1. IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE

PROGRAMA DE FORMACIÓN: Técnico en Implementación y Mantenimiento de Sistemas de Internet de las Cosas (IoT).
CÓDIGO DEL PROGRAMA DE FORMACIÓN:
PROYECTO ASOCIADO: Desarrollo e Implementación de soluciones IoT para el monitoreo, control y análisis de variables físicas en entornos industriales y residenciales.
FASE DEL PROYECTO: Ejecución
ACTIVIDAD DEL PROYECTO:
1.Establecer los parámetros de Operación de router, switch y dispositivos finales, AP de acuerdo a la topología y servicios.
2. Establecer los parámetros de Operación de los dispositivos IoT, Gateway IoT, Sensores, actuadores según el tipo de solución.
COMPETENCIA: Configuración de la red de telecomunicaciones.
RESULTADOS DE APRENDIZAJE:
1.Realizar la configuración los equipos de networking, de acuerdo con el diseño de la solución y la topología de red.
2.Realizar la configuración de los Dispositivos IoT, de acuerdo con el diseño de la solución.
DURACIÓN DE LA GUÍA: 96 horas.

2. PRESENTACIÓN

Esta guía busca que usted aprendiz tenga la habilidad y la destreza de realizar la interconexión de objetos o dispositivos a Internet (IoT) para permitir un control y gestión de forma remota y en tiempo real de los mismos. Toda esta información recopilada a través de sensores o dispositivos debe estar representada de manera sencilla en una plataforma que permita la conexión de datos, aplicaciones, dispositivos, sensores y todo tipo de hardware, en un único entorno. Por lo tanto, debe estar en capacidad de interpretar el diseño de red, identificar los equipos en la red, configurarlos y conectarlos apropiadamente para su correcto funcionamiento.



Las redes constituyen sistemas coherentes de interconexión entre dispositivos separados que permiten compartir información y recursos tales como servidores, estaciones de trabajo y periféricos. Una red debidamente diseñada e implementada puede brindar la rapidez y confiabilidad de comunicación que resulta esencial para todo sistema eficiente.

Con esta guía fundamentará conceptos como: Interpretar el diseño de red, reconocer la topología a implementar, conocer cómo se configuran los equipos para integrarlos a la red de forma segura y su puesta en operación acorde con los requerimientos.

Bienvenido a este nuevo reto en su aprendizaje y muchos éxitos en el desarrollo de estas actividades de aprendizaje.

¡APROVECHA ESTA OPORTUNIDAD DE APRENDIZAJE!

3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

- **Actividades de Reflexión inicial**.

a. Reflexiona y discute con un equipo de trabajo (3 aprendices) sobre estos interrogantes: Elije un objeto personal de tu casa y haz una lista de datos útiles que te gustaría obtener de él, a través de internet, para monitorear y controlar desde tu sitio de estudio. ¿Por qué son importantes?

¿Qué elementos “inteligentes” te gustaría que tuviera tu casa? Menciona 5. Explica en que te beneficiarían y cómo tendrías el control de esos objetos.

Escribe 5 riesgos de seguridad asociados a la red supuesta según la pregunta anterior. ¿Cómo podemos hacer para estar un poco más a salvo de esos riesgos que afectan la seguridad?

b. Luego realiza lo siguiente:

- Socializa compartiendo tus respuestas y puntos de vista. Ingresando al foro de discusión en la plataforma SENASofiaplus.

Tiempo estimado para la actividad: 2 horas

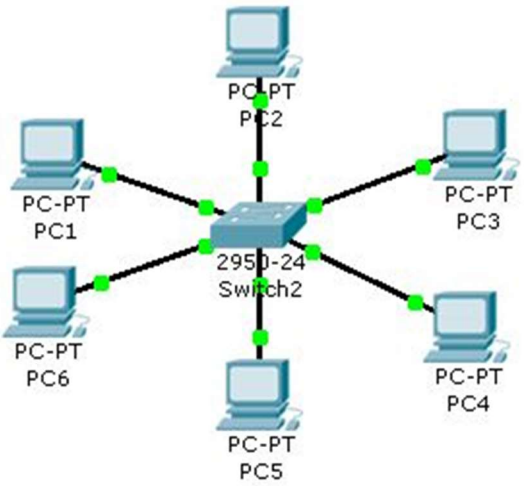
3.1 Actividades de contextualización e identificación de conocimientos necesarios para el aprendizaje.

Aprendiz como pudo apreciar en el desarrollo de las actividades de reflexión inicial, usted ya ha podido meditar en torno a qué nuevo tipo de redes aporta el Internet de las Cosas, identificando conocimientos sobre el tema de objetos, variables, dificultades, la seguridad y el alcance de su compresión general, aportando razonamiento e ideas que contribuyan a la solución de preguntas planteadas anteriormente.

