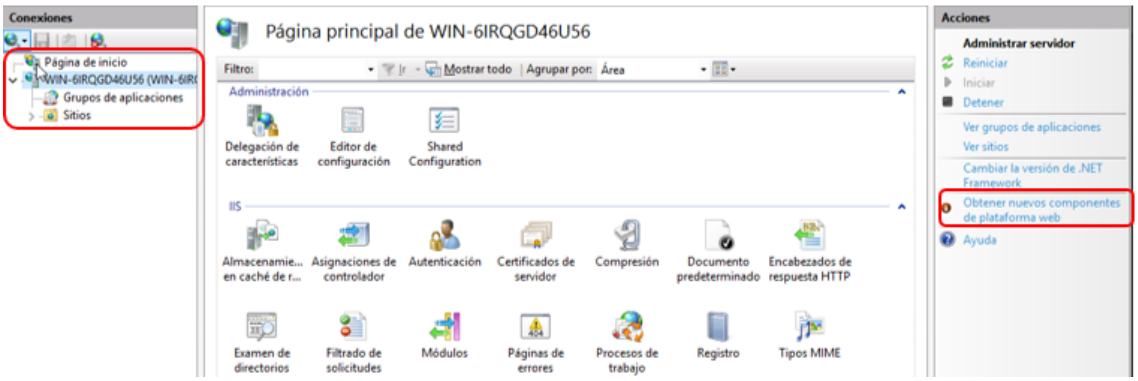
c) Se prosigue el proceso de instalación con Siguiente hasta dar clic en instalar y con el paso de unos minutos se termina de completar esta acción.



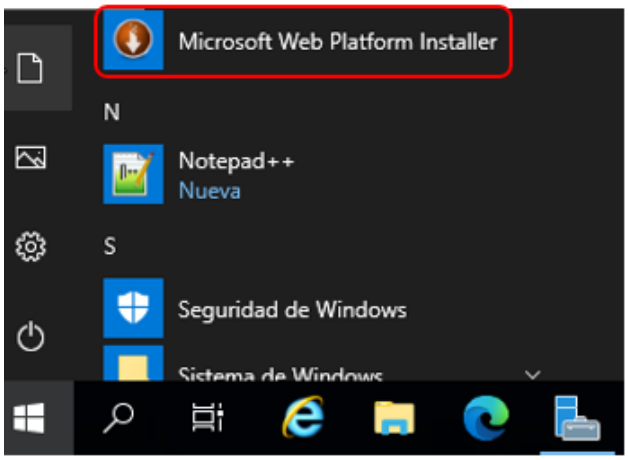
d) Una vez finalizado, se da clic en “Herramientas” y después en “Administración de Internet Information Services (IIS)”.



e) Se ingresa al web server y se da clic en “Obtener nuevos componentes de plataforma web”.



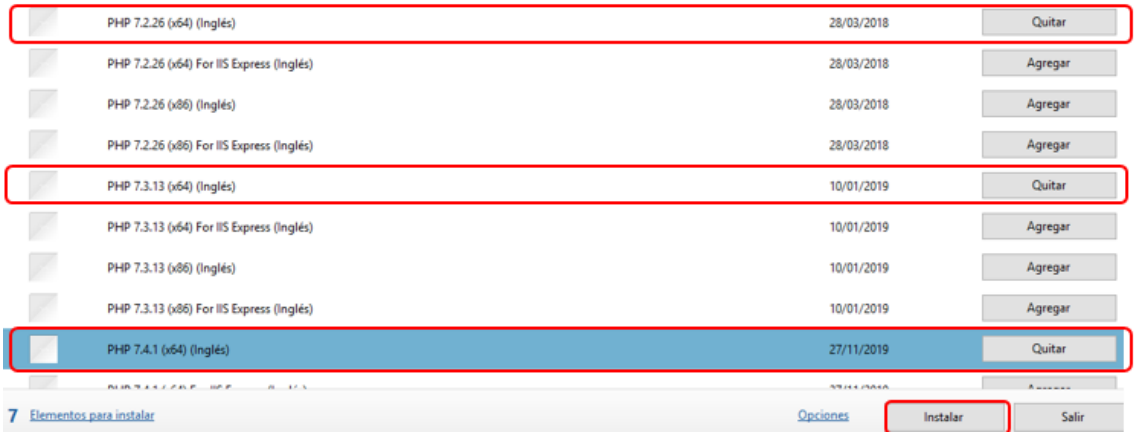
f) Se descarga y procedemos con la instalación del archivo de complementos para el web server. Una vez finalizado se encuentra en el menú Inicio y se da clic en “Microsoft Web Plataform Installer”.



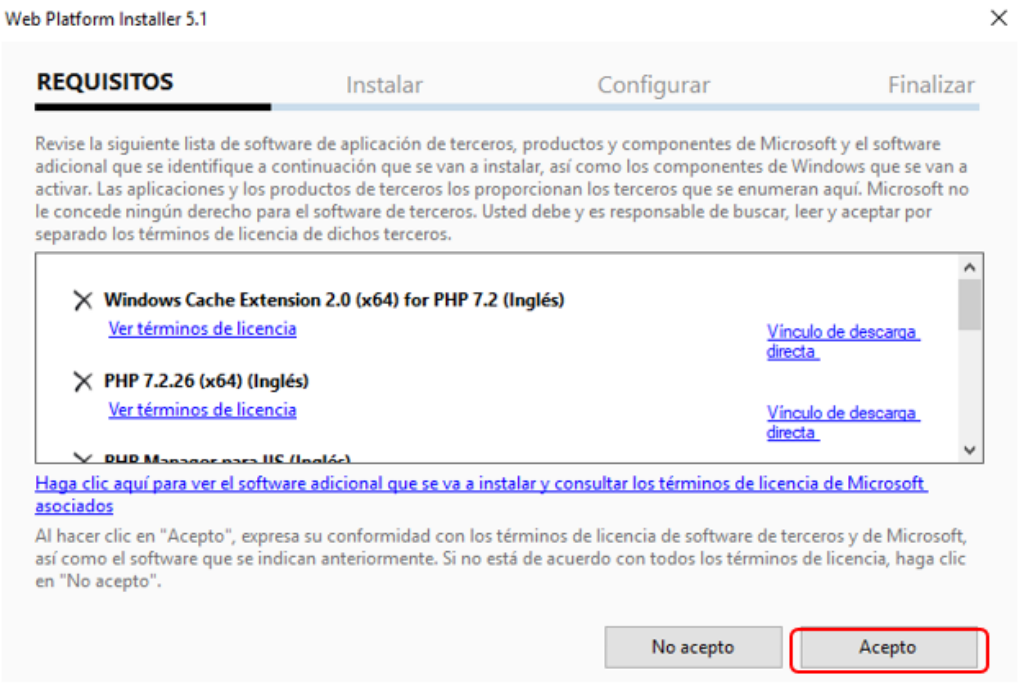
Parte 3: Instalar complementos PHP

a) Ejecutamos el “Web Platform”, clic en Productos y se busca “PHP”.

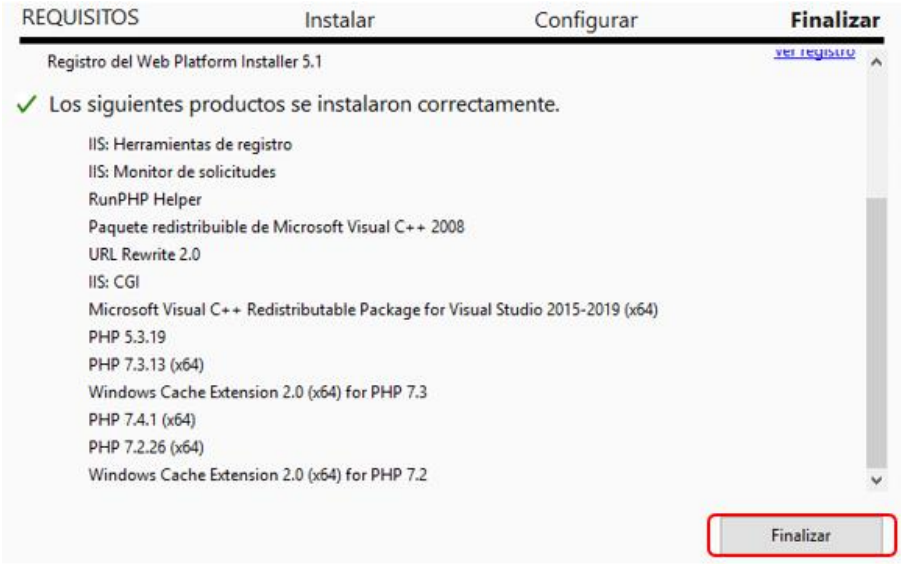
b) Se selecciona las opciones en base a los requerimientos si es de x86 o x64. Y se da clic en Agregar las versiones 7.2.x en adelante.



