PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
CARRERA DE: INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

Trabajo de Titulación

Tema: Evaluación del uso de Cisco Discovery Protocol para mejorar la visibilidad de dispositivos en redes administradas con Simple Network Management Protocol

AUTOR:
Juan Gabriel Bustamante González

DIRECTOR:
Juan Francisco Chafla Altamirano

QUITO DM, JULIO DE 2025

DEDICATORIA

A mis padres, Franquito y Raquelita,

por enseñarme el valor del esfuerzo y del amor incondicional.

Por creer en mis sueños antes que yo mismo,

por brindarme sus manos cuando más lo necesité,

y por caminar a mi lado con paciencia, amor y guía.

Este logro es reflejo de su ejemplo,

y lleva en cada palabra la gratitud que les tengo.

AGRADECIMIENTO

A lo largo de este camino académico he contado con el apoyo incondicional de personas que han sido fundamentales para alcanzar esta meta. Hoy quiero expresar mi más profundo agradecimiento a mis hermanos por haberme apoyado y estar siempre pendientes de mí.

En especial, gracias a mis papis, Franquito y Raquelita, por su amor infinito, por ser mi guía constante y por brindarme la oportunidad de formarme académicamente. Gracias por su paciencia, por creer en mí aun en los momentos más difíciles, y por enseñarme con el ejemplo que el esfuerzo y el corazón llevan lejos. Este logro también es suyo, y lo llevo con orgullo.

A mis docentes y director, por todas las guías y enseñanzas brindadas, sin lugar a duda han sido de mucho valor para mí y las llevo siempre conmigo.

Y a mí mismo, por no rendirme, por levantarme cada vez que lo necesité, y por llegar hasta aquí con pasión y determinación.

¡Gracias a todos!

RESUMEN

Este proyecto analiza la implementación de Cisco Discovery Protocol (CDP) como complemento en redes gestionadas mediante el protocolo SNMP (Simple Network Management Protocol), con el objetivo de mejorar la visibilidad y administración de los dispositivos conectados. A través de entornos de prueba controlados, se evaluó cómo la incorporación de CDP permite obtener información más precisa, detallada y en tiempo real sobre la topología y estado de la red. Esta integración facilita la identificación de dispositivos, la resolución de incidencias y el monitoreo proactivo, elementos clave en una gestión de red eficiente. Los resultados evidencian que el uso combinado de SNMP y CDP proporciona una visión más completa de la infraestructura, lo que se traduce en una administración más ágil y robusta de los recursos de red.

CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

LISTA DE ABREVIATURAS

SNMP	*Simple Network Management Protocol* (Protocolo Simple de Administración de Redes).
CDP	*Cisco Discovery Protocol* (Protocolo de Descubrimiento de Cisco).
NMS	*Network Management Station* (Estación de Gestión de Red).
VACM	*View-based Access Control Model* (Modelo de Control de Acceso Basado en Vistas).
USM	*User-based Security Model* (Modelo de Seguridad Basado en Usuarios).
TTL	*Time To Live* (Tiempo de vida).
PoE	*Power over Ethernet* (Energía sobre el cable).
MAC	*Media Access Control* (Control de Acceso al Medio).
VLAN	*Virtual Local Area Network* (Red de Área Local Virtual).
SNAP	*Subnetwork Access Protocol* (Protocolo de Acceso a Subredes).
FCS	*Frame Check Sequence* (Secuencia de Verificación de Trama).
LLDP	*Link Layer Discovery Protocol* (Protocolo de Descubrimiento de Capa de Enlace).
OSI	*Open Systems Interconnection* (Interconexión de Sistemas Abiertos)
TCP/IP	*Transmission Control Protocol / Internet Protocol* (Protocolo de Control de Transmisión / Protocolo de Internet)
LAN	*Local Area Network* (Red de Área Local)
MAN	*Metropolitan Area Network* (Red de Área Metropolitana)
WAN	*Wide Area Network* (Red de Área Amplia)
ISO	*International Organization for Standardization* (Organización Internacional de Normalización)

CAPITULO 1: INTRODUCCION

Evaluación del uso de Cisco Discovery Protocol para mejorar la visibilidad de dispositivos en redes administradas con Simple Network Management Protocol.

1.1 JUSTIFICACION

La realización de una demostración práctica del uso combinado de Cisco Discovery Protocol (CDP) y Simple Network Management Protocol (SNMP) se justifica como una herramienta clave para mejorar la administración de redes complejas. Este estudio se sustenta en la necesidad de optimizar la visibilidad y el control sobre los dispositivos interconectados en redes dinámicas y críticas, especialmente en entornos corporativos y de telecomunicaciones donde una gestión eficiente puede prevenir fallos costosos (Network Working Group, 1990).

Los principales factores que respaldan la realización de esta demostración incluyen la importancia de proporcionar evidencia tangible sobre cómo CDP complementa a SNMP al ofrecer información detallada y en tiempo real de los dispositivos vecinos, como nombres de host, direcciones IP y configuraciones (Bhattarai, 2020). Esto permite un diagnóstico más preciso en escenarios de resolución de problemas y mejora la capacidad de mantener un inventario actualizado de la red. Además, al mostrar cómo CDP contribuye a identificar dispositivos mal configurados y optimizar la conectividad, se puede destacar su rol fundamental en la prevención de interrupciones operativas (Cisco Systems, 2015).

Por último, este estudio se sustenta en la creciente demanda de redes más seguras y robustas, donde herramientas como CDP y SNMP se convierten en pilares para garantizar la eficiencia en la administración. La demostración no solo fortalecerá el conocimiento técnico, sino que también proporcionará argumentos prácticos para implementar estas tecnologías en la gestión de redes.

1.2 PLANTEAMIENTO DEL PROBLEMA

Con el crecimiento de los sistemas informáticos y la latente necesidad de compartir la información dentro de los entornos empresariales, las redes de computadoras como medio de transmisión de los datos juegan un papel muy importante dentro una empresa; su correcto funcionamiento permite soportar una variedad de servicios -que cada vez van en aumento- dentro de una organización.

Siendo entonces que las redes se han convertido en una herramienta indispensable y crítica de trabajo, es muy importante su correcta operación para que garantice un adecuado flujo de datos y procesos de nuestro negocio. Para que una red funcione en óptimas condiciones es muy necesario contar con un buen diseño e implementación de la misma, pero no basta con eso, para asegurar ese buen funcionamiento a lo largo del tiempo se requiere también darle mantenimiento y sobre todo de una adecuada administración.

Las redes hoy en día son cada vez más populares y las podemos encontrar en casi cualquier industria, sin embargo, muchas empresas dejan de lado la administración y se enfrentan a diferentes problemas que no siempre se resuelven con el aumento del ancho de banda. Mediante la administración de la red podemos identificar problemas de diferente índole, que van desde los más básicos como dispositivos o interfaces apagadas, hasta los más complejos como latencias elevadas, cuellos de botella, bucles, etc. Por todo esto, hacer una buena administración de nuestra red es tan necesario como indispensable, sólo así se puede garantizar su buen funcionamiento que soporte la operación del negocio (Blog Altare | Tendencias Tecnológicas Y Digitalización, 2022).

Para la administración de redes existen varios protocolos en el mercado, en este trabajo nos enfocaremos en dos de los más utilizados, SNMP como protocolo genérico y CDP como protocolo propietario de Cisco.

¿Cómo contribuye el uso de CDP a mejorar la administración de una red gestionada con SNMP?

1.3 OBJETIVOS

1.3.1 GENERAL

- Evaluar el uso de Cisco Discovery Protocol para mejorar la visibilidad de dispositivos en redes administradas con Simple Network Management Protocol.

1.3.2 ESPECIFICOS

- Identificar las principales características de los protocolos CDP y SNMP.
- Analizar los beneficios de la integración de CDP en redes gestionadas con SNMP.
- Implementar un laboratorio de simulación que permita validar las ventajas del uso conjunto de ambos protocolos.

1.4 MARCO TEORICO Y CONCEPTUAL

1.4.1 MARCO TEORICO

La administración de redes es un campo fundamental en la ingeniería de telecomunicaciones, cuyo objetivo es garantizar el funcionamiento óptimo de una infraestructura de comunicación. Para ello, se utilizan protocolos especializados de gestión los cuales permiten monitorear dispositivos y recolectar información clave para la operación de la red.

Existen varios protocolos de administración de redes, SNMP y CDP son dos entre los más comunes. SNMP proporciona métricas de rendimiento en tiempo real y CDP mejora la identificación de dispositivos conectados.

1.4.2 MARCO CONCEPTUAL

- **Simple Network Management Protocol:** Es un protocolo de aplicación ampliamente utilizado en la administración de redes de datos. Su objetivo principal es facilitar la supervisión y gestión de dispositivos de red mediante la recopilación de información de su estado y funcionamiento.
- **Arquitectura de SNMP:** SNMP opera en una arquitectura cliente-servidor, donde los componentes clave son: El Agente SNMP, el NMS y la MIB (Network Working Group, 1990) (Network Working Group, 2002).
- **Versiones de SNMP:** Existen algunas versiones de SNMP, cada una con mejoras en cuanto a su funcionalidad, pero principalmente en cuanto a seguridad. Las versiones son: SNMPv1, SNMPv2c y SNMPv3 (Network Working Group, 2002) (Network Working Group, 2002) (Network Working Group, 2002).
- **Cisco Discovery Protocol:** Es un protocolo propietario y desarrollado por Cisco Systems que facilita el descubrimiento y la identificación de dispositivos Cisco dentro de su red. Su principal objetivo es proporcionar información detallada sobre los dispositivos vecinos, permitiendo a los administradores conocer la topología física y optimizar la operación de la red. CDP opera en la capa de Enlace de Datos por lo que no depende del direccionamiento IP para intercambiar información (Cisco Systems, 2004). CDP es una excelente herramienta para entornos Cisco, pero por su naturaleza propietaria su uso se ve limitado en redes con dispositivos de otras marcas (CCNADESDECERO.es, s.f.).

- **Administración de redes:** Son los métodos y protocolos utilizados para gestionar infraestructuras de comunicación.
- **Topología de red:** Estructura física y lógica de los dispositivos conectados.
- **Modelo OSI:** Capas de comunicación que permiten el funcionamiento de protocolos como CDP y SNMP.

1.5 ALCANCE

Este trabajo de titulación tiene como objetivo evaluar el impacto y los beneficios del uso de Cisco Discovery Protocol en una red gestionada con Simple Network Management Protocol. Para tal efecto se realizará una simulación práctica con Cisco Packet Tracer y PRTG Network Monitor, aplicativos gratuitos que nos permitirán visualizar la información obtenida del monitoreo de dispositivos mediante SNMP, así como la identificación y descubrimiento de dispositivos Cisco con CDP. Esta demostración será realizada con una red de área local con topología de estrella extendida, la cual nos permitirá configurar ambos protocolos y evidenciar su funcionamiento. Está fuera del alcance de este trabajo, configuraciones avanzadas y de seguridad, así como el uso de otras plataformas de monitoreo distintas a las mencionadas.

CAPITULO 2: TEORIA DE NETWORKING

En la era digital, las redes de comunicación se han convertido en uno de los pilares más importantes de la conectividad global. La capacidad de intercambiar información de manera eficiente y segura es esencial para la operación de sistemas informáticos, aplicaciones empresariales y el acceso a servicios en línea.

A lo largo de este capítulo se explora los conceptos esenciales de las redes de comunicación, abarcando los principios básicos de infraestructura y transmisión de datos. Se explorará el modelo OSI (Open Systems Interconnection), una referencia teórica que organiza la comunicación en siete capas, facilitando el diseño y comprensión de los protocolos de red. Asimismo, se abordará el modelo TCP/IP (Transmission Control Protocol / Internet Protocol), el cual define el conjunto de reglas que rigen el intercambio de información en Internet y otras redes.

A través de este capítulo, se establecerán los cimientos base requeridos para comprender el modo de trabajo de las redes modernas y su papel en la conectividad global, preparando el terreno para un análisis más profundo en secciones posteriores.

2.1 Uso de las Redes de Computadoras.

Con el nacimiento de las computadoras en la década de los 70s y su llegada a hogares y oficinas en diversas partes del mundo, también surgió una nueva era de la información: la era digital. Gracias a sus numerosas ventajas, esta modalidad fue ganando terreno frente a los medios tradicionales, como el papel, hasta convertirse en la norma.