Hoy en día ya no sorprende que podamos conectarnos a Internet con objetos cotidianos porque IoT engloba incluso, desde sensores de temperatura o de presencia para el control de la calefacción o la luz en los hogares, cámaras IP, equipos PLC, routers, puntos de acceso WiFi hasta sistemas industriales automatizados.

Actividad.

Planteamiento de Caso. En el siguiente gráfico se muestra una red instalada por una empresa sobre una estructura cableada con topología en estrella. Se han certificado las conexiones y la infraestructura está conforme a lo planteado. Sin embargo, no se tiene la certeza de cómo hacer para que la información que se va a enviar del PC1 al PC5 llegue a ese destino y no a otro, es decir, que lo identifique sin equivocación.



Junto con tu grupo de trabajo (3 aprendices) idea un mecanismo para garantizar que un mensaje enviado de un computador a otro llegue al destino deseado sin equívoco. Registra la respuesta en un video de máximo 4 minutos donde cada uno dará su opinión al respecto usando una didáctica expositiva a sus compañeros.

Tiempo estimado 30 minutos.

La actividad anterior implica que cada equipo debe estar debidamente identificado en la red, lo que nos lleva a relacionarnos con el Protocolo Internet ó IP cuya función es precisamente, identificar el origen y el destino de la información. La mayoría de los equipos de conexión a red admiten IPv6, la versión más reciente de la norma Internet Protocol (IP), que sustituye a IPv4 (que admite direcciones de 32 bits en formato decimal) lo que se traduce en aproximadamente 4.300 millones de direcciones, una cifra que han agotado en gran medida todos los dispositivos conectados en todo el mundo. IPv6 puede admitir direcciones de 128 bits en forma hexadecimal, lo que se traduce en aproximadamente 340 sextillones (3,4 x 1038) de direcciones, una cifra casi ilimitada que puede manejar ampliamente todos los dispositivos de la Internet de las Cosas imaginables. Enrutar todo el tráfico mundial que se genere por las redes de datos, realizar mejores funciones a nivel de procesamiento de rutas, sumarizar rutas, brindar optimizaciones y rendimiento en el tráfico de la red, todo esto y más será posible con IPv6. Para profundizar esta actividad participa activamente de la socialización dada por parte del instructor y la siguiente actividad.

Actividad:

Identificar y reconocer los tipos de direccionamiento en redes de datos.

Estimado aprendiz antes de comenzar esta actividad resuelva el siguiente cuestionario de preguntas:

1. Qué es el direccionamiento IP?
2. Cuál es la estructura de datos de IPv4?
3. Cuáles son los rangos de Direcciones IP disponibles por Clases de Red A, B, C, D, E?
4. De lo que usted menciona, defina el significado de submáscara de red o prefijo y la cantidad de host que se pueden direccionar por cada clase.
5. Defina para cada clase: dirección de red, dirección de host, primer host, último host, prefijo y dirección de broadcast.

Elabore una presentación y socialice en clase el trabajo grupal realizado. El instructor realizará las aclaraciones pertinentes y complementará conocimientos respecto a IPv4, clases, subredes y enrutamiento.

Complemente la información a través del video Direccionamiento IPv4 y Subredes (https://www.youtube.com/watch?v=SHbBso63X38&t=128s) y CURSO de REDES 2019 para PRINCIPIANTES (https://www.youtube.com/watch?v=Tf0adcLBPdI). Consulte y elabora un mapa conceptual sobre: VLSM, CIDR y FLSM.

Tiempo estimado 10 horas

La versión del Protocolo de Internet **IPv6** es un conjunto de especificaciones del grupo de trabajo de ingeniería de Internet que en realidad es una versión actualizada del IPv4. Dado que es la última versión, se utiliza para identificar diferentes dispositivos en Internet para que puedan ser localizados. Este protocolo define sus propios tipos de direcciones Dirección Unicast global, dirección local única, dirección Unicast, Anycast y dirección de enlace local. Dentro de su proceso de aprendizaje de redes IoT será de vital importancia la aplicación de este tipo de direccionamiento, razón por la cuál a continuación se presenta una serie de actividades orientadas a adquirirlo y posteriormente aplicarlo.

Actividad

DIRECCIONAR HOST EN REDES DE DATOS

Resuelva los siguientes interrogantes:

¡Porque es importante aumentar el rango de direcciones IP para los sistemas 5G e IoT?
¿Que cambia respecto de IPv4 a IPv6? Escriba ejemplos de IPv6 según los tipos de direcciones definidas para el protocolo (Dirección Unicast global, dirección local única, dirección Unicast, Anycast y dirección de enlace local).

A continuación, con base en el simulador Packet Tracert y el siguiente video: DECODIFICANDO CONOCIMIENTOS. [Configurar el Direccionamiento IPv6]: https://www.youtube.com/watch?v=KtuxHLFP5fY identifique el procedimiento para configurar direcciones IPv6 en una red.