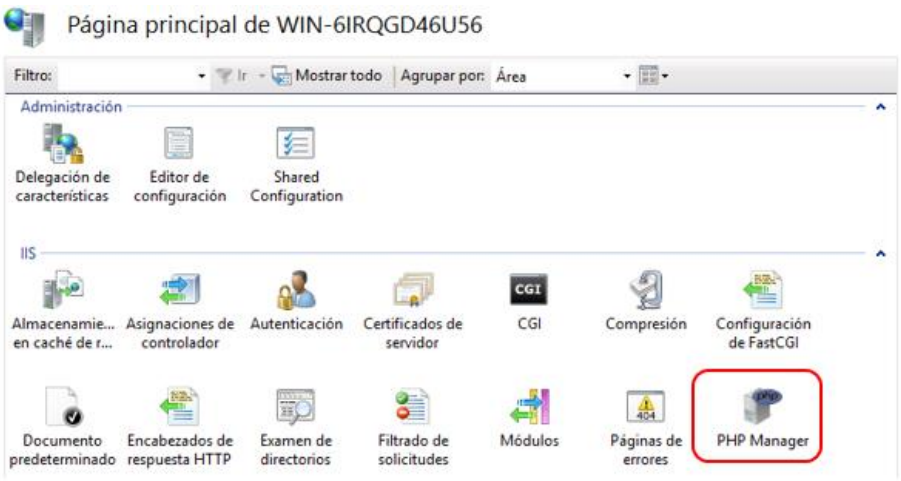
c) En la siguiente ventana, clic en Aceptar y se continua el proceso de instalación.



d) Se concluye el proceso y muestra el resultado de los paquetes instalados para concluir clic en Finalizar

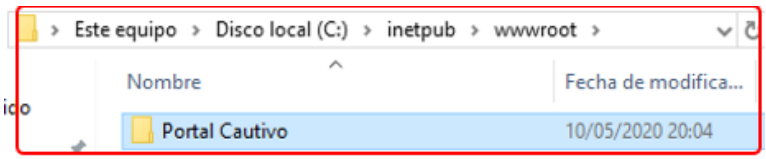


e) Al actualizar la página de administración de IIS se muestra arriba el en funcionamiento de PHP.

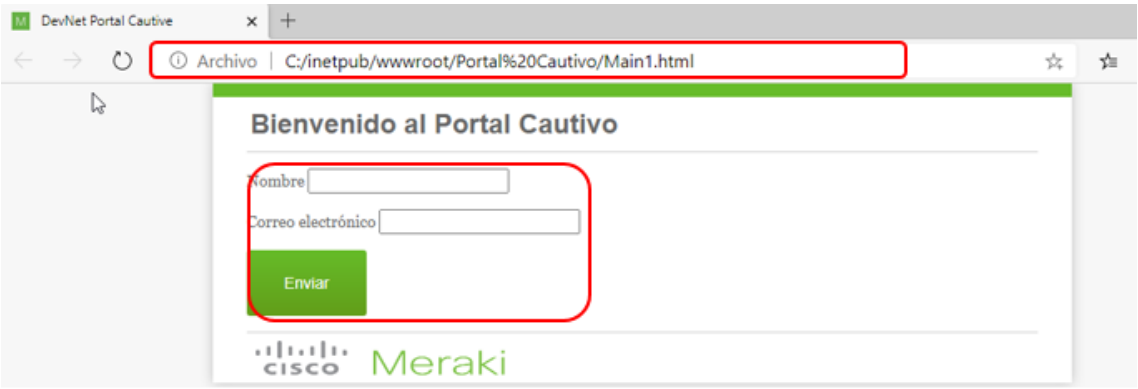


Parte 4: Crear una página en HTML y PHP

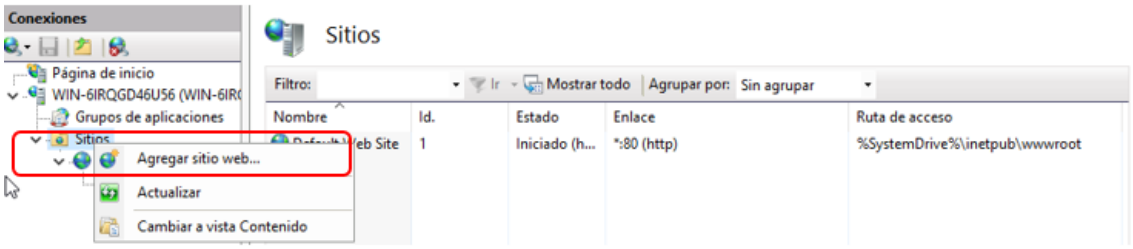
a) En la siguiente ruta del servidor C:\inetpub\wwwroot, se crea una carpeta llamada Portal Cautivo.



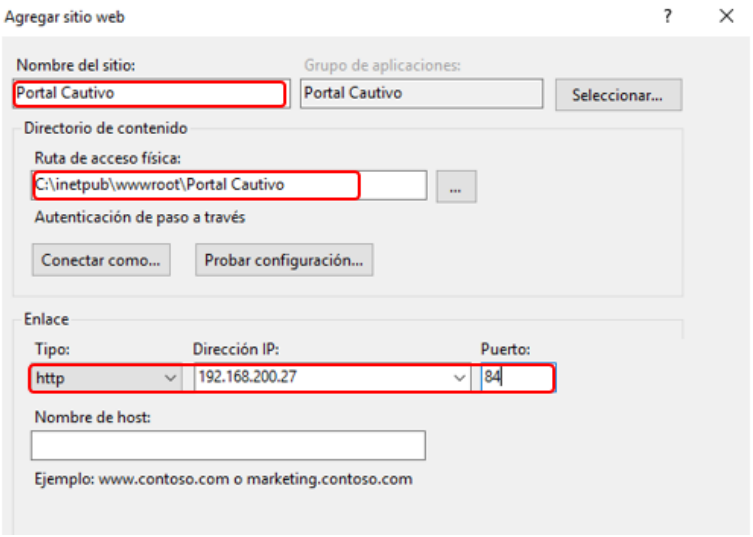
b) En esta carpeta se debe tener el código en HTML que sirve para el formato de la página web. Esto se puede hacer en cualquier editor de código o bloc de notas y se guarda con la extensión ".html". Una vez finalizado la página debe presentar dos entradas de texto y un botón para almacenar los datos.



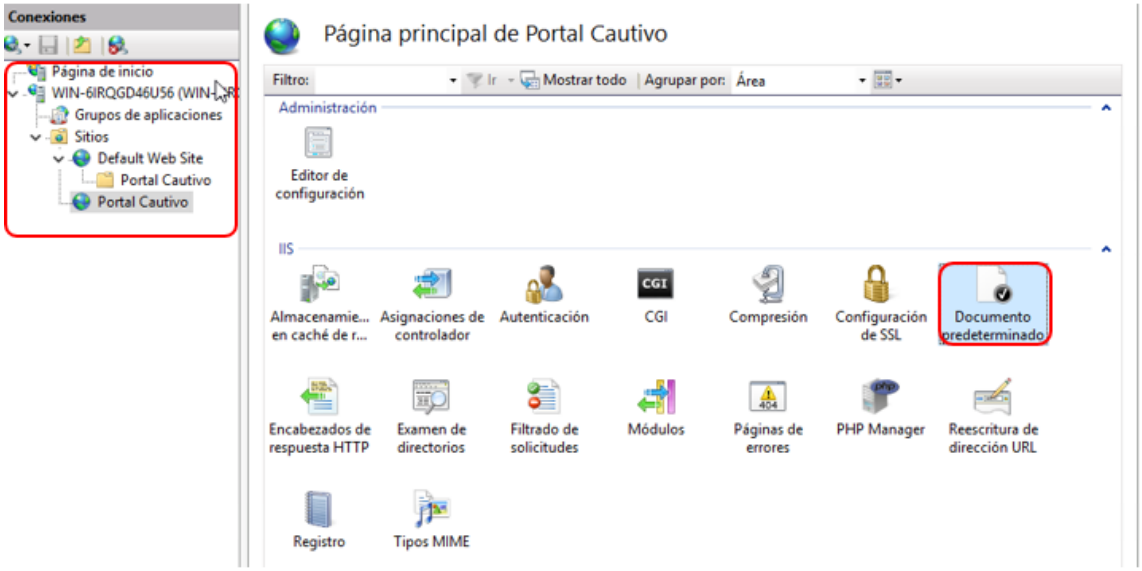
c) Ahora se debe levantar la página web con su respectivo script para lo cual, en el Administrador de IIS se agrega un nuevo sitio.



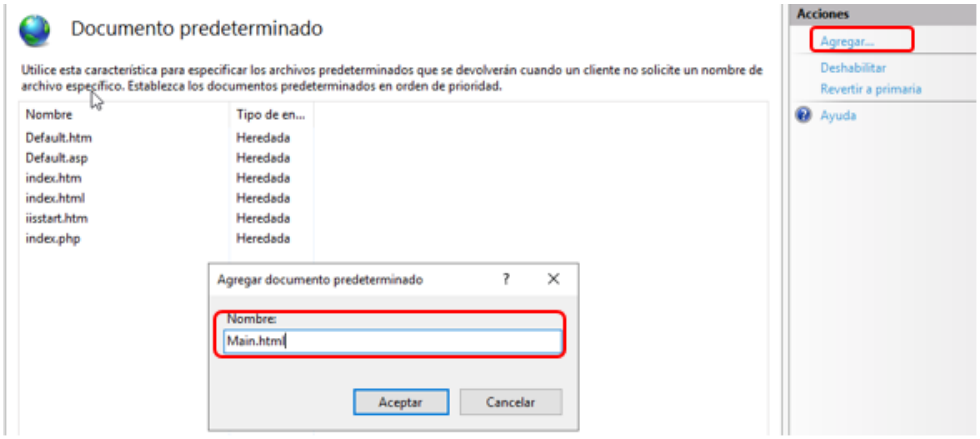
d) Se ingresa la información para poder levantar el servidor.