El manejo digital de la información transformó el entorno laboral, permitiendo que los empleados contaran con computadoras asignadas para sus tareas. En lugar de transportar hojas de papel y carpetas pesadas, podían almacenar toda su información en sus dispositivos sin el riesgo de olvidar o perder documentos importantes. Esta

comodidad favoreció la autonomía y la eficiencia, beneficiando tanto a los empleados como a las organizaciones.

Sin embargo, no todo fue perfecto. Al necesitar imprimir un documento, los empleados sin acceso directo a una impresora debían transferir el archivo a un disquete, copiarlo o abrirlo en dicha computadora y finalmente imprimirlo. Asimismo, cuando un funcionario modificaba un archivo y quería compartirlo con otros empleados, debía copiarlo y distribuirlo manualmente, equipo por equipo. Esto generaba duplicidad de documentos, costos adicionales y una mayor dificultad para consolidar cambios realizados por distintas personas, aumentando el riesgo de pérdida de información. Este aislamiento en cierta manera complicaba el trabajo colaborativo entre los empleados.

Ante estos desafíos, surgió la necesidad de una solución que permita mejorar la comunicación dentro de las empresas, pero de una manera más eficiente. Se buscaban alternativas que permitieran:

- Evitar la duplicación de equipamiento e información.
- Facilitar la comunicación efectiva, reduciendo tiempo y costos.

La primera respuesta a estos problemas fue la interconexión de equipos compartidos, comenzando con impresoras en red. Al permitir que varios empleados accedieran a un mismo dispositivo, las empresas lograron reducir gastos, evitando la necesidad de comprar una impresora para cada trabajador. Estos primeros esfuerzos marcaron el nacimiento de las redes de información.

Durante la década de los 80, las computadoras se volvieron cada vez más populares, lo que impulsó la creación de las primeras redes de equipos. Sin un estándar definido, estas redes eran diseñadas de manera independiente por distintos fabricantes, enfocándose únicamente en satisfacer las necesidades específicas de cada empresa. Como resultado, muchas tecnologías de red eran incompatibles entre sí, lo que dificultaba la

comunicación y obligaba a las empresas a reemplazar sus equipos para mantener la conectividad. Esto representaba un alto costo, haciendo evidente la necesidad de una estandarización del software y hardware de redes.

Para abordar este problema, se establecieron los primeros estándares para redes de área local (LAN, Local Area Network), ofreciendo pautas de diseño que permitían la interconexión de dispositivos de distintos fabricantes dentro de una misma red. Estos estándares facilitaron la instalación y expansión de redes empresariales.

Con el crecimiento de las compañías y el uso masivo de computadoras, pronto se evidenció que las LAN eran insuficientes. Ya no sólo se necesitaba compartir información dentro de un mismo edificio, sino también entre sucursales ubicadas en distintas regiones. Para solucionar esto, se desarrollaron redes de área metropolitana (MAN, Metropolitan Area Network) y redes de área amplia (WAN, Wide Area Network), extendiendo la conectividad a mayores distancias y permitiendo la comunicación eficiente entre empresas.

Dado que las redes crecían en tamaño y complejidad, fue necesario establecer un enfoque estructurado para su diseño: así nació el concepto de Arquitectura de Red. Este se refiere a la organización lógica y física que permite que una red funcione correctamente y pueda expandirse con eficiencia. Dicha arquitectura contempla elementos clave como la disposición de sus nodos (topología), los canales por los que fluyen los datos, y los protocolos que rigen la interacción entre los diferentes dispositivos conectados.

2.1.1 Topologías de Redes

La topología de red es la forma en la cual los dispositivos están interconectados entre sí dentro de una red, dando lugar o creando las posibles rutas para la transmisión de los datos.

Existen dos tipos de topologías, física y lógica. La topología física se refiere a la disposición física de los dispositivos de red, es la estructura visible o forma en que los equipos están conectados mediante cables o medios inalámbricos; por su parte la topología lógica establece cómo interactúan los dispositivos en la red y cómo se transmiten los datos dentro de ella.

Las topologías lógicas no se ven a simple vista, se puede decir que son virtuales y dependen de los protocolos de comunicación que se utilicen. Entre las más comunes tenemos:

- Ethernet.
- Redes conmutadas.

Las topologías físicas son visibles por sus cables, aunque también pueden usar medios inalámbricos. Entre las más comunes tenemos:

- Bus.
- Anillo.
- Estrella.
- Estrella extendida.
- Jerárquica.
- Malla.

2.1.1.1 Topología en Bus

Este esquema conecta todos los dispositivos de forma lineal a través de un solo cable, existen terminales que van al inicio y fin de la línea de comunicación y la información viaja de equipo en equipo.

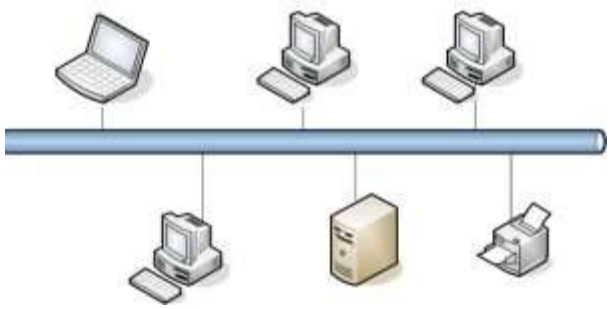


Figura 1. Topología en Bus. Tomado de (FMUSER International Group INC., 2021)

2.1.1.2 Topología en Anillo

La topología en anillo establece una conexión entre los dispositivos formando un circuito cerrado, donde cada nodo está vinculado con sus dos vecinos inmediatos. Esta configuración no posee un inicio o final definidos. La información circula en una única dirección, recorriendo secuencialmente cada punto de la red hasta llegar al destinatario, quien será el que extraiga su contenido.

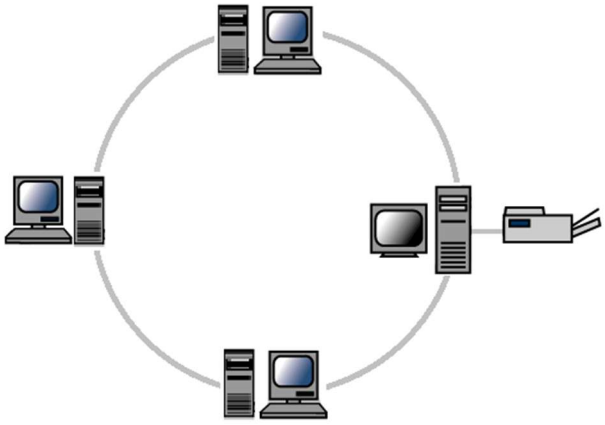


Figura 2. Topología en Anillo. Tomado de (ESCUELA DE EDUCACIÓN TÉCNICA NUMERO 2 LANUS, s.f.)

2.1.1.3 Topología en Estrella y Estrella Extendida

La topología en estrella es la más utilizada en las LAN. Esta topología similar a los radios de una rueda de bicicleta tiene un equipo central al cual se conectan de forma directa cada uno de los dispositivos, el equipo central puede ser un router, switch o hub que cumple un rol de concentrador de todas las conexiones.

Si bien la implementación de una red con topología en estrella puede resultar en costos mayores, sus ventajas justifican ese costo extra, pues al tener cada host conectado al equipo central, nos brinda una mayor confiabilidad de la red. En el supuesto caso de que un host falle, será el único aislado de la red, mientras que los demás dispositivos seguirán conectados y la red podrá continuar operando.

Otra ventaja de esta topología es la seguridad, ya que, al tener un dispositivo concentrador, se puede también centralizar la seguridad para acceder a la red.

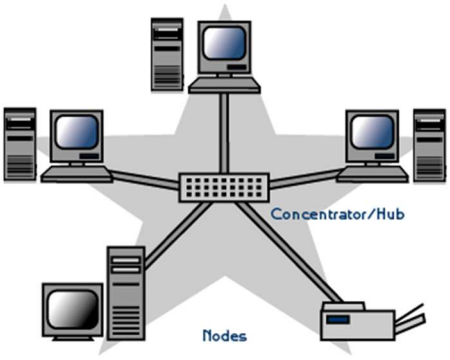


Figura 3. Topología en Estrella. Tomado de (ESCUELA DE EDUCACIÓN TÉCNICA NUMERO 2 LANUS, s.f.)

Cuando crece la red y se requiere conectar más equipos, se agrega otro equipo concentrador que irá conectado al principal, dando lugar a la topología en estrella extendida.

2.1.1.4 Topología Jerárquica

La topología jerárquica organiza los dispositivos en niveles o capas, dando forma a una estructura con forma de árbol donde sus ramales se van bifurcando a medida que aumentan los niveles. Esta topología se basa en una jerarquía donde cada nivel tiene una función específica dentro de la red.

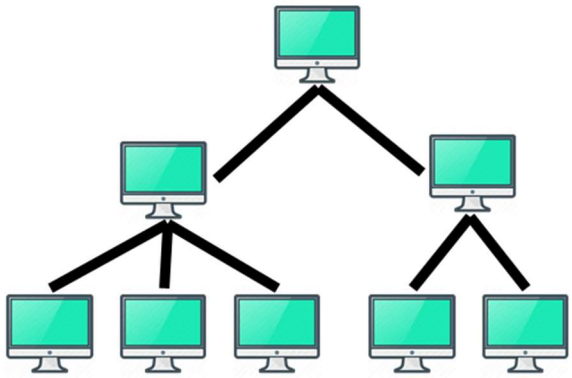


Figura 4. Topología Jerárquica. Tomado de (Arciniega, 2023)

2.1.1.5 Topología en Malla

Esta topología busca reducir fallas de conexión a través de la redundancia, para ello realiza una conexión de todos los dispositivos entre sí y si un enlace falla hay otros que dan continuidad a la operación de la red. Esta topología, aunque tiene su principal ventaja de ser redundante, puede resultar bastante costosa.

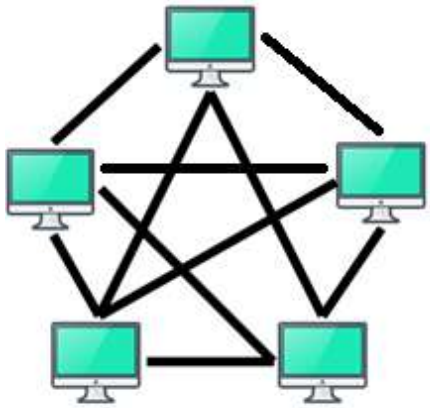


Figura 5. Topología en Malla. Adaptado de (Arciniega, 2023)

2.1.1.6 Topología Lógica

La topología lógica de red hace referencia a la forma como los hosts se comunican entre sí a través del medio. Se clasifican en dos grandes grupos, por difusión y por transmisión de testigos.

En la topología de difusión, todos los dispositivos conectados hacen uso de un único medio compartido para transmitir datos. Cuando uno de ellos emite información, esta se dispersa por todo el canal, siendo accesible por todos los nodos, sin requerir

enlaces punto a punto entre ellos. Es un enfoque donde el mensaje viaja como un anuncio público: lo escucha quien lo necesite.

La transmisión mediante testigo es un método de control de acceso en redes, donde un token electrónico circula ordenadamente entre los dispositivos conectados. Solo el nodo que posee el testigo en ese momento tiene permiso para transmitir datos. Si no tiene nada que enviar, simplemente lo pasa al siguiente en la secuencia, manteniendo así el orden y evitando colisiones. Esta técnica es utilizada en tecnologías como Token Ring y FDDI, que además comparten una configuración física basada en un anillo cerrado.

2.1.2 Conexión Física

Un componente esencial en el diseño de una red es la elección de los medios por los cuales viajarán los datos. Entre las opciones más utilizadas se encuentran el cable de par trenzado (en su versión estándar y blindada), la fibra óptica y el cable coaxial, cada uno con características propias que influyen en el rendimiento, alcance y nivel de interferencia que pueden manejar.

2.1.2.1 Cable de par trenzado

El cable de pares trenzados es un cable de cuatro pares de cables de cobre, los cuales están trenzados entre sí. Es el medio más utilizado para el cableado de las redes modernas, a diferencia de otros, éste tiene mayor facilidad para su instalación y sus costos son muy accesibles.