Participe en la socialización orientada por el instructor sobre esta actividad y de acuerdo con lo anterior, complemente la información de IPv6 a través del video [Packet Tracer - Implemente un Esquema de Direccionamiento IPv6 Subred]: https://www.youtube.com/watch?v=VDXwh3yr-G8. Deje evidencia de las prácticas simuladas y el informe de cada una de ellas. Elabore el **Taller N° 1** suministrado por el instructor.

Tiempo estimado 6 horas

CONFIGURAR DISPOSITIVOS DE RED

Aprendiz, el concepto de interconexión total a través de la red forman parte del llamado Internet de las cosas o Internet of Things (IoT) que puede suponer un enorme riesgo para el usuario, ya que aunque tengamos el móvil o el portátil protegidos con antivirus y programas, cosas como la Smart TV o la nevera que pueden conectarse a Internet no disponen de este nivel de protección y por tanto, son blancos fáciles de ser hackeados y abrir una vulnerabilidad para que un pirata entre en nuestra red. Por lo tanto, todo dispositivo IoT que esté en casa puede ser configurado para aumentar su seguridad y proteger la información. Adicionalmente, como todos estos dispositivos se conectan a internet es necesario saber cómo se configuran para su correcto funcionamiento. Recuerde que los equipos fundamentales de una red son el servidor, los terminales, los dispositivos de red y el medio de comunicación. Para reforzar este conocimiento participe activamente del siguiente proceso.

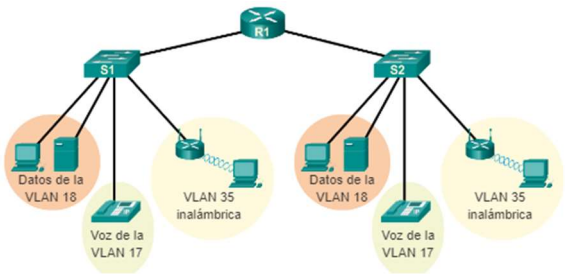
Actividad:

Estimado aprendiz, en esta actividad de aprendizaje después de conocer cómo se direccionan los hosts en una red, es importante conocer los diferentes dispositivos que la componen y las funciones que desempeñan cada uno de ellos. En grupos de 4 personas, realice una consulta en su Centro de Formación para diagramar la red con los dispositivos que la componen representados en un plano y una descripción aparte que involucre los aspectos técnicos de funcionamiento incorporados por cada uno de ellos. El resultado de esta consulta debe verse reflejado en la socialización que cada grupo haga de la información encontrada; cada exposición debe ser preparada con una presentación audiovisual y un folleto entregable a cada uno de los otros grupos.

Tiempo estimado 10 horas

CONFIGURAR SWITCHES O CONMUTADORES DE RED

VLAN -Virtual Local Área Network (Red de Área Local Virtual)



Es un segmento lógico más pequeño dentro de una red física cableada. Los diferentes hosts se combinan en una solución de red independiente de su ubicación: siempre que estén conectadas entre sí en la misma LAN, es posible combinarlos mediante una VLAN. No supone ningún problema que la LAN abarque varios switches. Los switches deben ser gestionables (Managed Switches).

Este tipo de configuración, estimado aprendiz, va a permitir crear redes IoT que agrupen equipos en un determinado segmento de red usando lo visto en la actividad anterior (subredes), garantizar más seguridad y administrar los equipos de forma eficaz.

Actividad

CONFIGURAR REDES DE ÁREA LOCAL VIRTUALES

En esta etapa de su aprendizaje es importante que elabore un mapa conceptual que le permita tener una noción y una apropiación clara sobre los siguientes conceptos: tipos de VLANs, membresía, enlace troncal, etiquetado y VLAN nativa basado en la lectura del link: https://sites.google.com/site/modulovlan/3-2-enlace-troncal-de-la-vlan/3-2-1-enlaces-troncales-de-la-vlan. Una vez realizado esto, socialice en su grupo de trabajo lo aprendido y contraste las repuestas. Posteriormente, el instructor en la sesión de clase resolverá dudas e inquietudes.

Para crear VLANs emplea el simulador Packet Tracert y configura empleando los comandos de la página https://www.itesa.edu.mx/netacad/switching/course/module3/#3.2.1.2 . Desarrolla el ejercicio propuesto en https://www.itesa.edu.mx/netacad/switching/course/module3/#3.2.2.5.