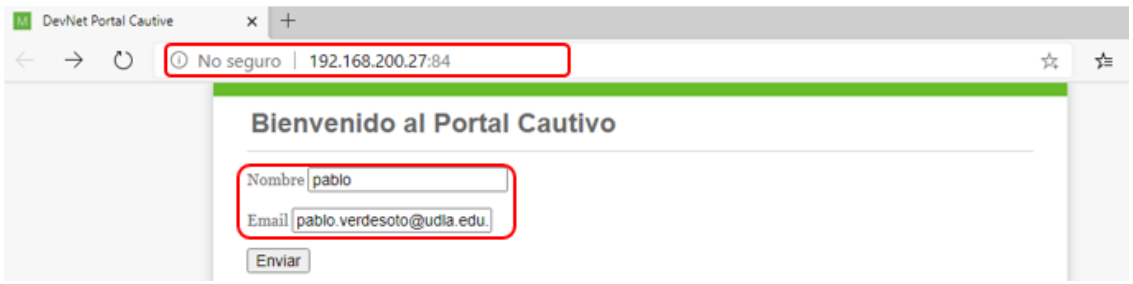
e) Clic en “Documento predeterminado” para agregar una nueva dirección por defecto que en este caso será “Main.html”.



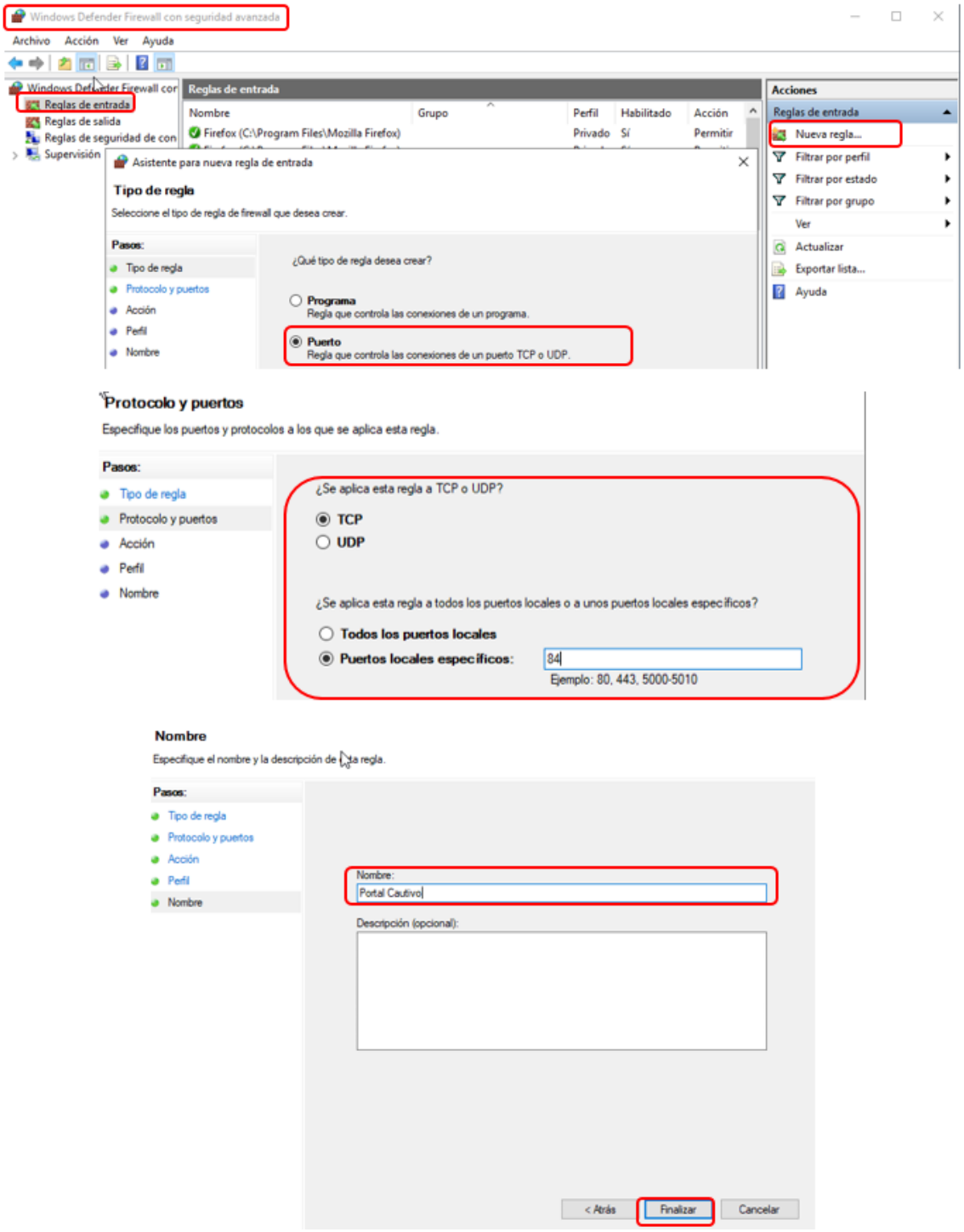
f) Clic en Agregar y escribimos la página de inicio y procedemos a probar con la IP local.



g) En un navegador con la dirección IP local y el puerto, se genera nuestro portal Cautivo.

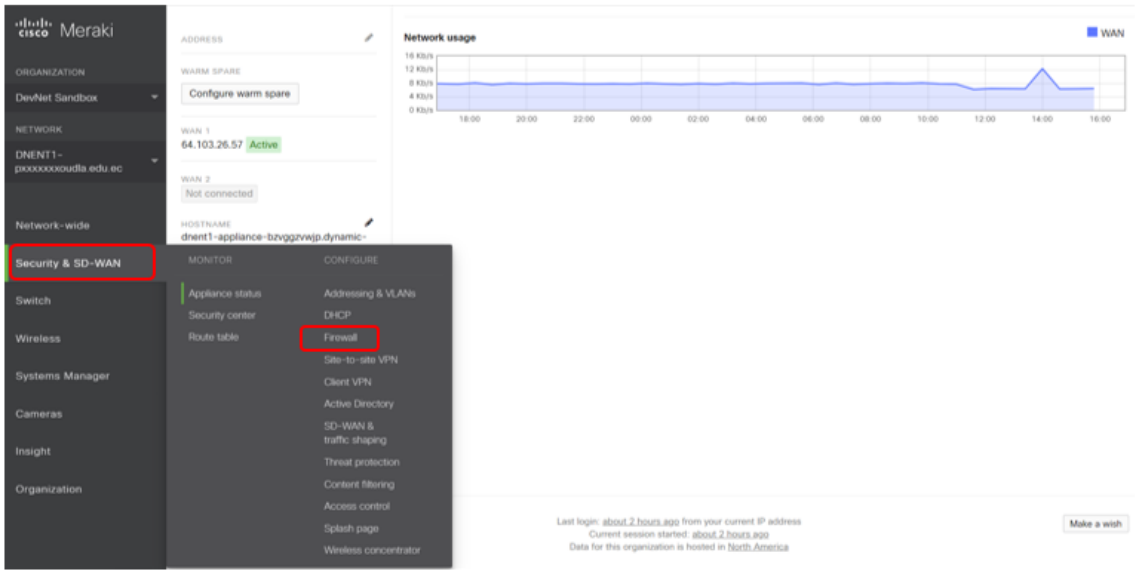


h) Para finalizar se configura el Firewall para permitir el paso por el puerto 84 que fue designado. En “Protección avanzada del firewall” se crea la regla de entrada (inbound rules), clic en Nueva regla y se configura con el puerto.



Parte 5: Configurar Meraki

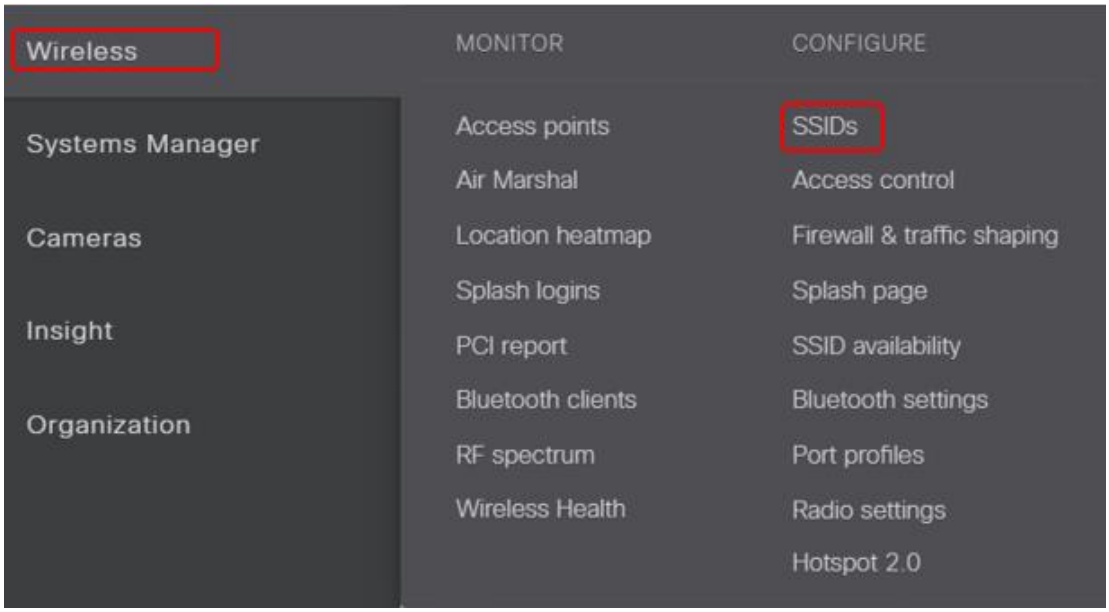
a) En un navegador se accede al Dashboard de Meraki, en la organización y red que este configurada los equipos. Se debe crear una regla en el router MX, en Security & SD-WAN clic en “Firewall”.