Este cable se compone de cuatro hilos de cables que están trenzados entre sí con el propósito de reducir la interferencia electromagnética y mejorar la transmisión de datos. Cuando un cable transporta corriente, genera un campo electromagnético alrededor de él, y si varios cables estuvieran dispuestos en paralelo, este campo se intensificaría, causando interferencias. Trenzar los cables permite que el campo electromagnético generado por cada cable vaya en direcciones opuestas, haciendo que esa interferencia se neutralice.

2.1.2.1.1 Cable de par trenzado blindado (STP)

El cable (STP, Shielded Twisted Pair) es un cable que posee una fina lámina metálica cubriendo a cada par de cables, luego alrededor de los cuatro pares hay otra lámina y finalmente lo envuelve una cubierta plástica. Todo este recubrimiento le brinda mayor robustez para instalaciones en exteriores y también añade cierta resistencia a interferencias externas.

Existe una variante que es el cable apantallado (ScTP, Screened Twisted Pair), este cable es un tanto más ligero que el STP, posee el recubrimiento externo que envuelve a todos los cables, pero no tiene el recubrimiento interno que envuelve a cada par de cables trenzados.

Aunque estos tipos de cables poseen ventajas debido a su tiempo de vida útil y a su protección contra interferencias, su instalación y costos son más elevados.

Figura 6. Cable STP. Tomado de (www.blogspot.com, 2015)

2.1.2.1.2 Cable de par trenzado sin blindar (UTP)

El cable (UTP, Unshielded Twisted Pair), es el medio de red más común, a diferencia de los cables blindados, únicamente consta de cuatro pares de hilos de cobre cubiertos por aislantes plásticos codificados por colores y trenzados entre sí, y finalmente envueltos por una cubierta plástica exterior.

El cable UTP tiene muchas ventajas, posee un diámetro pequeño, más sencillo de instalar, menor uso de espacio y un coste mucho menor que otros tipos de medios, razones por las cuales se ha convertido en el tipo de cable mayormente utilizado.

2.1.2.2 Cable coaxial

El cable coaxial, mayormente conocido por su uso en las instalaciones de televisión pagada, es un medio con cuatro componentes:

- Recubrimiento exterior.
- Pantalla de cobre trenzada.
- Aislante de plástico.
- Conductor interior.

El núcleo o centro del cable es un conductor sólido de cobre al cual le rodea una capa aislante de plástico flexible. Luego, sobre la capa aislante se encuentra una malla de metal trenzado (cobre o aluminio) que protege la señal de interferencias externas y sirve como conexión a tierra. Finalmente, sobre la malla se coloca un recubrimiento que brinda protección exterior al cable.

Este cable utiliza un conector denominado BNC abreviatura de British Naval Connector, por su largo alcance ha sido muy común en instalaciones de corta y mediana distancia, aunque por su difícil instalación no ha tenido mucha acogida para lugares pequeños.

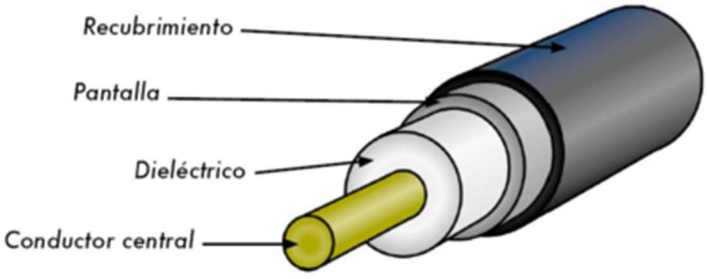


Figura 7. Cable Coaxial. Tomado de (Creative Commons, 2009)

2.1.2.3 Fibra óptica

El cable de fibra óptica es un medio de red que utiliza luz para la transmisión de datos. Las señales o datos son pulsos de luz que viajan desde el emisor hasta el receptor a través del vidrio, material del que está compuesta la fibra óptica. Para que los pulsos de

luz puedan ser enviados y recibidos, se necesita de dispositivos eléctricos emisores y receptores.

La fibra óptica está compuesta por varias capas diseñadas para proteger y optimizar la transmisión de datos mediante luz. Sus principales componentes son:

- Núcleo. Es el material a través del cual viaja la luz, y por ende el más importante, pues debe estar en óptimas condiciones para garantizar su buen funcionamiento. Está fabricado con una combinación de sílice principalmente junto con otros elementos.
- Revestimiento. Este material, hecho igualmente a base de sílice, pero con un índice de refracción más elevado, cumple una función crucial: guía la luz dentro de la fibra mediante reflexiones internas continuas. Gracias a este fenómeno, los pulsos luminosos que transportan la información se desplazan a lo largo del cable hasta su destino final.
- Protector. Material de plástico que protege la fibra de impactos y tensiones mecánicas.
- Cubierta. Hecha de materiales como PVC o polietileno, encargada de proteger al cable de factores externos como humedad y temperatura.
- Refuerzo externo. Capa externa para mejorar la resistencia y durabilidad del cable, a menudo se hace con fibras de aramida (Kevlar), material con el que se elaboran los chalecos antibalas.

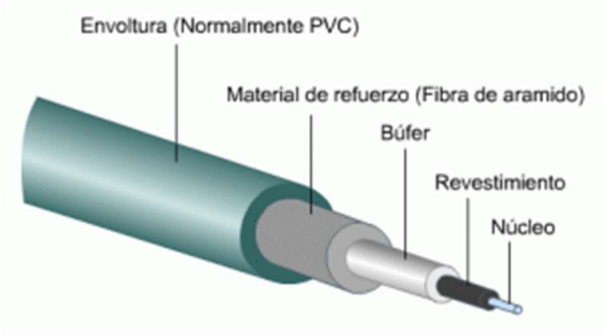


Figura 8. Cable de Fibra Óptica. Tomado de (Bilbao, 2015)

La luz viaja a través del núcleo de la fibra, pero solo puede hacerlo si ingresa con un ángulo específico que permita su propagación mediante reflexiones en las paredes del revestimiento. Este fenómeno, conocido como reflexión interna total, garantiza que la señal llegue al otro extremo del cable sin desviarse.

Cuando la luz ingresa en el interior de la fibra óptica, su recorrido está determinado por ciertas trayectorias específicas conocidas como modos. Si el núcleo de la fibra posee un diámetro amplio, permite que la señal se propague a través de varios caminos posibles, lo que caracteriza a las fibras multimodo. En contraste, un núcleo más delgado restringe el avance de la luz a una sola ruta, lo que define a las fibras monomodo.

2.1.3 Conexión lógica

La conexión lógica establece la forma en la cual los dispositivos pueden comunicarse. Para llevar a cabo esta comunicación se utilizan los protocolos de red, los cuales vienen a ser el lenguaje con el que los dispositivos pueden comunicarse. Sin protocolos, la comunicación ni la transmisión de datos sería posible.

Los protocolos son quienes dan los parámetros necesarios para la comunicación de datos. Determinan cómo se crea una red, cómo deben conectarse las computadoras, establecen el formato con el cual deben transmitirse los datos y también cómo se envían. Todas estas reglas son implementadas y administradas por diferentes organizaciones con alcance internacional:

- IEEE. Instituto de ingenieros eléctricos y electrónicos.
- ANSI. Instituto nacional americano de normalización.
- TIA. Asociación de la industria de las telecomunicaciones.
- ITU. Unión internacional de las telecomunicaciones, antes conocido como CCITT – Comité de consultoría internacional para telefonía y telegrafía.

Para que esta comunicación lógica sea posible, los protocolos hacen uso de las direcciones IP, que será el principio de operación de las redes de información.

2.2 Direccionamiento IP

Al hablar de una red sabemos que existe una determinada cantidad de dispositivos interconectados, algunas redes podrán ser pequeñas y con pocos equipos, pero también habrá otras más grandes y con muchos o muchísimos equipos, cada uno con un propósito y necesidad de comunicarse. Para que la comunicación pueda darse es necesario que los equipos se localicen e identifiquen entre sí, y para esto hacen uso de las direcciones IP. Las direcciones IP tienen dos partes, la primera parte es el identificador de red o subred y la segunda parte identifica al host o dispositivo.

Una dirección IP versión 4 se encuentra formada por 4 números separados por puntos, los números pueden ser entre el 0 y el 255 y también son conocidos como octetos, ejemplo 192.168.0.1.

Dependiendo del tamaño de las compañías, habrá casos de empresas grandes que requieran redes muy extensas y que soporten gran cantidad de equipos conectados, o así mismo empresas chicas con redes de menor tamaño y con poca concentración de equipos conectados en red.

Es aquí donde el direccionamiento IP se vuelve muy importante y es cuando empezamos a diseñar la red con las direcciones IP, repartiendo mayor capacidad al identificador de red o al identificador de host según sea nuestra necesidad. Este abanico

de posibilidades nos da lugar a las clases de redes, que de acuerdo con su tamaño pueden ser pequeñas, medianas o grandes, y se clasifican en clase A, clase B, clase C, clase D y clase E.

Figura 9. Clases de Redes. Tomado de (Ortiz, s.f.)

2.2.1 Clases de Redes

Dentro del sistema de direccionamiento IPv4, las clases de red actúan como una forma de segmentar el espacio de direcciones, determinando cuántos bits están destinados a identificar la red y cuántos al dispositivo dentro de ella. Esta clasificación permite adaptar el rango de direcciones según la escala y necesidades específicas de cada red, ya sea pequeña, mediana o extensa.

2.2.1.1 Direcciones clase A

Las direcciones de clase A están destinadas a infraestructuras de gran escala, capaces de soportar un número elevado de dispositivos conectados. En este tipo de direcciones, el primer octeto se utiliza para identificar la red, mientras que los tres octetos restantes se reservan para distinguir a los distintos hosts dentro de ella.

2.2.1.2 Direcciones clase B

Las direcciones clase B fueron diseñadas para redes de tamaño mediano a grande, capaces de manejar un buen número de dispositivos, utilizan 2 octetos para identificar la red y 2 octetos para identificar el host.

2.2.1.3 Direcciones clase C

Siendo las más comunes, las direcciones clase C son utilizadas para manejar redes con una pequeña cantidad de dispositivos, poseen 3 octetos correspondientes a red y 1 octeto correspondiente a host.

2.2.1.4 Direcciones clase D

Las direcciones de clase D fueron concebidas para facilitar la entrega simultánea de información a múltiples dispositivos dentro de una red, a través de un mecanismo conocido como difusión. Este tipo de dirección no identifica a un solo equipo, sino a un conjunto específico, permitiendo que un único host envíe datos a varios destinatarios a la vez, sin necesidad de establecer conexiones individuales con cada uno.

2.2.1.5 Direcciones clase E

Este grupo de direcciones IP son reservadas por la IETF (Grupo de ingeniería de Internet) para investigación. Estas redes, tendrán entre 240 y 255 en su octeto inicial.

2.2.1.6 Direcciones IP Públicas y Privadas

Internet es una gran red de redes, y su estabilidad y funcionamiento depende del correcto manejo del direccionamiento IP. Ese correcto manejo requiere de algún método que garantice que las direcciones IP sean únicas y no exista duplicidad, esta tarea la realiza la IANA Internet Assigned Numbers Authority.

Debido a la propagación del internet y el aumento de dispositivos conectados, las direcciones IP disponibles se han ocupado hasta casi agotarse, por lo cual se han desarrollado algunos mecanismos para atenuar este agotamiento.

Una de las soluciones desarrolladas para optimizar el uso de direcciones IP fue la implementación de IP privadas. Dado que los dispositivos suelen conectarse a Internet mediante un equipo de frontera, como un router o un firewall, se establece un límite entre la red WAN de Internet y la red LAN interna.

Aunque en Internet cada dispositivo debe contar con una dirección IP única, dentro de una LAN es posible utilizar un esquema de direccionamiento independiente. Esto se debe a que LAN y WAN son redes diferentes, lo que permite asignar distintos tipos de direcciones en cada interfaz del router, facilitando la administración de la red y reforzando la seguridad.

Ahora bien, aunque técnicamente es posible asignar cualquier dirección IP dentro del segmento LAN del router, esto no es recomendable. Si la dirección utilizada está también en Internet, podría generar conflictos y confusión en el dispositivo, dificultando su capacidad para determinar a qué red debe conectarse.

Por ello, se han reservado tres rangos de direcciones IP (uno para cada clase) para su uso exclusivo como direcciones privadas. Estas direcciones no son enrutables en Internet, lo que evita interferencias y se permite su uso y asignación conforme sea requerido.