Tiempo estimado de la actividad: 10 horas

CONFIGURACION DEL ENRUTAMIENTO ENTRE REDES

Aprendiz, después de crear las redes virtuales de área local es fundamental saber conectarlas con otras redes. Para tal fin configuramos el router y definimos el enrutamiento como el proceso de reenviar paquetes entre redes, siempre buscando la mejor ruta (la más corta). Para encontrar esa ruta óptima, se debe tener en cuenta la tabla de enrutamiento y algunos otros parámetros como la métrica, la distancia administrativa, el ancho de banda, etc. Lo hacen los dispositivos de red

llamados Enrutadores (o Routers en inglés), y su único propósito es aprender rutas por las cuales alcanzar otras redes, y así poder transferir paquetes de datos entre ellas.

Actividad

CONFIGURAR ENRUTAMIENTO ENTRE REDES

Para configurar routers construiremos primero una sólida base con conceptos básicos sobre enrutamiento, para tal fin, participa activamente de la socialización impartida por parte del instructor y resuelve el **Taller N°2** referente a enrutamiento estático, dinámico y cómo funciona RIPv2, IGRP, EIGRP, OSPF, ISIS y BGP.

Usando un simulador de red (Packet Tracer) o un emulador (GNS3) realiza la simulación de configuración de la ruta estática. Puedes guiarte usando el video: Enrutamiento Estático con 3 Router en Packet Tracer 7.3 https://www.youtube.com/watch?v=3aY7KXWynt0 y https://www.youtube.com/watch?v=3aY7KXWynt0 y la página https://cesarcabrera.info/como-se-configura-el-enrutamiento/#:~:text=En%20resumen%2C%20el%20enrutamiento%20es%20llenar%20la%20tabla,trav%C3%A9s%20de%20un%20protocolo%20de%20enrutamiento%20en%20particular.

Tiempo estimado de la actividad: 8 horas

CONFIGURAR SEGURIDAD PERIMETRAL EN LA RED

La seguridad perimetral es un método de defensa de las redes informáticas, consiste en instalar equipos de comunicaciones en los que se establece las políticas de seguridad necesarias para su óptimo funcionamiento; estos equipos se sitúan entre la red externa y la red interna, permitiendo o denegando el acceso a los usuarios internos y externos a los diferentes servicios de la red. La implementación de seguridad perimetral consta de tres etapas Segmentación de la Red, Firewall y un Sistema de Prevención de Intrusos IPS.

Firewalls (FW). El firewall (cortafuegos) es un dispositivo o sistema capaz de cifrar, limitar o decodificar el tráfico de comunicaciones entre un ordenador, o una red local, y el resto de internet, con el objetivo de impedir que sistemas o usuarios no autorizados tengan acceso. Es un dispositivo relacionado con la seguridad perimetral, es decir, protege de todos los elementos sensibles de ser

atacados dentro de un sistema informático. Esto implica que cada paquete de tráfico transmitido debe ser analizado y aceptado o rechazado en función de su potencial riesgo de seguridad para nuestra red. Establece las políticas de seguridad necesarias para su óptimo funcionamiento; estos equipos se instalan entre la red externa y la red interna, permitiendo o denegando el acceso a los usuarios internos y externos a los diferentes servicios de la red.

Actividad

CONOCER LOS FIREWALLS HW Y SW DE REDES

Para complementar la información anterior, consulte y elabore una presentación grupal para socializar en clase: tipos de firewall hardware y software (Norton Free Firewall, OpenDNS, Firewall AVS, PeerBlock, Glasswire TinyWall, SmoothWall, OPNsense, Pfsense, Untangle Firewall). El instructor realizará las aclaraciones pertinentes y complementará conocimientos.

El firewall PFSense es el más utilizado debido a sus múltiples ventajas y características y es muy confiable para servidores FreeBSD. Entre sus funciones se tiene: Es actualizado desde su sitio web, tiene Interfaz gráfica, se puede implementar como firewall perimetral, enrutador y Servidor DHCP y DNS. Igualmente, se puede configurar como punto de acceso inalámbrico y punto final de VPN. Para complementar la información remítase al enlace https://www.pfsense.org/about-pfsense/. Elabore un informe en el cual presente el resumen de la lectura y un diagrama mostrando las maneras de conexión dentro de una topología de red.

Tiempo estimado de la actividad: 3 horas

CONFIGURAR SERVIDOR PARA DENEGACION DE ACCESO

Estimado aprendiz en el apartado a continuación podrá conocer que es un servidor proxy, cuál es su función operativa dentro de la red de datos, las ventajas que trae consigo la implementación de este en la topología dispuesta. Con las indicaciones del instructor realice la instalación del servicio que permitirá denegar el acceso a diferentes direcciones de red (URL) para los usuarios de red de acuerdo con una lista de privilegios.