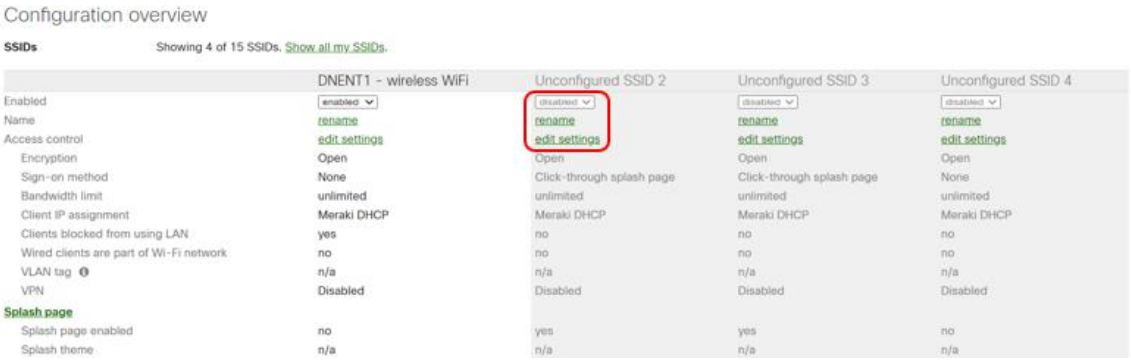
b) Deslizamos en la página hasta Forwarding Rules, y añadimos la nueva regla para permitir el acceso de Meraki hasta el Web Server de manera local.

c) Clic en guardar y ahora consultamos la IP Publica del router y se mediante la WAN se despliega el portal cautivo del servidor.

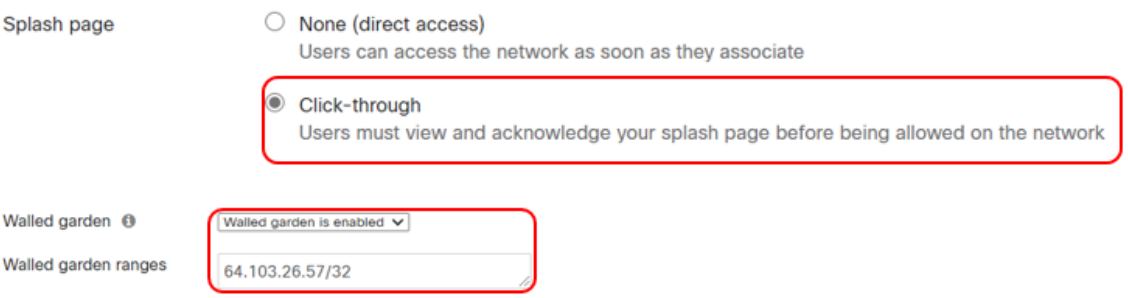
d) En Wireless y después clic en SSID, se debe configurar el Access Point para poder propagar la red en los dispositivos.



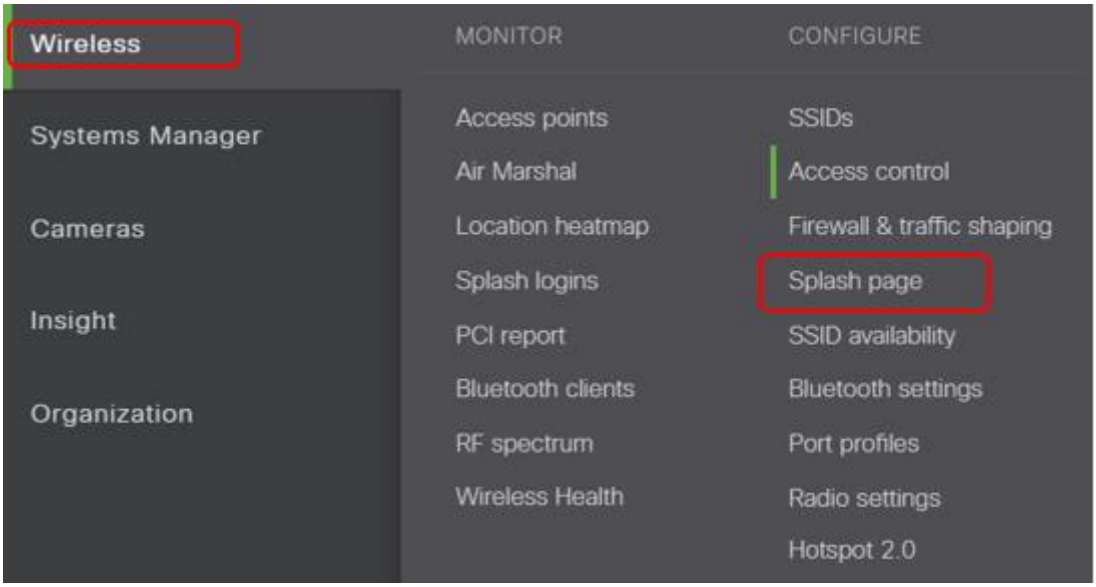
e) Clic en el recuadro para poder activar cualquier SSID (enable) o modificar una de ellas y cambiamos el nombre a “Portal Cautivo”. Una vez finalizado se debe editar los detalles.



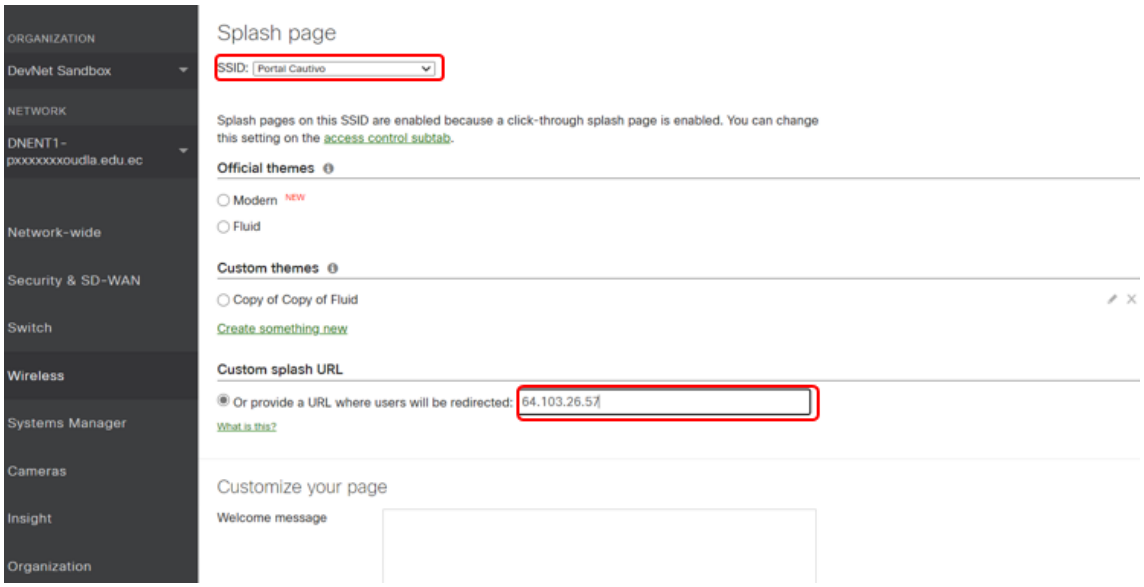
f) En los parámetros se debe cambiar en “Splash page” y seleccionar “Click-through” el cual configura la red para que exista registro previo. Deslizamos la página en “Walled Garden” se escribe la IP publica de la WAN para que el resto de dispositivos no locales puedan ingresar al Portal Cautivo.



g) Para finalizar se agrega la página web del servidor que se presenta al iniciar la conexión antes de poder tener acceso al SSID. Para lo cual clic en Wireless y después “Splash page”.



h) Aquí se configura de varias maneras la presentación, ya que existen plantillas predefinidas de páginas en modo “click-through” pero, se usa la previamente creada y la que apunta a la dirección WAN configurada con la conexión del Web Server.