Tabla 1. Direcciones IP Privadas

Clases de Direcciones IP	**Rango de redes privadas**
Clase A	10.0.0.0 hasta 10.255.255.255
Clase B	172.16.0.0 hasta 172.31.255.255
Clase C	192.168.0.0 hasta 192.168.255.255

Nota: Esquema de direcciones IP privadas.

La conexión de una LAN a Internet requiere de la conversión de las direcciones privadas a direcciones públicas. Este proceso se denomina Conversión de direcciones de red (NAT, Network Address Translation).

2.3 Tipos de Redes

Existen tres tipos de redes, redes de área local (LAN), redes de área metropolitana y redes de área amplia (WAN).

2.3.1 Redes de área local (LAN)

Las redes de área local son redes de tamaño pequeño o local, entendiéndose por tamaño pequeño a un espacio geográfico reducido, mas no a un reducido número de dispositivos.

Estas redes utilizadas tanto en casas como oficinas permiten la instalación de dispositivos locales, brindando servicios desde compartición de equipos, como impresoras y escáneres, hasta almacenamiento de información y servicios de comunicación como telefonía IP.

Las redes de área local fueron pensadas para hacer lo siguiente:

- Trabajar en una zona de espacio reducido.
- Permitir el acceso a los recursos de red a muchos usuarios.
- Brindar conectividad a tiempo completo con los servicios locales.

2.3.2 Redes de área metropolitana (MAN)

Estas redes son más grandes que las LAN y pueden cubrir una zona más amplia como una ciudad, por ejemplo. Este tipo de redes interconectan redes LAN separadas por una distancia considerable, pero que se encuentran dentro de un territorio cercano. Para el enlace entre las diferentes LAN que pueden formar la MAN, comúnmente se utiliza la fibra óptica o los enlaces de radiofrecuencia.

Un ejemplo de una red MAN podría ser un banco con sus distintas sucursales, ubicados todos dentro de una misma ciudad.

2.3.3 Redes de área amplia (WAN)

Las redes de área amplia interconectan las redes locales, proporcionando acceso a dispositivos muy distantes. Este tipo de redes es mayormente utilizado por las empresas cuando se requieren conectar oficinas geográficamente distantes como es la interconexión entre oficinas en diferentes ciudades o países, por ejemplo.

Las redes amplias fueron pensadas para operar en los siguientes escenarios:

- Trabajan en áreas geográficamente lejanas.
- Permitir interacción en vivo a distancias grandes.
- Brindar acceso a servicios/recursos remotos.
- Ofrecer servicios de gran escala como: correo electrónico, Internet y comercio electrónico.

Diferencias entre las LAN, MAN, y WAN:

- Las MAN interconectan usuarios que se encuentran a distancias mayores que las de una LAN, pero menores que una WAN.
- Las MAN interconectan redes dentro de un perímetro urbano, creando una red más grande que posteriormente podría convertirse en una WAN.
- El ancho de banda que posee una red local es por lo general mayor al de una red metropolitana o amplia, salvo casos donde se utilice fibra óptica con velocidades muy elevadas.

2.4 El Modelo OSI

El desarrollo de las LAN, MAN y WAN desde sus inicios presentó múltiples desafíos. Durante la década de los 80, la popularidad y uso de las redes aumentaron

significativamente, a medida que las empresas descubrían que su implementación les permitía optimizar recursos y mejorar la productividad.

Sin embargo, el crecimiento acelerado también trajo consigo problemas como la incompatibilidad entre dispositivos, lo que dificultaba la comunicación entre equipos de distintos fabricantes. Fue entonces cuando las grandes compañías se dieron cuenta de que depender de tecnologías no estandarizadas no era la mejor solución. En su lugar, necesitaban un sistema universal que permitiera la conexión eficiente de todos los dispositivos, sin importar su origen o fabricante.

Frente a la urgencia de establecer reglas unificadas, la ISO (Organización Internacional de Normalización) llevó a cabo un análisis de los modelos de red ya existentes, con la finalidad de proponer estándares que promovieran la conexión fluida y la compatibilidad entre distintos sistemas y dispositivos tecnológicos

Producto de esto, en 1984 la ISO creó el modelo OSI, compuesto por siete capas que detallan todos los procesos necesarios para la transmisión y recepción de datos en una red. El modelo define con precisión las funciones de cada capa, lo que permite comprender mejor cómo viaja la información y visualizar su transformación hasta convertirse en bits que atraviesan el medio de transmisión, llegando al dispositivo de destino para volver a interpretarse como información útil.

La división en capas aporta diversos beneficios, entre ellos:

- Interoperabilidad: Hace posible que dispositivos de distintes marcas se puedan comunicar entre sí sin problemas.
- Estandarización: Facilita el desarrollo tecnológico sin preocuparse por incompatibilidades.
- Modularidad: Los procesos realizados en una capa no afectan a las demás, dándole cierta autonomía.

- Comprensión estructurada: Divide el proceso de comunicación en partes más manejables, facilitando su estudio y diagnóstico.

El modelo OSI consta de siete capas numeradas, cada una con una función en particular, obedeciendo las siguientes normas:

- Una capa cualquiera utiliza los servicios de la capa inferior y proporciona servicios a la capa superior.
- Cada capa del computador emisor interactúa con su capa similar en el computador receptor enviando el mensaje a través de las capas inferiores.
- Los datos en la computadora origen se van traspasando capa por capa desde la superior hasta llegar a la inferior, convirtiéndose en bits para la transmisión, luego al llegar al computador receptor se ejecuta el proceso inverso, donde las capas desde la inferior a la superior transforman los bits recibidos en datos. Esta comunicación de capa a capa se denomina igual a igual.
- En cada capa, conforme se hace la transformación de datos a bits, se agrega al mensaje un formato de control conocido como Encabezado, mediante los cuales el computador receptor conoce el origen y destino de la información enviada. Luego de recibir los bits, se retiran los encabezados y se transforman nuevamente en datos. A este proceso se lo denomina Encapsulamiento.
- Cada capa posee su propia unidad de información, diferente en nombre y estructura, conocida como PDU (Protocol Data Unit) por sus siglas en inglés. (Stallings, 2000)

Las capas que conforman el modelo OSI son:

Tabla 2. El Modelo OSI

CAPA	NOMBRE	FUNCIONES	PDU
7	Aplicación	Recibe los datos de la capa de presentación y los transforma a un formato legible para las diferentes aplicaciones.	Dato
6	Presentación	Actúa como un intérprete entre la capa de aplicación y las capas inferiores, asegurando que los datos que se envían desde una aplicación puedan ser entendidos por la aplicación del receptor.	Dato
5	Sesión	Se encarga de establecer, mantener y finalizar las sesiones de comunicación entre aplicaciones ubicadas en diferentes dispositivos.	Dato
4	Transporte	Agrupa los paquetes en segmentos y se encarga de verificar que el transporte de datos no contenga errores.	Segmento
3	Red	Se encarga de "convertir" las tramas en paquetes para luego enrutarlos hacia el destino.	Paquete
2	Enlace de Datos	A partir de los Bits crea la Trama, y además se encarga del control de flujo y errores mediante la FCS.	Trama
1	Física	Define reglas para acceso al medio y hace posible la transmisión.	Bit

Nota: Las 7 capas del modelo OSI

2.4.1 Capa Física

La capa física es quien se encarga de las conexiones físicas de la computadora hacia la red, permite el acceso al medio. Es aquí donde se controla niveles de voltaje, distancias máximas de transmisión y todo lo relacionado a la conexión física como tal. La capa física se encarga de transmitir los bits de información a través del medio desde el equipo emisor hacia el receptor.

2.4.2 Capa de Enlace de Datos

La capa de enlace de datos garantiza una transmisión confiable de información entre dispositivos conectados directamente. Sus responsabilidades incluyen gestión del direccionamiento físico, reglar como acceden los equipos a la red, notificación cuando hay errores y distribución ordenada de tramas. También tiene la tarea de construir, reconocer y gestionar las tramas que transportan los datos. Si se presentan fallas como duplicaciones, pérdidas o daños en las tramas, esta capa interviene para corregirlas. Incluso puede ajustar la velocidad de transmisión para evitar que un dispositivo más lento se vea sobrepasado por uno más rápido.

2.4.3 Capa de Red

La capa de red tiene la responsabilidad de transportar los datos desde el dispositivo emisor hasta el receptor, sin importar la distancia física que los separe. Para lograr este objetivo, se apoya en dispositivos como los routers, que analizan las posibles rutas disponibles y seleccionan el camino más adecuado para encaminar la información hacia su destino final.

2.4.4 Capa de Transporte

La capa de transporte actúa como el encargado logístico de los datos: divide la información proveniente de las capas superiores en segmentos, los entrega a la capa de

red para su envío físico, y luego, al llegar al destino, reensambla esas piezas para que las capas de sesión, presentación y aplicación puedan interpretarlas correctamente.

Mientras que las capas superiores se centran en la interacción directa con el usuario y las aplicaciones, la capa de transporte y las tres inferiores se especializan en llevar los datos a través de la infraestructura de red. En este nivel, se establece un trayecto virtual entre los dos dispositivos involucrados, un canal temporal por el cual se mueven los datos que, una vez finalizado el envío, se desactiva.

Para asegurar que la información llegue íntegra y sin errores, la capa de transporte implementa mecanismos de control que detectan y corrigen fallos que puedan surgir durante la transmisión.

2.4.5 Capa de Sesión

La capa de sesión se encarga de crear y gestionar el canal de comunicación entre dos dispositivos que están intercambiando información. Su función principal es iniciar la sesión, mantenerla activa durante el intercambio de datos y finalizarla correctamente una vez concluido el proceso. Además de ofrecer soporte directo a la capa de presentación, esta capa se ocupa de coordinar el flujo del diálogo entre ambos extremos, garantizando una transmisión ordenada y estructurada.

2.4.6 Capa de Presentación

La capa de presentación actúa como un puente entre los sistemas de origen y destino, garantizando que los datos enviados por la capa de aplicación de un dispositivo sean comprensibles para la aplicación del otro. Su papel se asemeja al de un traductor digital: adapta y transforma los distintos formatos de datos a una estructura común. Además, es la responsable de aplicar procesos de cifrado para proteger la información durante la transmisión y de descifrarla al llegar a su destino.

2.4.7 Capa de Aplicación

La capa de aplicación representa el punto de encuentro entre el usuario y los servicios de red. Es en este nivel donde se gestionan tareas como el acceso a archivos, su impresión y otras funciones vinculadas directamente con las necesidades del usuario. Además, esta capa coordina los mecanismos que garantizan la integridad de los datos y establece protocolos para la detección y recuperación ante posibles errores, asegurando una interacción eficiente y confiable con la red.

2.5 El Modelo TCP/IP

Creado por el departamento de defensa de los Estados Unidos, este modelo surgió de la necesidad de comunicación entre puntos muy distantes, para lo cual los datos debían pasar por diferentes tipos de tecnologías como: cables, enlaces microondas, fibras ópticas e inclusive enlaces satelitales.

Para el departamento de defensa era necesario la transmisión inmediata de los datos independientemente de la condición de cualquier nodo o red. Debido a que la transmisión se podía dar en cualquier momento y bajo cualquier condición, se requería del diseño de un modelo que sea seguro y rápido.

Se diseña entonces el modelo TCP/IP el cual posee cuatro capas: Capa de Acceso a la Red, Capa de Internet, Capa de Transporte y Capa de Aplicación.

Pese a que el nombre de algunas capas del modelo OSI tiene semejanza con el nombre de las capas que conforman modelo TCP/IP es necesario distinguir sus funciones y no confundirse. Dado que el número de capas varía entre ambos modelos, las funciones asignadas a la capa 2 en el modelo OSI no necesariamente coinciden con las que desempeña la capa 2 en el modelo TCP/IP. Esto se debe a que en TCP/IP algunas funciones están agrupadas de forma diferente, lo que puede generar diferencias en sus

funciones por capa. Por ejemplo, el direccionamiento IP se encuentra en la capa 3 del modelo OSI, pero para el modelo TCP/IP sería a la capa 2.