CONFIGURAR SERVIDOR DE RED PROXY SQUID-3

Es un servidor de seguridad proxy que proporciona seguridad a la red. Filtra tráfico de nodo entrante a ciertas especificaciones que significan que solo se filtran los datos de la aplicación de

red transmitidos. Tales aplicaciones de red incluyen el Protocolo de transferencia de Archivos (FTP), Telnet, Protocolo de Transmisión en Tiempo Real (RTSP) y Bit Torrente. Cuando un cliente solicita acceso a los recursos del servidor, como archivos, páginas web y bases de datos, el cliente primero se conecta con el servidor proxy que luego establece una conexión con el servidor principal. La puerta de enlace de la aplicación reside en el servidor de seguridad del cliente y del servidor. El servidor proxy oculta las direcciones de Protocolo de Internet (IP) y otra información segura en nombre del cliente. Un computador del sistema interno puede comunicarse con otro externo usando protección de firewall. Realice la lectura del documento mostrado en el enlace y elabore un resumen del mismo: http://ijarcs.info/index.php/Ijarcs/article/viewFile/3412/3651.

Tiempo estimado de la actividad: 3 horas

CONFIGURAR SEGURIDAD EN DISPOSITIVOS DE REDES INALAMBRICAS

Apreciado aprendiz, en este apartado usted podrá encontrar saberes en referencia a las redes inalámbricas, las diferencias entre los protocolos de seguridad para redes inalámbricas definidos por la IEEE, para esto se presenta dos tablas las cuales resumirán los conceptos a adquirir.

Participe activamente en la sesión, por parte del instructor, sobre que consiste cada uno de los mecanismos de seguridad establecidos por la IEEE para las redes inalámbricas (Protocolos de seguridad WEP, WPA, WPA2). Establezca las diferencias entre sí y presente los diferentes estándares 802.11 existentes con su evolución a través del tiempo. Posteriormente el instructor resolverá dudas e inquietudes. Documento de apoyo Carceller, C. , Campos, S. , & García, M. (2013). *Servicios en red.* Madrid, ES: Macmillan Iberia, S.A. (pp. 234 - 243).

Tiempo estimado de la actividad: 4 horas

ACTIVIDAD

CONFIGURAR DISPOSITIVOS EN REDES IoT

Estudio de caso. Hoy en día en algunos lugares existe la preocupación por una alimentación sana. Los alimentos orgánicos junto con huertas de patio se han popularizado entre algunas personas que quieren cultivar sus propios alimentos. Muchas de estas personas no tienen mayores conocimientos en agricultura y estarían dispuestos a adquirir algún equipo que les ayude con la tarea de cuidar las plantas.

Ante esta necesidad surge la idea de desarrollar un sistema de riego automático que ayude en esta labor. Para esto un empresario le ha contratado a usted como técnico y le ha sugerido utilizar tecnologías de IoT para desarrollar un producto y ofrecerlo a las personas que tienen pequeñas huertas de jardín.

Para comenzar esta actividad resuelva el siguiente cuestionario de términos y palabras realizando una búsqueda en internet. Identifique la función de cada equipo o elemento dentro de una red IoT. Son ellos: Gateway IoT, Configuración Edge Gateway IoT, Sistemas operativo de Gateway IoT, sensores y actuadores. Posteriormente, elabore un esquema con los elementos que consideres necesarios para la resolución del problema (Redes de sensores, tarjetas inalámbricas de bajo consumo, actuadores, enrutadores inalámbricos). El esquema realizado servirá como un diseño previo para las siguientes actividades. Espera las observaciones por parte del instructor

Tiempo estimado de la actividad: 2 horas

Actividad

CONFIGURAR GATEWAY IoT

El IoT se usa ya en entornos laborales, los servicios públicos, la fabricación y la producción y distribución de todo tipo de mercancías, así como para facilitar la comunicación entre los trabajadores y sus mandos o con los clientes. El Internet de las cosas ya está a la orden del día.

Esto se ha logrado gracias a los avances en electrónica, miniaturización, sensores, redes de datos inalámbricas, la aparición de nuevos estándares de comunicaciones. Piensa en lo siguiente ¿Cuál es el papel que juegan las puertas de enlace predeterminadas o gateways dentro de este entorno del internet de las cosas? ¿Cuál es el dispositivo que cumple esta labor de enrutamiento en su casa?

Grupos de 2 personas

Tiempo estimado: 30 Minutos

Aprendiz, en el ámbito de las telecomunicaciones, el objetivo principal de un gateway es servir de puente entre los diferentes tipos de tecnologías de la comunicación. Estas tecnologías pueden variar en términos de tipos de conectividad, interfaces o protocolos. Por ejemplo, su Gateway de Internet en casa conecta su Red de Área Local (LAN) con su Proveedor de Servicios de Internet (ISP). Este gateway enlaza la WAN del ISP a través de tecnologías como PPP o HDLC con su LAN con TCP/IP.

El gateway IoT sigue el mismo principio de tender puentes entre las comunicaciones de diferentes tecnologías. Crea un puente entre los sensores/actuadores IoT e Internet. El gateway IoT agrega todos los datos, traduce los protocolos del sensor y preprocesa los datos antes de enviarlos.