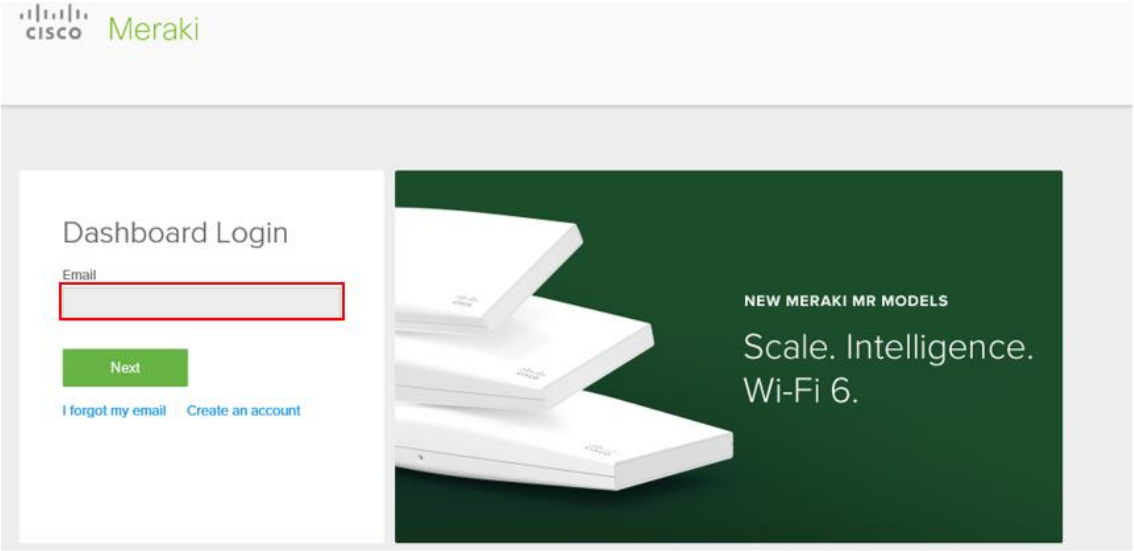


Guía de Laboratorio Integración de Meraki con API.

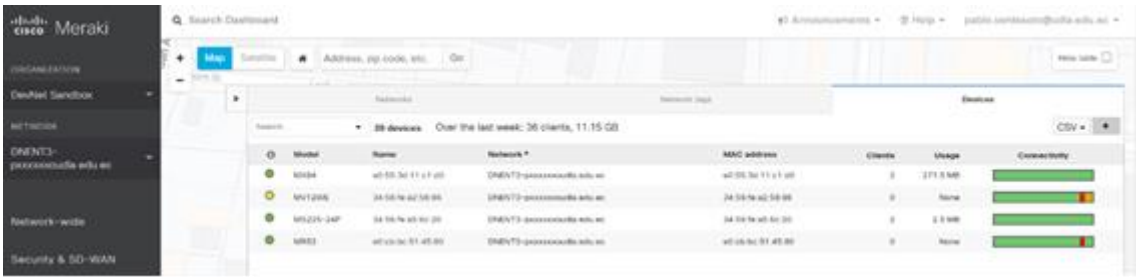
Parte 1. Conociendo Meraki

El panel o Dashboard de Meraki se maneja con la integración de una API en base al protocolo HTTP para transporte y JSON para serialización.

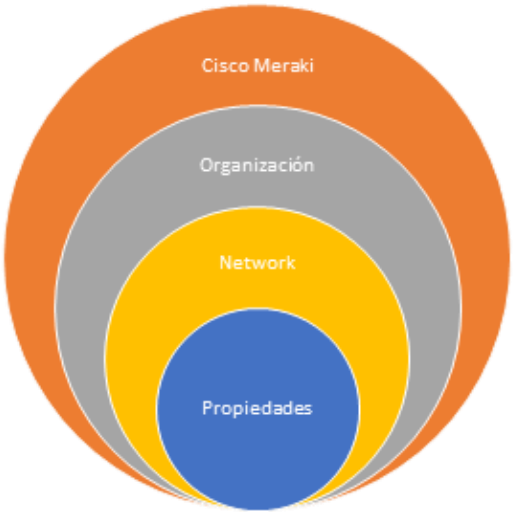
a) Para acceder a la página de acceso del Dashboard se ingresa a la dirección https://account.meraki.com/login/dashboard_login?go=%2F y se ingresa con las credenciales de Cisco ID.



b) En el inicio se muestra las diferentes Organizaciones con los equipos registrados o a los *Sandbox* que ofrece Cisco, solo las personas designadas como administradores tienen acceso a la consola.



c) El esquema de Meraki está constituido de la siguiente manera

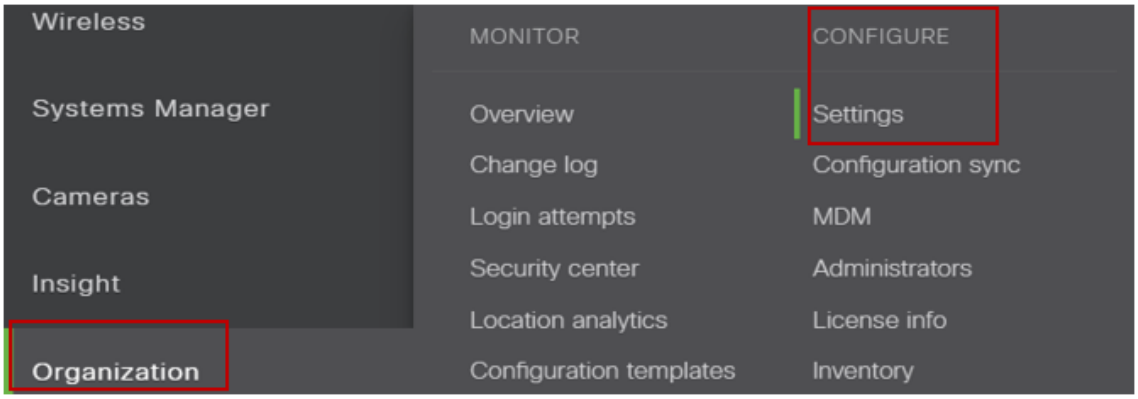


Al usar solicitudes HTTP la tabla adjunta muestra las posibles respuestas.

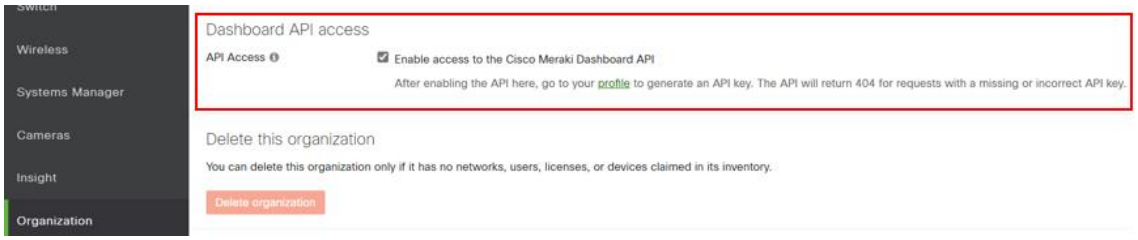
Código de estados HTTP	
2xx Exitoso	
200	Exitoso/OK
3xx Redirección	
301	Redirección Permanente
302	Redirección Temporal
303	No modificado
4xx Error Cliente	
401	Error No Autorizado
403	Prohibido
404	No encontrado
405	Método no permitido

Parte 2. Generar API Key

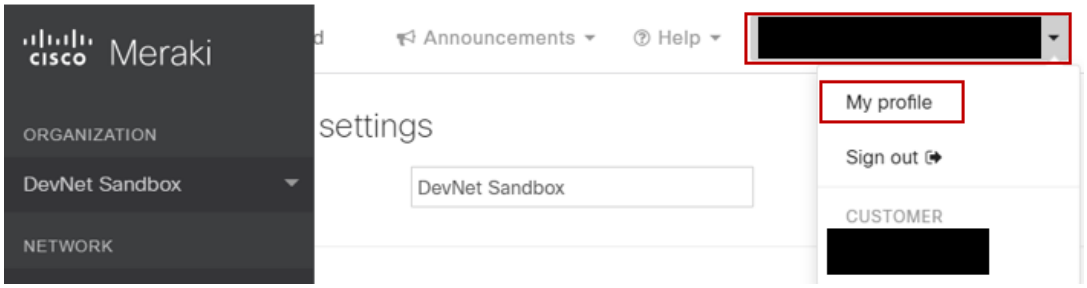
a) Para ingresar en la Organización, se sobrepone el mouse en el panel de la izquierda en *Organization*, en el submenú *Configure* y clic en *Settings*.



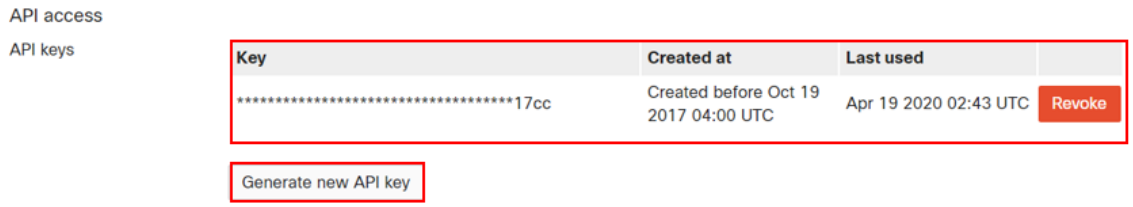
b) Se da clic en API Access para habilitar el acceso por una API *key* de valor único.



c) Se da clic en el usuario y después clic en *My profile*.