2.5.1 Capa de Acceso a la Red

En esta capa se realizan las tareas necesarias para que un paquete IP pueda entrar en la red, ya sea una LAN, MAN o WAN. Para ello, la capa de acceso determina cómo se establecerá la conexión con el medio físico de transmisión, en función del tipo de hardware presente en la interfaz de red

Entre las funciones principales de la capa de acceso a la red se encuentran la asociación de direcciones IP con direcciones MAC, así como el encapsulamiento de los paquetes IP dentro de tramas adecuadas para su transmisión a través del medio físico.

2.5.2 Capa de Internet

El propósito de la capa Internet es el de poder enviar paquetes desde y hacia un dispositivo, para lo cual se vale de los protocolos de enrutamiento. En la capa de Internet se determina la mejor ruta y la conmutación de paquetes.

Funciones del protocolo IP:

- Definir un esquema de direccionamiento para un paquete que va a ser enviado.
- Facilitar el intercambio de datos entre la capa de Internet y la capa de Acceso a red.
- Encaminar los paquetes hacia los hosts remotos.

2.5.3 Capa de Transporte

La capa de transporte se encarga de ofrecer servicios de comunicación extremo a extremo entre el equipo emisor y el receptor, estableciendo una conexión lógica entre

ambos. En esta capa, los datos se segmentan para su envío y se reensamblan al llegar a destino, garantizando una transmisión ordenada y eficiente.

Entre los protocolos que operan en esta capa destacan TCP, que es orientado a conexión y proporciona mecanismos de control como ventanas deslizantes, numeración de secuencia y acuses de recibo para asegurar la entrega confiable; y UDP, que al ser no orientado a conexión, permite una transmisión más rápida mediante la segmentación y envío directo de los datos, aunque sin garantías de entrega ni orden.

2.5.4 Capa de Aplicación

La capa de aplicación se encarga de gestionar los protocolos de alto nivel, así como aspectos relacionados con la representación de datos, su codificación y el control del diálogo entre aplicaciones. En el modelo TCP/IP, esta capa asume las funciones que en el modelo OSI corresponden a las capas de sesión, presentación y aplicación, consolidando así todas las tareas vinculadas a la interacción directa con el usuario y asegurando que la información esté adecuadamente preparada para ser transmitida a través de las capas inferiores.

2.6 Relación de SNMP y CDP

Se ha estudiado los fundamentos de las redes, comprendiendo sus conceptos básicos y su importancia en la conectividad moderna. Sin embargo, una red no es sólo cables, dispositivos y configuraciones; requiere una administración eficiente para garantizar su desempeño, seguridad y escalabilidad.

Aquí es donde entra en juego la administración de redes, un aspecto clave para los profesionales encargados de mantenerlas operativas y optimizadas. En este contexto, dos protocolos destacan por su relevancia: SNMP y CDP.

SNMP es la herramienta esencial para el monitoreo y gestión de dispositivos en la red, permitiendo a los administradores recopilar datos de estado y rendimiento, detectar

fallos y aplicar configuraciones de manera remota. Gracias a este protocolo, los administradores pueden detectar anomalías, recibir alertas sobre posibles fallos y en general garantizar una operación eficiente de la red.

Por otro lado, CDP está diseñado para proporcionar información detallada de los dispositivos vecinos que están conectados en la red, permitiendo conocer su configuración, sistema instalado y además hace posible elaborar y mantener actualizada la topología de la red.

En los siguientes capítulos se profundizará en estos protocolos, descubriendo cómo se implementan y cómo pueden hacer la diferencia en la administración eficaz de una red.

CAPITULO 3: SIMPLE NETWORK MANAGEMENT PROTOCOL

Hoy en día las redes de datos son tan populares dentro de los entornos empresariales que se podría decir que casi todas las organizaciones -sin importar su tamaño - cuentan con una red LAN para sus operaciones cotidianas. Sus funciones, beneficios y de manera especial sus precios cada vez más accesibles, han permitido que su popularidad aumente y sean consideradas ya no un lujo sino una necesidad elemental para casi cualquier empresa.

Su implementación ha traído un gran beneficio para la competitividad y eficiencia de las empresas, sin embargo, aunque existe una gran cantidad de compañías que cuentan con una red, muchas dejan de lado algo tan necesario como la Administración de la red.

El aumento del ancho de banda se ha convertido en la salida más fácil y común de una organización para "resolver" sus problemas en la red, aunque no siempre es la mejor alternativa. A parte de generar un incremento en los costos, no garantiza la resolución a todos los problemas.

A través de una correcta administración de la red se pueden encontrar y resolver problemas como: Cuellos de botella, bucles de conexión, fallos en equipos, pérdidas de paquetes y en general una serie de inconvenientes que podrían estar afectando el desempeño de una red, y que por supuesto no serán solucionados mediante el aumento del ancho de banda contratado. Es por lo que la Administración de Redes se vuelve una práctica esencial en el giro de negocio de una empresa, permitiendo aprovechar de mejor manera sus recursos.

En este capítulo estudiaremos SNMP y sus conceptos más importantes que nos permitan entender su modo de operación, analizando su arquitectura, sus componentes y las versiones existentes con sus características específicas de cada una.

3.1 Administración de Redes

La gestión de redes es un conjunto de tareas que se ejecutan con el propósito de garantizar el correcto funcionamiento de una red, manteniendo un óptimo desempeño y haciéndola cada vez más eficiente y segura. Estos aspectos se logran mediante un constante monitoreo de los equipos donde se pueda evidenciar los eventos que se estén dando en nuestra red.

Entre los múltiples beneficios que brinda una efectiva administración de red y que podemos mencionar están los siguientes: Dar seguridad frente a intrusos, asegurar un correcto tráfico de información sin pérdidas de paquetes, asegurar la disponibilidad de la red, mejorar los tiempos de respuesta, todo esto con una debida planificación, instalación y supervisión que permita su operación y escalabilidad.

Partiendo del concepto de Gestión o Administración de Red, el administrador es quien debe monitorear y verificar el funcionamiento de todos los equipos en su red, para lo cual es necesario valerse de un protocolo que haga posible la gestión de los equipos.

3.1.1 Protocolos de Red

Los protocolos de red son un grupo de normas y procedimientos que dictaminan la manera en la cual se comunican los equipos de una red. Además, los protocolos determinan el diseño lógico de una red, cómo se conectan las computadoras a la red, cómo se formatean los datos para su transmisión y recepción. Sin los protocolos la comunicación entre computadoras no sería posible, no habría forma de transformar los datos en bits ni tampoco los bits en datos en los procesos de transmisión de información entre emisor y receptor.

En otras palabras, el protocolo es el lenguaje de comunicación que usan los distintos dispositivos para comunicarse entre sí e intercambiar información.

3.1.1.1 Protocolos de Administración de Red

Definido el concepto de gestión de red como el conjunto de técnicas orientadas a garantizar el correcto funcionamiento de una red, el protocolo de gestión de red es el lenguaje que hace factible la comunicación entre el Administrador y los equipos que serán administrados.

Al hablar de Protocolos de Administración de Red es necesario mencionar dos elementos importantes: Gestor y Agente.

Gestor. - También conocido como Supervisor, es un software que se encuentra en el equipo de administración, se convierte en la herramienta con la cual el Administrador de Red realiza peticiones de administración a los equipos administrados, quienes contarán con un agente.

Agente. - Es el software que al contrario del Gestor se ubicará en el equipo administrado, atiende (recibe y responde) las solicitudes del Gestor y además tiene acceso a información del equipo en el cual está instalado.

Los protocolos de administración de red son quienes definen la forma y reglas a seguir en la interacción entre estos dos participantes.

Algunas de sus características son:

- Establecen la comunicación entre Gestor y Agente.
- Definen o interpretan el significado de los mensajes intercambiados entre Gestor y Agente mediante el uso de las MIB.
- Tienen la capacidad de acceder e incluso cambiar la información del dispositivo de red.
- Pueden entender las estructuras de información de administración SMI.
- Realizan tres operaciones esenciales:
    - Get – Gestor obtiene datos del agente.

- Set – Gestor establece parámetros en el agente.
- Notify – Agente notifica al gestor de eventos relevantes.

Existe un amplio número de protocolos para la gestión de redes, entre los más comunes podemos mencionar a CMIP basado en el modelo OSI y SNMP basado en TCP/IP.

CMIP (Common Management Information Protocol) o Protocolo Común de Gestión de Información es un protocolo para gestión de redes que fue pensado y creado posteriormente a SNMP; con el objetivo de corregir los problemas que tenía SNMP en su primera versión, CMIP buscaba ser un protocolo más seguro, completo y mejor estructurado, sin embargo, se volvió mucho más complejo y su implementación requería de mayores recursos, dándole una ventaja a SNMP que es más simple y ligero, convirtiéndolo en el más popular.

3.2 SIMPLE NETWORK MANAGEMENT PROTOCOL

SNMP es un protocolo de capa siete cuyo objetivo primordial es el de permitir la administración remota de los equipos de red. Existen varios protocolos de gestión de red, algunos de ellos desarrollados por las mismas marcas que fabrican los dispositivos y que sólo pueden funcionar en sus propios equipos, y otros que, siendo estandarizados pueden utilizarse en casi cualquier equipo, independientemente de su marca, volviéndose ésta una de las principales ventajas de SNMP.

3.2.1 Ventajas y Desventajas de SNMP

Entre las principales ventajas del protocolo podemos mencionar:

- Es un protocolo estándar, lo que quiere decir que es abierto para casi todas las marcas de equipos.

- Permite el monitoreo de equipos de todo tipo: Dispositivos de red, dispositivos de impresión, dispositivos de seguridad, sistemas operativos, servicios en servidores y en general casi cualquier dispositivo que tenga conectividad en red.
- Fácil implementación.
- La información que se intercambia para la administración de los equipos ocupa poco espacio, volviéndolo liviano.
- Permite la definición de las variables, pudiendo elegir el administrador las características que le interesan monitorear.
- Es el protocolo de gestión mayormente utilizado a nivel mundial.
- Es escalable, gracias a su sencillez de implementación y actualización.

Entre las desventajas de SNMP resaltan las siguientes:

- Deficiente control de seguridad. Aunque esta desventaja proviene de la primera versión de este protocolo, en sus dos siguientes versiones ha sido mejorada. Acceso a usuarios no permitidos y posibilidad de interceptar información de los dispositivos eran las mayores falencias que le aquejaban.
- Información poco organizada. Al igual que el caso anterior, la primera versión del protocolo no presentaba una estructura organizada de la información, algo que de igual manera se corrigió en las versiones siguientes.

SNMP trabaja principalmente sobre UDP en los puertos 161 para envíos normales (calendarizados) y 162 para envíos tipo “trap” (notificaciones), aunque también puede operar sobre protocolo TCP.

3.2.2 Componentes de SNMP

SNMP es un protocolo de la capa de aplicación que consta de tres partes esenciales:

- Estación de Administración de RED (NMS – Network Management Station).
- Equipos administrados.
- Agente.

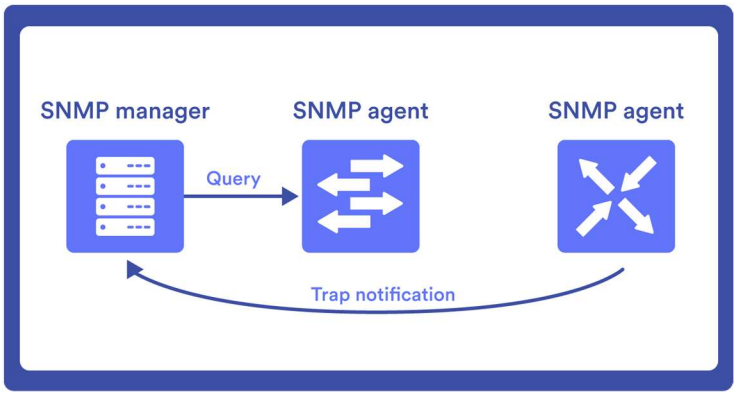


Figura 10. Componentes SNMP. Tomado de (Pandora FMS, s.f.)

3.2.2.1 Estación de Administración de Red (NMS)

Es la cabeza principal del sistema ya que realiza las tareas de monitoreo y control de los equipos gestionados, los NMS son quienes emiten las solicitudes que los agentes deben responder. Siendo considerado el núcleo de un sistema de monitoreo, debe existir al menos un NMS para cada red administrada, y además debe contar con los recursos necesarios para su correcto procesamiento.

3.2.2.2 Equipos Administrados

Son los equipos que se encuentran conectados en la red, los cuales recolectan y envían la información a los NMS.