Los dispositivos IoT se conectan al gateway IoT utilizando modos de transmisión inalámbricos de corto alcance como Bluetooth LE, Zigbee, Z-wave, o de largo alcance como LTE, LTE-M, Wifi, y luego se conectan a Internet (Nube Pública) a través de Ethernet LAN o Fibra Óptica WAN (HDLC/PPP).

El empresario indica al equipo para consultar el siguiente libro para profundizar sobre gateways y determinar cuál es el mejor protocolo para las necesidades del proyecto. Realiza un cuadro comparativo de los protocolos de comunicación descritos en el libro del enlace a continuación (pág. 90). https://www.researchgate.net/publication/327702411_Capitulo_3_Internet_de_las_cosas_IoT Describe adicionalmente los pasos hechos en cada protocolo para el registro de los dispositivos clientes.

Tiempo: 3 Horas

Durante la discusión del diseño el empresario considera importante adquirir un Edge Gateway comercial y te solicita realizar un informe de configuración práctico que describa que es un Edge Gateway y los pasos para configurar este producto. Te sugerimos esta página, si deseas puedes poner otra fuente: https://docs.microsoft.com/en-us/learn/modules/set-up-iot-edge-gateway/.

Tiempo estimado: 2 Horas 30 Minutos

El empresario está preocupado porque las soluciones para gateway que hay en el mercado son muy costosas. Ana dice que se puede utilizar plataformas de hardware y software de uso libre para ello recomienda ver la siguiente página.

https://aprendiendoarduino.wordpress.com/2019/10/23/gateways-iot-2/

¿Qué ventajas encuentras usando estas tecnologías?

Tiempo estimado: 2 Horas

El jefe pregunta ahora por el sistema operativo. Ana recomienda que tu des tu opinión y te sugiere esta página. https://www.arrow.com/en/research-and-events/articles/iot-operating-systems (Utiliza el traductor del navegador web)

Bajo la posición de defender Linux como sistema operativo. ¿Cuáles son las ventajas de Linux respecto a otros sistemas operativos, especialmente considerando las soluciones de Gateway?

Tiempo estimado: 2 horas

3.2 Actividades de apropiación del conocimiento (Conceptualización y Teorización).

CONFIGURAR SERVICIOS VIRTUALES DE RED

Apreciado aprendiz, en el apartado a continuación usted podrá adoptar un glosario de saberes y terminologías necesarias para el desarrollo técnico y para la configuración de equipos virtuales, tales como: Hipervisor, Máquina virtual, Firewall, Proxy, ISO, IOS, VPN, TUNEL, entre otros. Tales saberes son indispensables para la implementación de una red virtual estructurada con un nivel de seguridad perimetral para garantizar la protección de datos que fluye a través de la red.

Usted estará en la capacidad, con el acompañamiento del instructor, de configurar un equipo para la virtualización de sistemas operativos, comunicar dos o más máquinas virtuales en red, implementar un firewall para establecer reglas de permisos y denegaciones, habilitar un servidor Squid-3, crear BlackList para denegación de servicios de internet a usuarios dentro de la red y de limitar el ancho de banda a cada usuario o dependencia de la red entre otros.

Actividad

Una vez terminada la actividad anterior, participe del sondeo inicial que realiza el instructor a través del debate acerca de las temáticas a tratar en esta actividad, aquí es importante identificar los saberes previos que trae consigo. Para tal fin resuelva los interrogantes: ¿Qué es un hipervisor? ¿Para qué se utiliza un hipervisor? ¿Qué tanto beneficia implementar hipervisores en la red? ¿Qué es una máquina virtual? ¿Para qué se utiliza una máquina virtual? ¿Sus beneficios en la red? ¿Qué es una imagen ISO? ¿la importancia de usar imágenes ISO en la red? Defina servidor, su importancia y uso. ¿Qué es seguridad en la red? ¿Para qué se definen esquemas de seguridad en la red? ¿Por qué es impórtate resguardar el tráfico de la información que fluye por la red? ¿Qué es una VPN? ¿Para qué me puede servir una VPN? ¿Cuáles son sus usos en la red?

Tiempo estimado de la actividad: 8 horas

CONFIGURAR SISTEMAS HYPERVISOR PARA REDES

El instructor realiza la presentación sobre la diversidad de hipervisores existentes tales como: Virtual Box, VMware, XenServer y sus principales funcionalidades de acuerdo con su desarrollador, su uso para virtualización de sistemas operativos Linux, Windows, Free BSD, Mac entre otras.