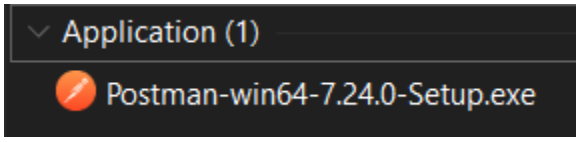
d) Deslizamos la página y en el apartado API *Access* generamos una nueva API *key* o se puede revisar cuales se encuentran activas.



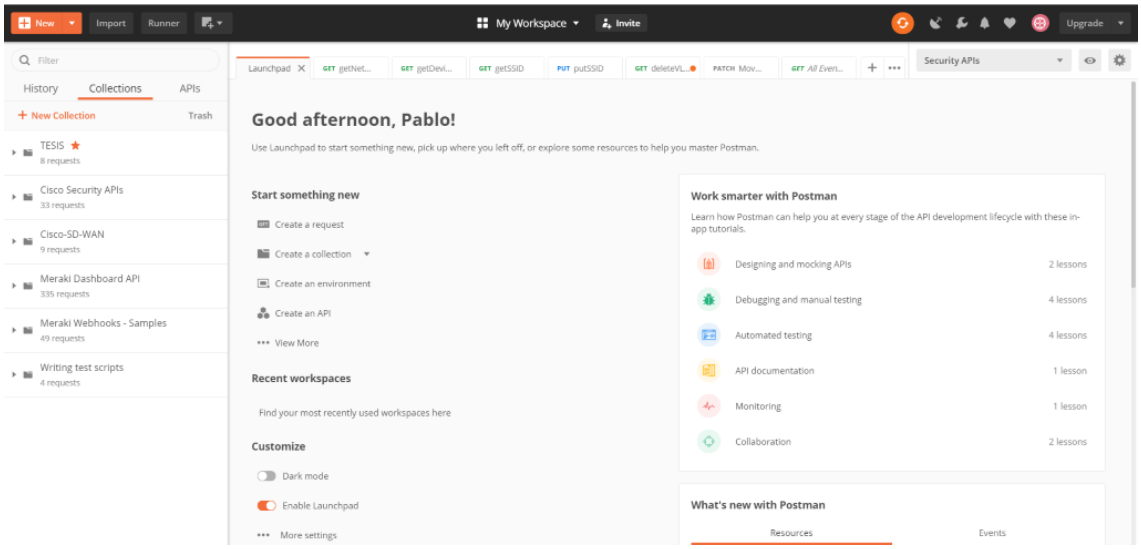
Parte 3. Descarga e Instalación de Postman

a) En un navegador se ingresa en la siguiente dirección https://www.postman.com/ y clic en *Download*.

b) Se accede a la ruta de descarga y con doble clic se ejecuta el programa para continuar el proceso de instalación.



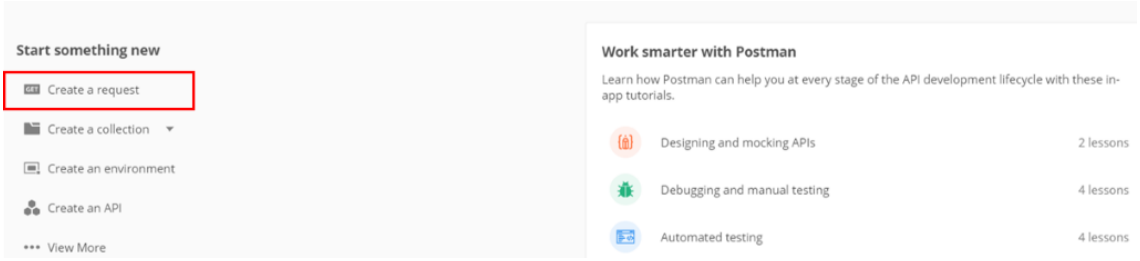
c) Finalizado el proceso de instalación se ejecuta la aplicación y se presenta el *launchpad* de inicio.



Nota. Postman es una conexión entre la API y JSON, recomendado por DevNet ya que cuenta con gran disponibilidad repositorios, compatible con un gran número de lenguajes de programación por ejemplo Java, C#, Python, etc.

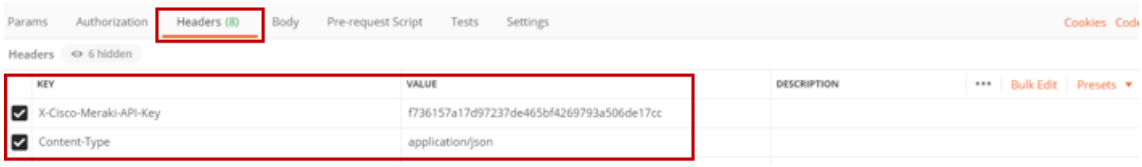
Parte 4. Método GET

a) Para comprobar que esté en funcionamiento la API con Meraki se ejecuta un nuevo proyecto, en el menú de inicio se da clic en *Create a request*.

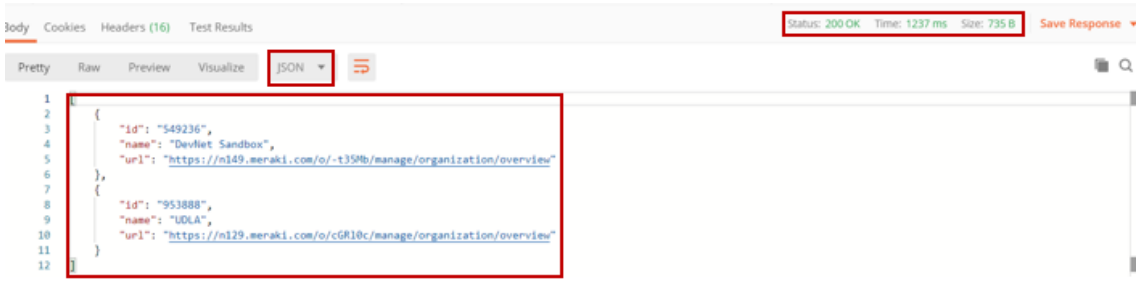


b) En el nuevo proyecto se coloca en el campo se solicitud HTTP la siguiente dirección: https://api.meraki.com/api/v0/organizations.

c) En la pestaña *Headers* como valor *X-Cisco-Meraki-API-key* se coloca el valor de la *API-KEY* y en *Content-Type* el lenguaje de tipo *application/json*.



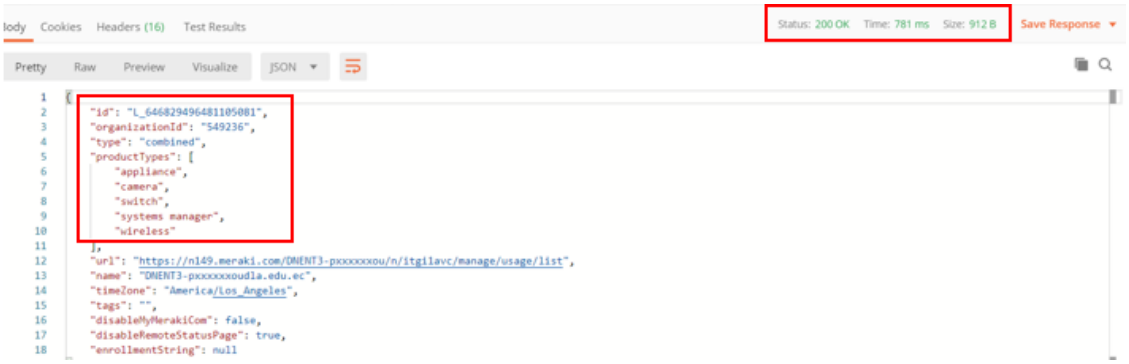
d) Se da clic en *Send*. Y se obtiene los valores para cada Organización que se tiene con el valor de la API Key.



Nota. El estado de una solicitud *GET* es *200 Ok*, caso contrario es *404 Not Found*.

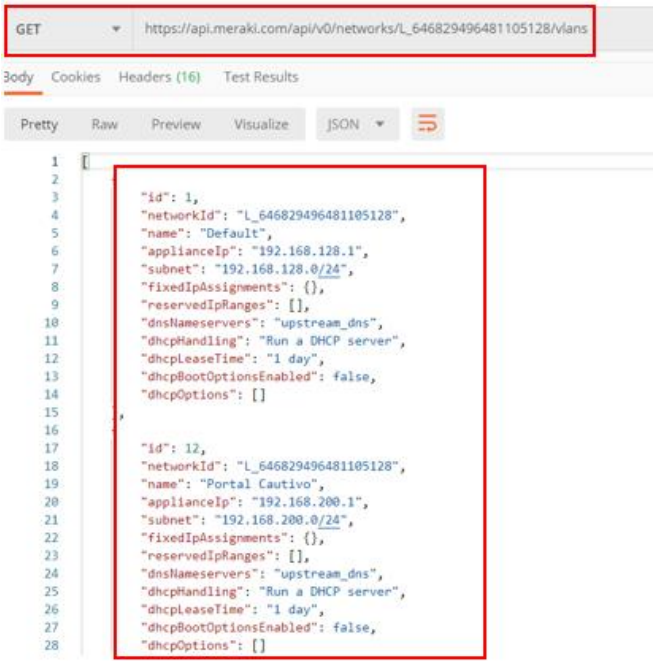
El ID de la Organización permite obtener el resto de componentes de una red, para lo cual se cambia la URL de solicitud a y en los corchetes se debe corregir el valor de la organización a la cual se solicita el *request*: https://api.meraki.com/api/v0/organizations/{organizationId}/networks.

e) De igual manera cada red que conforma una organización tiene un ID respectivo para funciones internas.