3.2.2.3 Agente

Es la parte de software de administración de red que se encuentra en el equipo administrado, tiene conocimiento de la información local del equipo (memoria, almacenamiento, temperatura, etc.) la misma que traduce a un formato adecuado para ser enviada al gestor.

3.2.3 Actividades de SNMP

Las actividades que se ejecutan en SNMP podemos dividirlas en dos grupos, las que se realizan en el lado del servidor, y las que se realizan del lado del cliente, teniendo cada uno sus propias funciones.

Actividades que se llevan a cabo del lado del servidor (gestor):

- Se almacenan los datos en su repositorio, lo cual permite tener información histórica y no solo del momento presente.
- Proporciona la interfase al administrador, brindándole el medio para interactuar y controlar la red.
- Permite dar formato a los datos almacenados, convirtiéndolos en información útil a manera de indicadores para el administrador.

Actividades que se llevan a cabo del lado del cliente (agente):

- Recopilar la información del dispositivo.
- Brindar la información necesaria al gestor, sea en respuesta a una solicitud recibida, por actividades periódicas configuradas o bien generadas por un evento (notificación).
- Actuar frente a las solicitudes emitidas por el gestor.

3.2.4 Operaciones de SNMP

Entre las características de los protocolos de gestión de red se pueden mencionar tres operaciones claramente definidas:

- Get (Obtener). - El gestor obtiene datos del agente.
- Set (Establecer). - El gestor establece los valores de los parámetros en el agente.
- Trap (Interrupción). - Cuando el agente notifica al gestor de algún evento suscitado mediante una alerta.

3.2.5 Estructura de los mensajes de SNMP

Para hacer posible la gestión de red, gestores y agentes deben comunicarse entre sí, comunicación que es posible mediante el uso de mensajes, los cuales consisten en:

- Identificador de versión de SNMP
- Comunidad SNMP. Nombre identificativo que se le otorga a la comunidad para la realización de operaciones, se utiliza con fines de autenticación y puede tener propiedades de solo lectura o escritura también (según versión).
- PDU. Unidad de datos del protocolo SNMP.

Los mensajes de SNMP comúnmente tienen un tamaño de 484 bytes, pero en ocasiones este tamaño puede ser mayor.

3.2.5.1 Proceso de comunicación entre Gestor y Agente

Cuando un equipo va a enviar un mensaje, se llevan a cabo las siguientes tareas:

- Se construye la PDU requerida como objeto.

- Se remite la unidad de datos del protocolo, junto con los identificadores de comunidad y las direcciones de origen, a un mecanismo de autenticación que produce otro objeto como respuesta.
- Ahora, el mismo equipo emisor a partir del objeto recibido del servicio de autenticación elabora el mensaje a enviar.
- Finalmente, una vez construido el mensaje, éste es enviado al dispositivo destino a través de la red utilizando un protocolo de transporte.

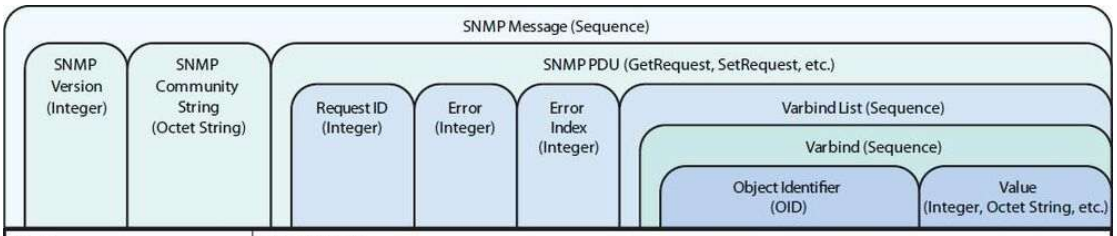
Luego, por el lado contrario, una vez que el dispositivo destino recibe el mensaje se realiza el siguiente proceso:

- Se realiza un chequeo del datagrama recibido, se lo evalúa y si es válido pasa al siguiente paso, caso contrario se descarta y no se ejecuta ninguna otra acción.
- Se revisa que la versión del mensaje SNMP corresponda a la configurada en el equipo receptor, caso contrario de igual manera se descarta el mensaje.
- Validada la versión, se pasan los datos del mensaje al servicio de autenticación, estos son: usuario, comunidad, dirección de origen y nuevamente se evalúan los mismos, si están erróneos el mensaje es descartado y se genera una notificación de error, si están correctos pasa a la última etapa del proceso.
- Finalmente, el receptor revisa la PDU para verificar la comunidad, si es reconocida se procesa conforme a su contenido, si no se reconoce la comunidad se descarta el mensaje. En caso de que la PDU solicite una respuesta, el receptor iniciará con el proceso inmediatamente.

3.2.5.2 Estructura de una PDU de SNMP

Cada mensaje de SNMP contiene una unidad de protocolo (PDU), las cuales son utilizadas para la comunicación entre gestores y agentes SNMP. La PDU de SNMP define los siguientes campos: Versión, nombre de la comunidad, tipo de unidad de dato de protocolo, el ID de solicitud y lista de variables de enlace.

- Versión. - Es un valor numérico que indica la versión de SNMP utilizada, se utiliza 0 para SNMPv1, 1 para SNMPv2c y 3 para SNMPv3. El número 2 no se utiliza.
- Nombre de la comunidad. - La comunidad se utiliza para la autenticación de agentes y sistemas NMS, este campo es una cadena de caracteres definida por el administrador de la red, y puede ser de dos tipos de permisos: sólo lectura o escritura/lectura.
- Tipo de PDU. - Este campo indica la operación específica que solicita el mensaje, puede ser: GetRequest, GetNextRequest, SetRequest, GetResponse o Trap.
- ID de solicitud. – Es un número único que identifica a cada solicitud de SNMP, permitiendo asociar respuestas con solicitudes específicas.
- Lista de variables de enlace. – Este campo contiene las variables MIB asociadas a la operación.



Field	Description
SNMP message	A Sequence representing the entire SNMP message consisting of the SNMP version, Community String, and SNMP PDU.
SNMP Version	An Integer that identifies the version of SNMP. SNMPv1 = 0
SNMP Community String	An Octet String that may contain a string used to add security to SNMP devices.
SNMP PDU	An SNMP PDU contains the body of the SNMP message. There are several types of PDUs. Three common PDUs are GetRequest, GetResponse, SetRequest.
Request ID	An Integer that identifies a particular SNMP request. This index is echoed back in the response from the SNMP agent, allowing the SNMP manager to match an incoming response to the appropriate request.
Error	An Integer set to 0x00 in the request sent by the SNMP manager. The SNMP agent places an error code in this field in the response message if an error occurred processing the request. Some error codes include: 0x00 – No error occurred 0x01 – Response message too large to transport 0x02 – The name of the requested object was not found 0x03 – A data type in the request did not match the data type in the SNMP agent 0x04 – The SNMP manager attempted to set a read-only parameter 0x05 – General Error (some error other than the ones listed above)
Error Index	If an Error occurs, the Error Index holds a pointer to the Object that caused the error, otherwise the Error Index is 0x00.
Varbind List	A Sequence of Varbinds.
Varbind	A Sequence of two fields, an Object ID and the value for/from that Object ID.
Object Identifier	An Object Identifier that points to a particular parameter in the SNMP agent.
Value	SetRequest PDU – Value is applied to the specified OID of the SNMP agent. GetRequest PDU – Value is a Null that acts as a placeholder for the return data. GetResponse PDU – The returned Value from the specified OID of the SNMP agent.

Figura 11. Mensaje SNMP. Tomado de (Fandom, 2012)

3.2.5.2.1 Tipos de PDU utilizados en SNMP

Los tipos de PDU que se utilizan en SNMP son: GetRequest, GetNextRequest, SetRequest, GetResponse y Trap.

- GetRequest. - Es una PDU enviada por el Gestor solicitando el valor de una o más variables de la MIB al agente. Este tipo de PDU son generadas bajo demanda, es decir son producto de una solicitud y no como un evento periódico generado por sí solo. En respuesta, el agente envía un mensaje de tipo GetResponse indicando el éxito o fracaso de la solicitud. Con este mensaje se puede obtener ya sea uno o varios valores de un objeto, depende de cómo especifique la solicitud en la PDU.
- GetNextRequest. - Similar a la anterior, ésta es una PDU enviada por el gestor, solicitando el valor del siguiente objeto en la secuencia de la MIB,

lo que permite a un NMS explorar de manera dinámica tanto la estructura de una vista de la MIB como los datos contenidos en las tablas de objetos. El agente responde al NMS con el valor del siguiente objeto en la secuencia, dando posibilidad al NMS de explorar la MIB de forma eficiente.

- SetRequest. – Al igual que las anteriores, SetRequest es una PDU enviada por el gestor hacia el agente, pero en este caso no es para obtener información sino para modificar una o más variables MIB que se encuentren detalladas en la PDU y con los valores especificados ahí mismo. Las variables que serán modificadas se encuentran dentro de la lista VarBindList. Al igual que GetRequest, ésta PDU es generada sólo cuando se lo requiere, y también espera un mensaje GetResponse como respuesta.
- GetResponse. - Esta PDU, enviada por el agente, es generada en forma de respuesta. Este mensaje contiene los valores de los objetos MIB solicitados y/o los códigos de error (Error Index) para indicar algún problema, por ejemplo, un nombre de objeto inválido.

  El mensaje es elaborado en respuesta a los mensajes GetRequest, GetNextRequest o SetRequest.

  Los tipos de respuestas que se pueden enviar son:

  - Cuando la PDU recibida es de tipo GetRequest, se enviará el objeto con el o los valores correspondientes que fueron solicitados en la PDU. El ErrorStatus y Error Index serán igual a 0.
  - Si se trata de una PDU en respuesta a un mensaje tipo GetNextRequest, se enviará el objeto y valor siguientes al

especificado en la PDU solicitante. El ErrorStatus y Error Index serán igual a 0.

- Si el mensaje GetResponse es enviado en respuesta a una PDU de tipo SetRequest, se enviará la lista de los objetos y valores modificados. El ErrorStatus y Error Index serán igual a 0.
- Si el nombre de la variable indicada en la PDU no es igual al nombre de la MIB se envía un mensaje GetResponse con ErrorStatus igual a 2, y especificando el nombre del objeto que ha originado el error en el campo ErrorIndex.
- Si el valor especificado para una PDU de tipo SetRequest no es el adecuado, se envía un mensaje GetResponse con ErrorStatus igual a 3, así mismo señalando el objeto que ha generado el error en el campo ErrorIndex.
- Cuando el tamaño de la PDU recibida no es correcto, el agente enviará un mensaje GetResponse con ErrorStatus igual a 1.
- Cuando el valor especificado en la PDU SetRequest no puede ser seteado, el agente retornará un mensaje GetRequest con ErrorStatus igual a 5, indicando cual fue el objeto del error en ErrorIndex.

- Trap. Es una PDU que se genera por una interrupción, es decir es un mensaje no solicitado, sino que se genera por el propio agente para notificar al gestor acerca de un evento significativo que ha ocurrido en el equipo. También conocida como alarma, los dispositivos de red como switches, routers, impresoras, servidores, etc. pueden enviar traps al ocurrir ciertos eventos como: Cuando se desconecta una interfaz, cuando

cambia el status en un UPS o cuando se queda sin papel una impresora por mencionar algunos ejemplos.

Luego, cuando el Gestor recibe un Trap pasa sus datos a la aplicación SNMP para que sean transformados en información útil al administrador, en base a la cual se pueden generar reportes, enviar notificaciones por correo o tomar alguna acción según se lo requiera y configure.

Los datos que se agregan en una PDU de tipo trap son:

- Enterprise object identifier: Es un número identificativo (único) del agente que está generando la interrupción. Este valor puede tener hasta 255 caracteres de longitud.
- Agent-addr: Corresponde a la dirección IP del agente responsable de emitir la interrupción.
- Trap-type: Valor numérico que identifica la clase de trap que se está enviando, los cuales pueden ser:
    - (0) coldStart Trap: Cuando el dispositivo se ha reiniciado (de forma abrupta) de manera que pueda alterarse su configuración o la del agente. Comúnmente debido a la caída del sistema.
    - (1) warmStar Trap: Cuando el dispositivo se ha reiniciado (reinicio normal) sin haberse alterado su configuración o la del agente. Por lo general este evento es debido a una rutina de reinicio.
    - (2) linkDown Trap: Este tipo de trap se genera cuando el agente detecta el cambio de estado de activo a inactivo en una interface. El Trap posee como primer elemento de la

lista Variable-Bindings el nombre y valor de la interfaz caída.