Actividad

Esta actividad le permite transferir conocimientos técnicos orientados al hacer, en los que usted aprendiz, desarrollará destrezas y habilidades para la correcta instalación de hipervisores en un equipo servidor, a fin de crear diversidad de máquinas virtuales con diferentes sistemas operativos y simular una red física en una red totalmente virtual. Usted logrará establecer una comunicación exitosa entre las diferentes máquinas instaladas para el envío y recepción de paquetes de datos.

Realice el proceso de instalación de Virtual box como Hipervisor Open Source (software libre) tomado de su apartado oficial https://www.virtualbox.org/wiki/Downloads y que se adecúe a su sistema operativo. Documente la actividad en un informe para dejar evidencia del proceso.

En este punto del proceso el instructor lo orientará con el fin de adquirir los conocimientos técnicos en virtualización y emulación de sistemas operativos, guiando el proceso de instalación de máquinas virtuales en Hipervisor Virtual Box. Identifique los recursos de servidor y relaciónelos con los IOS (Sistemas Operativos) a usar, entienda cuál es la cantidad de recursos mínimos para la operatividad de estos, aclare el concepto de qué es una imagen ISO, las diferencias entre los sistemas operativos 32 y 64 bits y cuál es la función de estas dentro de la práctica.

El instructor explica, mediante una práctica, la comunicación entre máquinas virtuales ubicadas en el mismo segmento de red logrando switching entre ellas y utilizando interfaces de tarjetas de red virtuales y plantea un ejercicio al respecto a elaborar por usted. Realice la práctica y documente el proceso como evidencia.

Tiempo estimado de la actividad: 8 horas

Actividad

CONFIGURAR FIREWALLS DE RED

Esta actividad le permitirá a usted como aprendiz desarrollar destrezas y habilidades técnicas para la correcta instalación y configuración del cortafuegos, logrando establecer servicios de seguridad

perimetral en redes para ofrecer una mayor confiabilidad a los usuarios, tanto internos como externos, sobre la transparencia, protección de su información y para el acceso de diferentes servicios.

INSTALAR FIREWALL DE RED CON CONFIGURACIÓN BÁSICA

Con la orientación del instructor, de manera individual, instale Firewall Open Source PFsense en hipervisor Virtual Box, tenga en cuenta que trabaja bajo el sistema operativo Free BSD.

Para lo anterior apóyese en la plantilla a continuación presente:
https://drive.google.com/file/d/1Eu8LYg_09ZVyGeBh61E5rwh0UPOILGuf/view?usp=sharing.
Una vez instalado, realice la configuración básica del firewall según la orientación del instructor de acuerdo con la funcionalidad de cada panel de control de la plataforma.

Tiempo estimado de la actividad: 5 horas

Actividad:

CONFIGURAR SERVIDOR DE RED PROXY SQUID-3

Hasta este momento, usted apreciado aprendiz, ha adquirido un bagaje de saberes y ha desarrollado ciertas habilidades para la configuración. Si hacemos un recuento, podremos decir que se encuentra en la capacidad de realizar la correcta instalación de diferentes hipervisores y en ellos, la instalación de sistemas operativos que pueden comunicarse dentro de un mismo segmento de red. También la instalación y configuración básica del firewall, enrutar los diferentes equipos que encuentran en la red y permitir servicios como DHCP.

Para el desarrollo de esta actividad, con indicaciones del instructor, usted deberá realizar la activación y configuración del servidor squid-3 en firewall Pfsense. El proxy es una de las diversas funcionalidades que trae consigo el cortafuegos. Puede apoyarse en la plantilla alojada en el enlace: https://drive.google.com/drive/folders/1suwUWUQ8mW-3GbpKYjTRtiXjiltbzeXk?usp=sharing

Para la selección de sistemas operativos, configuración de NIC de máquinas virtuales, apóyese en el referente bibliográfico a continuación:
Carceller, C. R., Campos, S. C., & García, M. C. J. (2013). Servicios en red. Pag. (16-25) https://kupdf.net/download/servicios-en-red-pdf_5b0aaa52e2b6f51e34222137_pdf

Tiempo estimado de la actividad: 4 horas

ACTIVIDAD

CONFIGURAR DISPOSITIVOS EN LA RED IoT

Durante la investigación concerniente al diseño del sistema IoT un compañero de trabajo ha encontrado una página web para implementar un Gateway muy económico, no industrial y que puede cumplir con el requerimiento.

Te invitamos a analizar esta solución y realizar un diseño detallado para llevarlo a implementación:

http://cpham.perso.univ-pau.fr/LORA/RPIgateway.html
(Utiliza el traductor del navegador web)

Transferencia

Implementa la solución utilizando como requerimientos no funcionales:

- ✓ Arduino o raspberrypi 2 placas
- ✓ Módulos de protocolo de comunicación LoRa uno para el Gateway y otro para la placa que controla el sensor y el actuador
- ✓ Sensor de humedad compatible
- ✓ Relay compatible (simulador de actuador)
- ✓ Firebase como servidor de datos
- ✓ IDE compatible con la placa escogida Arduino o raspberry

El diseño final será evaluado por el instructor para valorar su funcionamiento acorde con los requerimientos y los parámetros establecidos para su correcto funcionamiento.