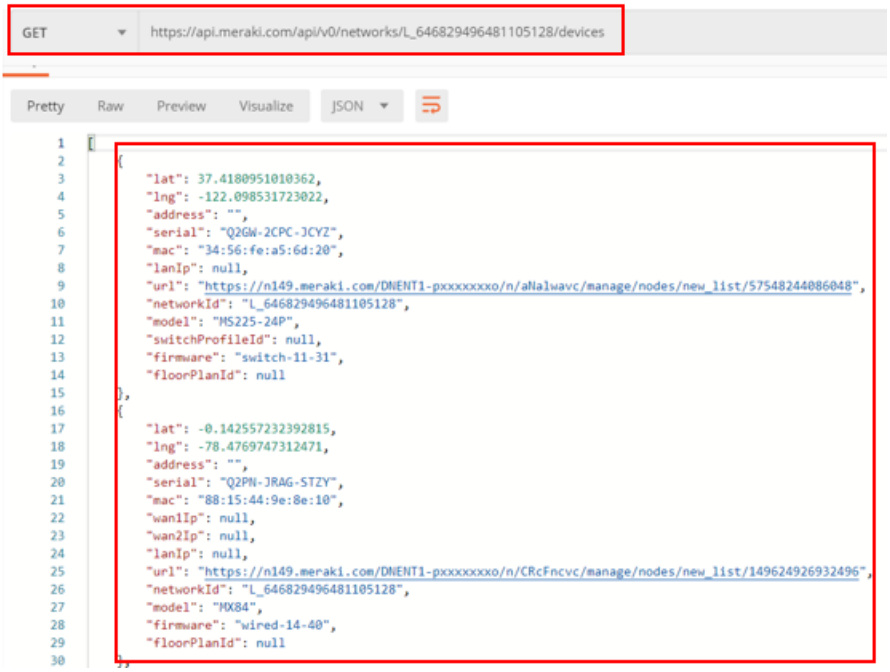


f) Se accede mediante la URL cambiando el parámetro en rojo https://api.meraki.com/api/v0/organizations/{networkId}/vlans

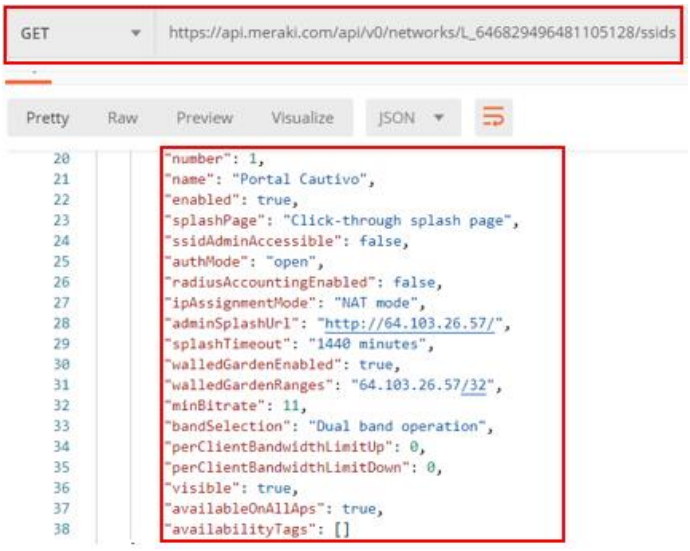
El ID propio de cada red permite realizar consultas específicas en cada una de ellas por ejemplo, consultar el número y características de VLAN.



g) Para listar los equipos y sus características se cambia la URL a https://api.meraki.com/api/v0/organizations/{networkId}/devices



h) Para listar las redes SSID y sus características se cambia la URL a https://api.meraki.com/api/v0/organizations/{networkId}/ssids



Parte 5. Método POST

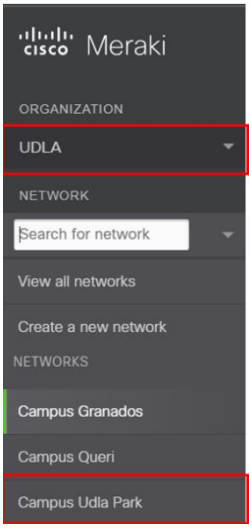
Nota. Existen limitaciones debido que a no en todas las solicitudes se permite crear información.

a) Para crear en una red en una Organización, se da clic en el combo box de solicitudes y se cambia a POST y se ingresa la siguiente URL https://api.meraki.com/api/v0/organizations/{organizationId}/network

b) Se da clic en *Body*, se selecciona el formato *raw*, y en el combo box *JSON*, se especifica la entrada para que sean interpretados los datos y clic en *SEND*.

c) La tarea tiene más tiempo de ejecución y si es exitosa su respuesta es *201 Created*, caso contrario se debe revisar los datos y la URL del método *POST*.

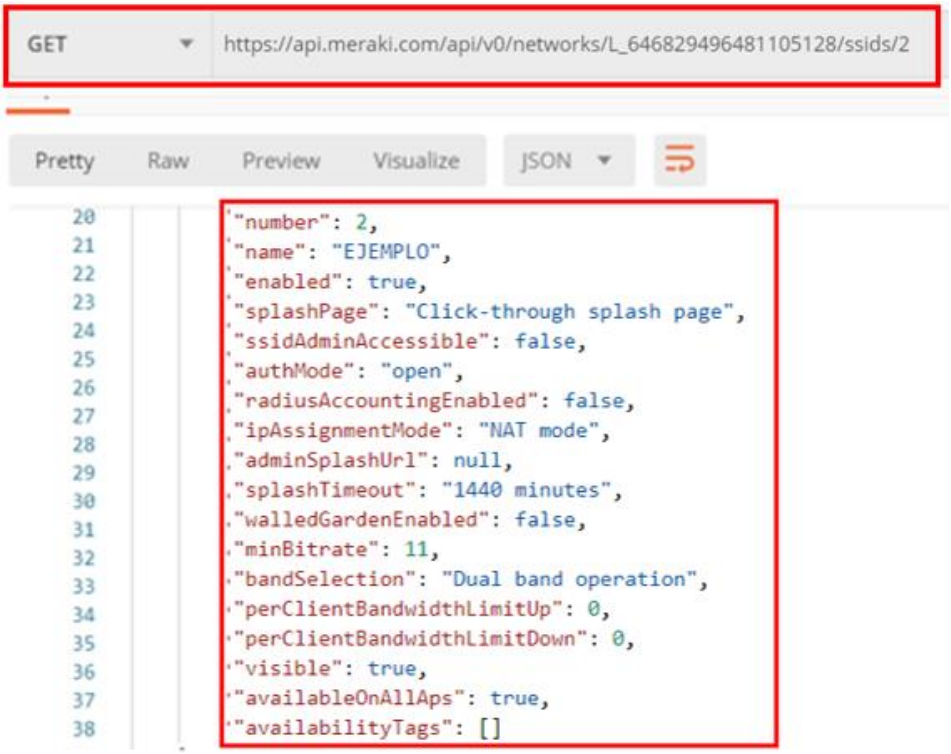
d) Al visualizar de igual manera en el *Dashboard* se refleja la red ya disponible.



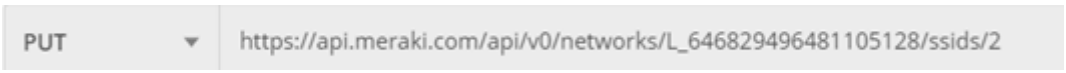
Parte 6. Método PUT

Nota. Existen limitaciones debido que a no en todas las solicitudes se permite actualizar la información.

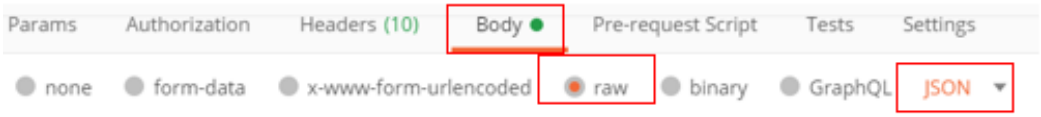
a) Primero se debe crear una red SSID se puede escoger por medio del Dashboard o Postman, y ponerle de nombre EJEMPLO.
b) En este caso la creación se realizar por Dashboard y se obtiene sus características mediante una solicitud *GET*.



c) Ahora en el combo box se selecciona PUT indicando que se va a realizar un cambio en la URL https://api.meraki.com/api/v0/networks/{networkId}/ssid/{ssidNumber}



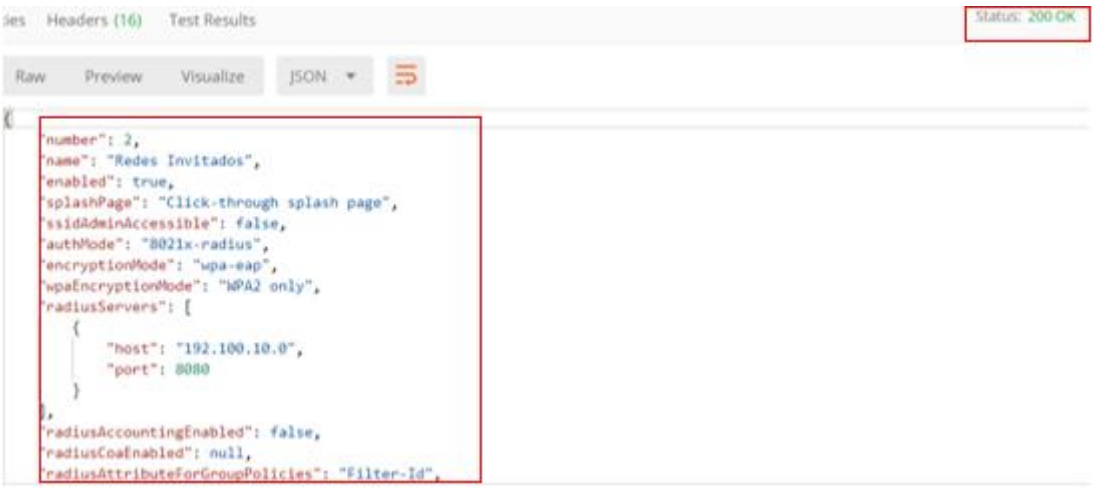
d) En el parámetro *Body*, se selecciona el formato *raw* y el lenguaje *JSON*.