- (3) LinkUp Trap: Por el contrario del anterior, este trap se genera cuando el agente detecta el cambio de estado de una interface de inactivo a activo, es decir cuando el enlace se ha reestablecido. Así mismo el Trap tendrá como primer elemento de la lista de Variable-Bindings el nombre y valor de la interfaz levantada.
- (4) AuthenticationFailure Trap: Generada por el sistema cuando un mensaje SNMP es recibido y la verificación del gestor falla.
- (5) egpNeighborLoss Trap: Un trap egpNeighborLoss se genera cuando la relación de la entidad con un vecino (EGP) se ha perdido. En este caso, el mensaje Trap tendrá como primer elemento de la lista de Variable-Bindings el nombre y la dirección del vecino afectado.
- (6) enterpriseSpecific Trap: Este trap se genera cuando la entidad emisora del mensaje reconoce que algún evento de tipo Enterprise-Specific ha ocurrido. El campo specific-trap indicará el trap que ha ocurrido.

- specific-trap: Es un valor numérico que permite identificar traps específicos definidos por fabricantes o detallar con mayor precisión la naturaleza de un trap genérico

- Time-stamp: Representa el intervalo de tiempo transcurrido desde el último inicio o reinicio del dispositivo hasta el momento que se envía el mensaje de Trap.
- Variable-Bindings: Es una lista tipo varBindList que agrupa pares nombre-valor, los cuales identifican los objetos MIB presentes en la PDU, para mensajes de peticiones Request contendrá su valor según corresponda.

3.2.6 Management Information Base (MIB)

La MIB es una estructura jerárquica predefinida que almacena información del equipo donde se encuentra, cada dispositivo contiene su propia MIB. Con cierta similitud a una base de datos, la MIB posee un listado de las variables que se pueden medir y monitorear en el dispositivo, las variables son también conocidas como objetos. La diferencia si se compara a una base de datos es que la MIB no almacena información del dispositivo, sino que la obtiene para ese momento mediante la ejecución de funciones previamente definidas.

La MIB se almacena como un archivo de texto dentro de cada dispositivo con agente SNMP.

El acceso a la información se hace posible mediante solicitudes SNMP bien realizadas por parte de un host (gestor) que ha pasado correctamente el proceso de autenticación, posteriormente el agente ejecuta funciones específicas para acceder a la información y dar respuesta a la petición del gestor. El agente determina (mediante configuración) cuales gestores podrán tener acceso a su información.

Aunque la MIB es una estructura estandarizada a nivel global, posee su cierta flexibilidad para permitir adherir características propias de los equipos y fabricantes.

Probablemente la parte más difícil de entender de un sistema SNMP sea la MIB, para facilitar su comprensión se la puede ver como un árbol jerárquico con su raíz al comienzo y sus hijos o ramales bifurcados hacia abajo. Cada hijo que se desprende de su nodo padre se nombra con un número y un string (nombre identificador), los mismos que son únicos para ese mismo nivel del árbol jerárquico.

Para hacer referencia a un nodo en particular del árbol se deberá seguir su ruta completa, empezando desde la raíz y descendiendo por cada nivel hasta llegar al nodo específico.

Conforme se desciende en el árbol, por cada nivel se agrega su identificador correspondiente (número o string) de forma concatenada formando una dirección.

Cada nivel descendiente en la jerarquía se escribe a continuación del anterior separado por un punto, de modo que la dirección completa será una serie o cadena de identificación (o números) separados por puntos. A esta dirección completa se la conoce como un identificador de objeto (OID Object ID). (Network Working Group, 2002)

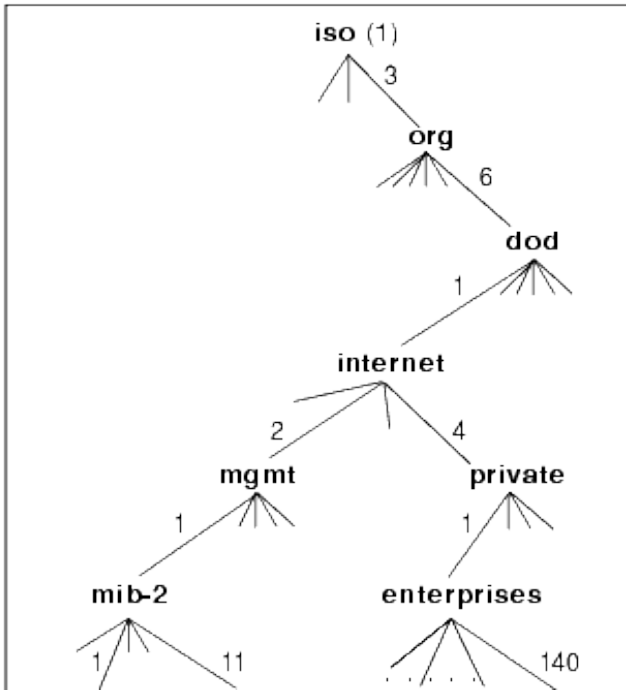


Figura 12. Estructura de una MIB. Tomado de (Oracle, 2025)

La figura 10 muestra un ejemplo de un OID, para este caso el OID puede ser identificado como 1.3.6.1.4.1.140.300 o bien:

iso.org.dod.internet.private.enterprises.bea.tuxedo

Las casas fabricantes que incluyen agentes SNMP en sus dispositivos a veces incluyen ramales personalizados con sus propios campos y datos, sin embargo, hay ramales estándar bien definidos que también pueden ser utilizados por cualquier dispositivo.

Existen dos tipos de MIB, la MIB-I y la MIB-II:

- La MIB-I presenta una estructura más simple y menos compleja, permite un máximo de hasta 100 objetos y fue orientada más hacia redes pequeñas.
- La MIB-II por el contrario contiene una estructura más elaborada, completa y versátil, permitiendo un número casi ilimitado de objetos y enfocada hacia redes TCP/IP más grandes como internet.

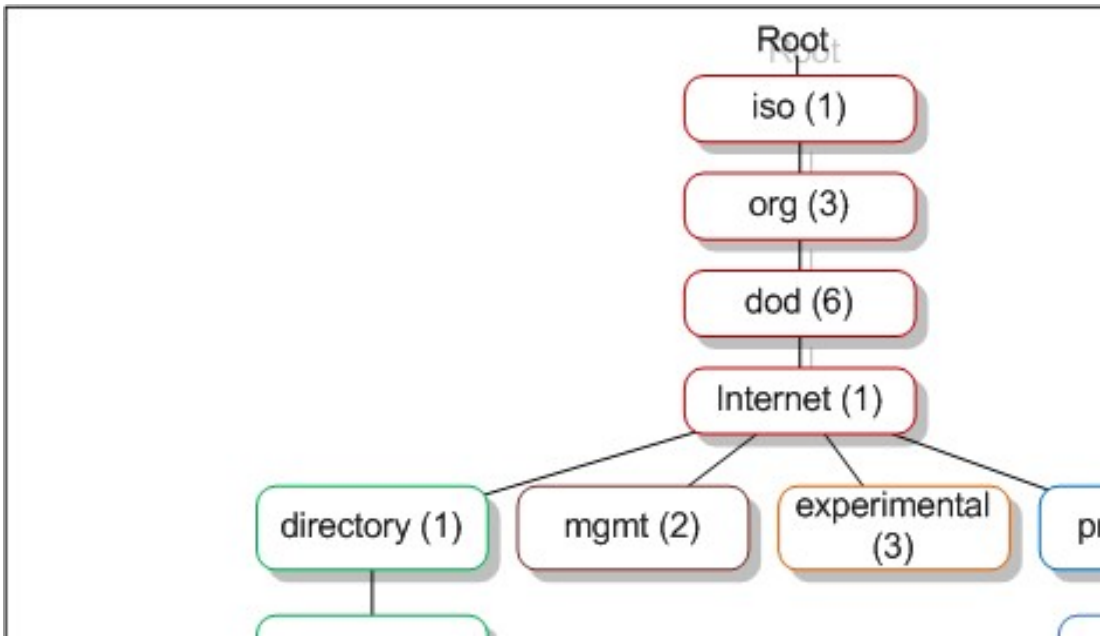


Figura 13. Árbol de OIDs. Tomado de (NETWORK ENGINEERING, 2017)

3.2.7 Problemas de SNMP

Debido a los bajos niveles de seguridad que posee SNMP, existe una variedad de amenazas que pueden afectarle, al tener un sistema de autenticación muy débil podemos tener algunos eventos como dispositivos no autorizados haciéndose pasar por autorizados, modificación en la secuencia y sincronización de mensajes e inclusive obtener información sobre los dispositivos que hay en la red, incluyendo usuarios, credenciales, configuraciones, etc.

Adicional a los riesgos mencionados anteriormente, existe otro problema que está relacionado a la congestión de la red, y es que el monitoreo o supervisión de la red se lo lleva a cabo sobre la misma red, y, en redes de poca capacidad el monitoreo podría llegar a consumir recursos importantes, sobre todo cuando se generan eventos inesperados como la caída de un enlace que conlleva a una tormenta de notificaciones Trap por parte de varios dispositivos al mismo tiempo.

Por otra parte, el monitoreo de la red se lo hace sobre la misma red, lo que puede dar lugar a otro inconveniente, y es que al momento de fallar la red nos quedamos sin el medio por el cual comunicamos los eventos que ocurren en la red, dejando al Administrador de la red con los ojos vendados.

Algunos de estos problemas se los ha ido solucionando conforme la aparición de nuevas y mejoradas versiones de SNMP como son la versión 2 y 3 que lo veremos más adelante en este capítulo.

3.2.8 Seguridad en SNMP

El protocolo SNMP cuenta con un instrumento de control de acceso a la información basado en una variable que es compartida entre gestor y agentes, esta variable es denominada *comunidad*.

Existen dos tipos de comunidades, una se denomina “Publica” y es aquella que cuenta con permisos de sólo lectura, mientras que la otra es conocida como “Privada” y cuenta con permisos de lectura y escritura.

Dado que el control para acceder al sistema está basado en conocer el nombre asignado a la comunidad, su nivel de seguridad es muy frágil, más todavía si se considera que el nombre que se utiliza de comunidad viaja por la red como texto plano, volviéndolo más susceptible a un ataque de escucha de información que transita por la red.

Por lo anteriormente expuesto se puede decir que existen dos tipos de controles de seguridad para SNMP: Por Autenticación y por Autorización.

- Autenticación. - Es un tipo de seguridad muy básico, en el cual se transmite el nombre de la comunidad SNMP sin encriptar y se compara si es correcto o no.
- Autorización. - Luego que el nombre de comunidad es validado, en el agente o gestor se configuran los permisos permitidos para ejecutar con dicha comunidad.

La comunidad SNMP a configurarse, puede ser de tres tipos:

- Read Only (ro): Permisos sólo de lectura.
- Read Write (rw): Permisos de lectura y escritura.
- Trap: Quiere decir que la comunidad permite recibir Traps desde el agente.

Debido a la poca seguridad que brinda el protocolo, éste fue uno de los principales puntos que se consideraron para la mejoría en sus versiones subsiguientes.

3.2.8.1 La evolución de la seguridad en SNMP

Debido a las falencias que posee el protocolo SNMP en su primera versión, era necesario incurrir en algunos cambios que implementen mejores y más robustos conceptos de autenticación y privacidad de la información que maneja.

Una versión segura debía mantener la información a salvo, por lo cual SNMPv1 necesitaba entrar en evolución.

El primer intento de dotar de seguridad al protocolo fue conocido como la versión SNMPsec, cuyos conceptos de seguridad son el punto de partida para las versiones posteriores y que se utilizan hasta el día de hoy.

Las principales mejoras en lo que a seguridad se refiere son la identificación precisa de los actores (gestor y agente), lograda a través del uso de herramientas criptográficas para permitir autenticación, integridad de los datos y por ende privacidad.