Tiempo estimado: 12 Horas

Ambiente Requerido

- Taller de Telecomunicaciones
- Biblioteca

Materiales

- Antenas
- Dispositivos de red (switch, router, firewall, sensores, gateways IoT, actuadores, etc.)
- Software para redes (simuladores, emuladores, plataformas IoT, etc.)
- Cable UTP
- Portátiles
- Video Beam o Pantalla de TV
- Tablero
- Marcadores Borrables.

4. ACTIVIDADES DE EVALUACIÓN

Evidencias de Aprendizaje	Criterios de Evaluación	Técnicas e Instrumentos de Evaluación
Evidencias de Conocimiento: **Evidencias de Desempeño**	Establece configuración de equipos networking de acuerdo con manuales técnicos y topología de red. Realiza las configuraciones de seguridad en los equipos de networking según políticas de la empresa. Activa protocolos y servicios en los Gateway IoT de	Observación directa/Lista de Chequeo Formulación de preguntas /Cuestionario

Evidencias de Producto:	acuerdo con manuales técnicos. Integra los dispositivos IoT de acuerdo con la solución. Identifica los entornos de virtualización de acuerdo con la solución IoT.	Valoración de producto/ Lista chequeo

4. GLOSARIO DE TERMINOS

Ad-hoc: Grupo de dispositivos inalámbricos que se comunican directamente entre ellos (punto a punto) sin la utilización de un punto de acceso.
AES (Estándar avanzado de cifrado). Técnica de cifrado de datos simétrica de bloque de 256 bits.
Ancho de banda. Capacidad de transmisión de un dispositivo o red determinado.
CTS (Limpiar para enviar). Señal enviada por un dispositivo para indicar que está preparado para recibir datos.
DDNS (Sistema dinámico de nombres de dominio). Permite albergar un sitio Web, servidor **FTP** o servidor de correo electrónico con un nombre de dominio fijo (por ejemplo, www.xyz.com) y una dirección IP dinámica.
Red Punto a Multipunto. Aquellas en las que cada canal de datos se puede usar para comunicarse con diversos nodos.
Red troncal. Parte de una red que conecta la mayoría de los sistemas y los une en red, así como controla la mayoría de los datos.
WPA2 (WiFi Protected Access 2). WPA2 es la segunda generación de WPA y proporciona un mecanismo de cifrado más fuerte a través del Estándar de cifrado avanzado (AES), requisito para algunos usuarios del gobierno.
Things as a Service (TaaS). Cuando la red en cuestión que gestiona es la nube, se llama así a la entrega de servicios y datos.
Red de área corporal (BAN). Red de la salud electrónicamente controlada gracias los sensores.
Web Social de las Cosas (SWoT). El componente social del Internet de las Cosas.
Identidad de las cosas (IDOT). Sistema que controla la direccionalidad.

1. REFERENTES BILBIOGRAFICOS

- **Libro: Biblioteca CDTI. TELECOMUNICACIONES. Tecnologías, redes y servicios. Ed. 1.** Huidobro Moya, José. Pág. 306.

- **Libro: Biblioteca CDTI. Ingeniería de Telecomunicaciones. Conceptos Básicos.** Restrepo Angulo Jairo. Pág. 227.

NETGRAFÍA

- **IPv4 - Estructura de Paquete**
  https://www.tutorialspoint.com/es/ipv4/ipv4_packet_structure.htm
- **VLSM y CIDR**
  https://sites.google.com/site/redesciscocnna/home/ccna-i/cap-6
- **Enrutamiento: Conceptos Fundamentales.**
  https://www.itesa.edu.mx/netacad/switching/course/module4/#4.0.1.1
  https://community.cisco.com/legacyfs/online/attachments/document/enrutamiento-conceptos_basicos.pdf
- **Configuración y conceptos básicos de switching**
  https://www.itesa.edu.mx/netacad/switching/course/module2/#2.0.1.1
- **Implementaciones de VLAN**
  https://www.itesa.edu.mx/netacad/switching/course/module3/#3.2.2.5

2. CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor (es)	CRISTIAN DELGADO	INSTRUCTOR	SENA VALLE CDTI	17 noviembre de 2020
	JUAN PABLO TOBAR	INSTRUCTOR	SENA VALLE CDTI	17 noviembre de 2020
	VICTOR M MOSQUERA	INSTRUCTOR	SENA VALLE CDTI	17 noviembre de 2020

3. CONTROL DE CAMBIOS (diligenciar únicamente si realiza ajustes a la guía)

	Nombre	Cargo	Dependencia	Fecha	Razón del Cambio

Autor (es)					