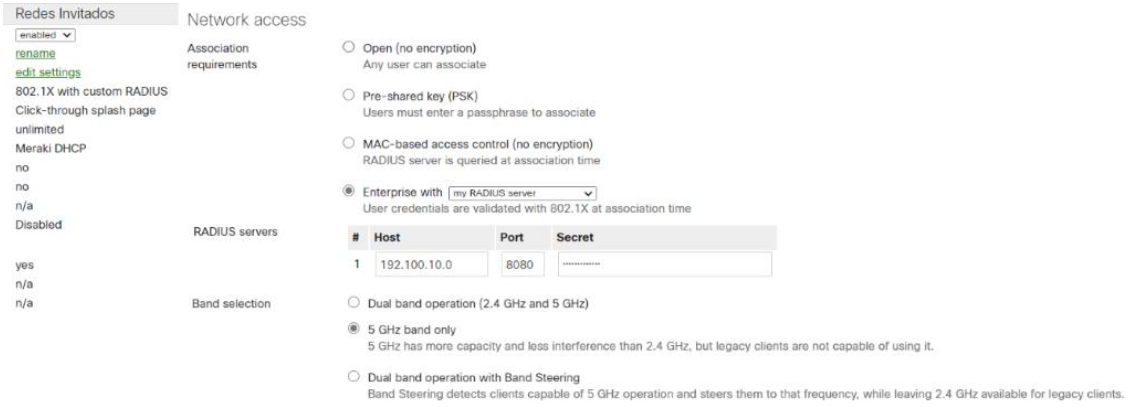
e) En el editor de texto se ingresa el código con los cambios realizados en base a las necesidades de la actualización y se clic en *SEND*.

```
"number": 2,
"name": "Redes Invitados",
"enabled": true,
"splashPage": "Click-through splash page",
"ssidAdminAccessible": false,
"authMode": "8021x-radius",
"encryptionMode": "wpa",
"wpaEncryptionMode": "WPA2 only",
"radiusServers": [
  {
    "secret": "34.hi@udla",
    "host": "192.100.10.0",
    "port": 8080
  }
```


f) Como resultado en la parte baja da el estado *200 OK* el cual nos refleja que no existe error alguno e imprime las nuevas características que ahora tiene la red SSID.



g) Otra forma de verificar es mediante el Dashboard dentro de las características del SSID dando clic en el link *edit settings*.

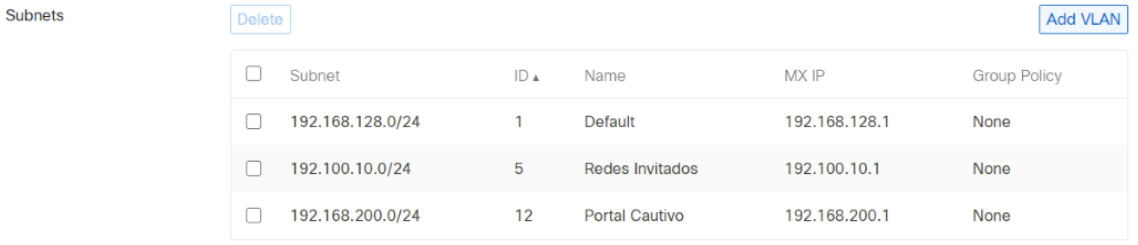


Parte 7. Método DELETE

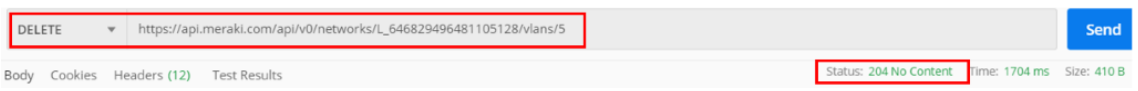
Nota. Existen limitaciones debido que a no en todas las solicitudes se permite eliminar información en otros casos se puede hacer una modificación de estado.

El método DELETE permite eliminar configuraciones u objetos en una red u organizaciones.

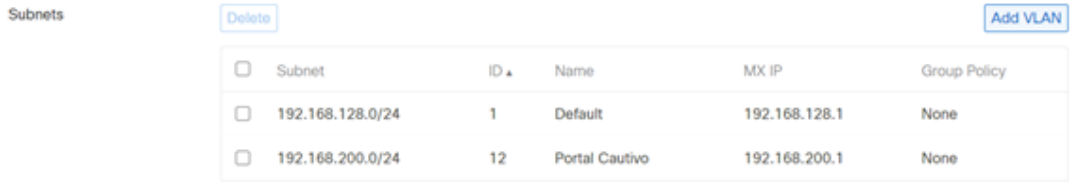
a) Para eliminar una red VLAN se necesitan los dos valores de identificación: *networkId* y el número de la VLAN.
b) Se consulta este valor mediante Postman o el Dashboard, aquí se visualiza tabla general de VLAN y se escoge la VLAN con ID 5 de nombre Redes Invitados.



c) En Postman se ingresa la URL y se cambia el método a DELETE.
d) Para finalizar se da clic en el botón SEND.



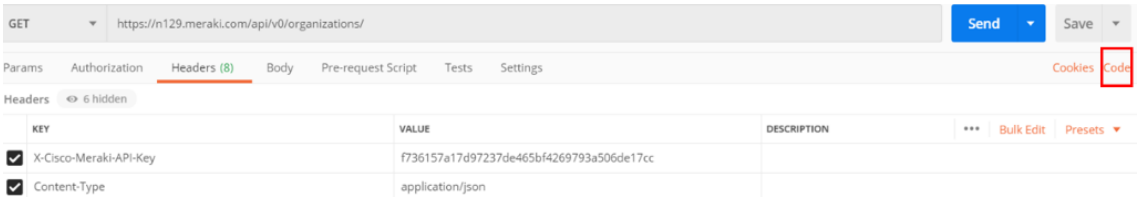
e) Para verificar se revisa en el Dashboard o con un método GET y como resultado la VLAN 5 ha sido eliminada.



Parte 8. Generar Código para otros lenguajes

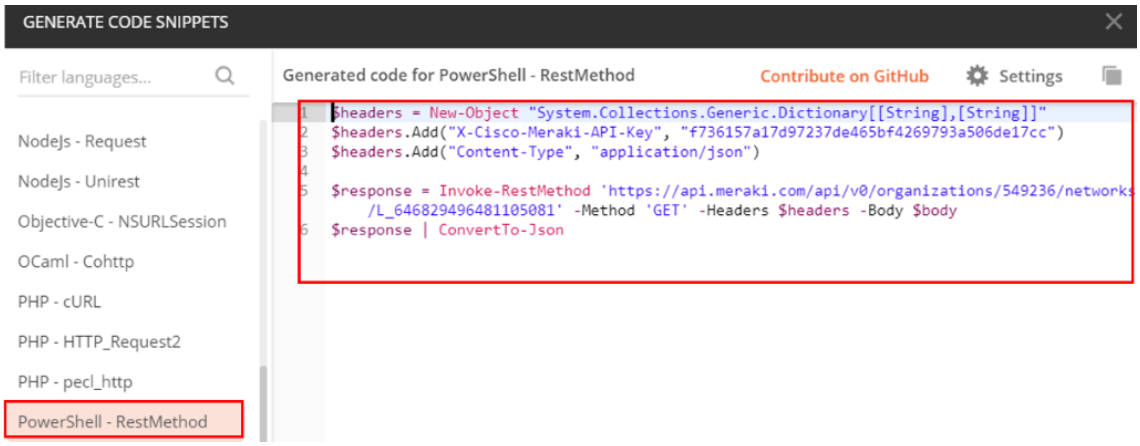
Una ventaja de Postman es generar de manera automática a diferentes plataformas o lenguajes de programación facilitando su implementación y despliegue.

a) Para generar el código en otros lenguajes se da clic en *Code*.



b) En el pop-up se escoge el lenguaje a realizar la traducción y en el apartado de la derecha se genera de manera automática el código.

c) Este código está adaptado de igual manera para el código original JSON.



d) En este caso se genera para PowerShell, se copia, pega y se ejecuta verificando que esta información es correcta.