Se introducen los siguientes conceptos:

- Party SNMP: Es un entorno virtual para ejecución de operaciones específicas, las mismas que son seleccionadas o escogidas de entre el total de operaciones permitidas por el protocolo. Cada party posee un identificador, una localización en la red, una vista MIB, un protocolo de autenticación y uno de privacidad.
- Vista MIB: Es un subconjunto de variables de una MIB que comparten un identificador de objeto. La vista MIB se define como una colección de vistas de sub-árbol.
- Política de control de acceso: Es el conjunto de mensajes autorizados del protocolo SNMP para la comunicación entre dos party SNMP.
- Protocolo de autenticación: Permite autenticar los mensajes y comprobar su integridad.
- Protocolo de privacidad: Su propósito es el de evitar las escuchas malintencionadas de los datos que viajan por la red. Para esto se utiliza un algoritmo que encripte los datos e impida que sean descifrados mientras son transmitidos.

Posteriormente se lanza la segunda versión de SNMP, en la cual se adopta los conceptos de SNMPsec, pasando entonces a llamarse SNMPv2p (party-based).

Inicialmente con el lanzamiento de la segunda versión de SNMP no se incluyeron nuevas definiciones en lo que a seguridad se refiere, los nuevos controles de seguridad surgieron más adelante, dando lugar a tres nuevas versiones del protocolo: SNMP v2c, SNMP v2u y SNMP v2* que los analizaremos más adelante.

3.2.9 Tipos de implementaciones de SNMP

Para entender de mejor manera los tipos de implementaciones de SNMP es necesario revisar que es el NMS y cómo funciona, lo que dará lugar a los tipos de implementaciones de un sistema de monitoreo de nuestra red mediante SNMP.

3.2.9.1 Arquitectura del NMS

Un componente fundamental de un sistema SNMP es el NMS, equipo central desde el cual se realiza la gestión y el monitoreo de la red, desde aquí se envían las solicitudes a los agentes SNMP y se recibe y almacena toda la información enviada por ellos.

El NMS bien puede ser una aplicación de software o un equipo de hardware dedicado para este fin.

Una vez identificada su importancia, es necesario considerar que el equipo que realice este rol esté en capacidad y cuente con los recursos necesarios para tal efecto. Dependiendo del tamaño de la red que se requiere monitorear, se pueden tener dos diferentes tipos de implementaciones de NMS: Centralizado y Distribuido.

- El NMS Centralizado es una implementación en donde se instala un solo NMS para toda la red, siendo el único equipo encargado del monitoreo para todos los dispositivos.

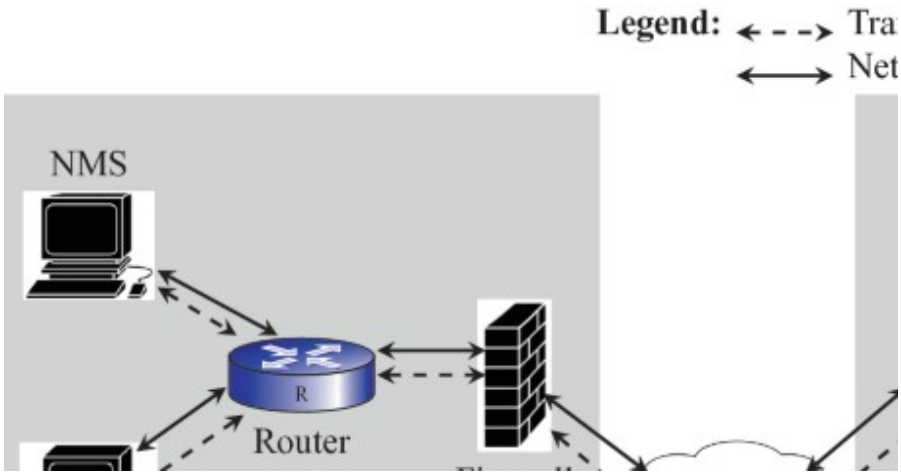


Figura 14. NMS Centralizado. Tomado de (SpringerNature, 2023)

Tener un solo NMPS puede dar lugar a algunos inconvenientes como:

- Punto único de falla. Ya que existe un único equipo encargado de la gestión de toda la red, si este equipo falla todo el servicio de monitoreo se vería afectado.
- Por otra parte, en redes grandes con una cantidad importante de dispositivos monitoreados puede provocar una saturación del NMS.
- Otro inconveniente de las redes muy grandes es que pueden tener oficinas geográficamente muy lejanas, en diferentes ciudades o países, lo cual implica que, si la red tiene un solo NMS, todo el tráfico de la red tendrá que viajar a través de los enlaces WAN hasta llegar al NMS, incrementando tiempos de respuesta, tráfico en los enlaces WAN y costos para la empresa.

Debido a estos motivos se ha considerado la alternativa de distribuir el trabajo entre varios NMS a lo largo de la red.

- Los NMS distribuidos no es más que la instalación de varios NMS con el objetivo de distribuir la carga de trabajo y atender todas las necesidades de gestión y monitoreo de la red por “zonas”. Esta alternativa sin lugar a duda incrementa los costos de implementación, pero podría ser beneficiosa

en algunos casos. Será responsabilidad del Administrador de la red hacer un adecuado análisis que permita determinar la necesidad o no de implementar un monitoreo distribuido. (O'Reilly & Associates, 2002)

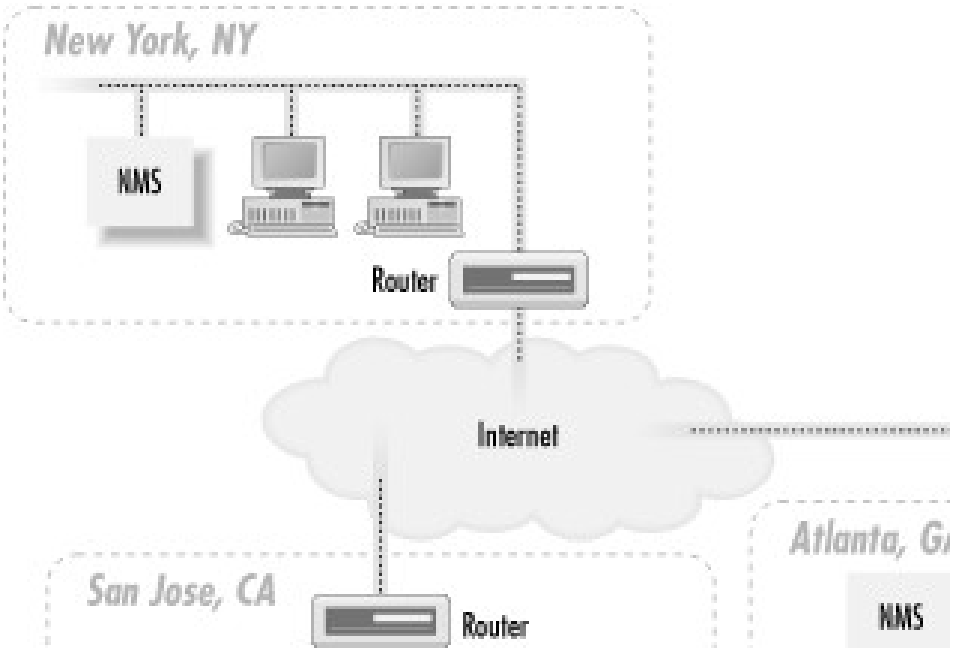


Figura 15. NMS Distribuido. Tomado de (O'Reilly & Associates, 2002)

3.2.9.2 RMON

Remote Network Monitoring, es una extensión de SNMP que permite almacenar datos sobre el uso y rendimiento de la red. A través de estadísticas del tráfico recopiladas, los administradores pueden obtener información para aplicar cambios que mejoren el rendimiento de la red.

Los datos sobre el tráfico de la red y de eventos importantes son almacenados en lo que se conoce como la sonda RMON o simplemente sonda. Entre los datos clave que almacena la sonda están:

- Estadísticas de tráfico: Se registra la cantidad de bytes entrantes y salientes.
- Monitorización de host: Se registra la actividad de dispositivos específicos en la red.

- Historial de eventos: Se registran todos los sucesos ocurridos.
- Alarmas: Permite la configuración de umbrales para diferentes métricas, disparando alertas cuando se alcancen los valores requeridos.

Haciendo una analogía, podemos ver a la sonda RMON como los indicadores KPI de la red, los cuales permiten al administrador observar cómo está operando su red y tomar acciones según sea necesario.

3.3 SNMP Versión 1

La versión 1 es la primera implementación del protocolo SNMP, la cual opera sobre los protocolos UDP, IP, DDP de AppleTalk e IPX de Novell.

Desde su creación el protocolo fue concebido para la administración de redes, de donde nacieron todos los conceptos que hemos mencionado anteriormente: Gestor, agente, MIB, NMS, etc. Las características propias de la versión 1, son:

3.3.1 Seguridad

- SNMPv1 posee una seguridad muy básica, basada únicamente en el nombre de la comunidad para autenticar gestores y agentes.
- Por cuestiones de seguridad inicialmente sólo se manejaba comunidad con permisos de lectura, posteriormente se incorporó también la comunidad con permisos de lectura/escritura.
- El nombre de la comunidad es enviado como texto plano por la red, haciendo más vulnerable a escucha no permitida.

3.3.2 Operaciones

- SNMPv1 maneja únicamente los siguientes tipos de operaciones: lectura (GET), leer siguiente (GETNEXT) y escritura (SET), lo cual en cierta forma lo volvía limitado.

3.3.3 MIB

- SNMPv1 utiliza una MIB más simple o con menos contenido en cuanto a la información que los gestores pueden obtener de los agentes administrados.

3.3.4 Compatibilidad entre versiones

- Los gestores de SNMPv1 no pueden comunicarse con agentes SNMPv2, mientras que gestores SNMPv2 pueden comunicarse con agente SNMPv1 y SNMPv2.

3.3.5 Tamaño del paquete

- Los paquetes de SNMPv1 son de menor tamaño que los de SNMPv2, lo cual puede ser una desventaja si el ancho de banda es de poca capacidad en la red.

3.4 SNMP Versión 2

La versión 2 de SNMP fue lanzada en 1993, la cual buscaba cubrir algunas de las limitaciones de la versión antecesora, procurando mejorar su funcionalidad y seguridad.

Entre las mejoras que incluye SNMPv2 podemos mencionar:

- Soporte para contadores de 64 bits, lo cual es una ventaja frente a los 32 bits de SNMPv1 ya que permite gestionar valores más grandes y evitar posibles desbordamientos en momentos con alto tráfico en la red. Algo muy útil para redes medianas o grandes y con altos volúmenes de tráfico.
- Se agrega la operación GetBulkRequest, la cual permite obtener una mayor cantidad de datos de una sola vez.

- Se agrega una MIB más estructurada y con más información de los agentes, permitiendo monitorear más variables de un dispositivo, así como la opción de gestionar una mayor variedad de dispositivos de red.
- Manejo de errores mejorado.
- Mayor robustez en la comunicación entre gestor y agente.
- Se agrega la notificación de eventos, para enviar alertas a los administradores de red de sucesos presentados.
- En cuanto a la seguridad incluye la autenticación, pero sin cifrado.

3.4.1 Modelos de SNMPv2

Con la versión 2 del protocolo se liberaron algunos modelos que intentaban solucionar los problemas de seguridad de SNMPv1, cada uno de estos modelos tenía sus características propias como se detalla a continuación:

3.4.1.1 SNMP v2p – Modelo de seguridad basado en partes.

- Proporciona una forma más flexible de autenticación y autorización.
- Sin embargo, no fue ampliamente aceptado por la sociedad debido a su compleja configuración y por falta de consenso entre la comunidad internacional.

3.4.1.2 SNMP v2u – Modelo de seguridad basado en usuarios.

- Fue liberado con el propósito de incrementar la seguridad, en su caso particular incorporaba la autenticación y autorización de usuarios individuales.
- Similar que con SNMPv2p, este modelo no fue ampliamente difundido ya que tenía los mismos inconvenientes de complejidad y falta de consenso.

3.4.1.3 SNMP v2c – Modelo de seguridad basado en comunidades.

- Debido a la poca aceptación y popularidad de los modelos anteriores, la versión SNMPv2c encuentra una ventaja en su sencillez para configurar, lo que pronto la convierte en el modelo más utilizado hasta el día de hoy. Éste no contiene ninguno de los modelos de seguridad anteriores y hoy en día se la conoce únicamente como SNMPv2.
- Utiliza el esquema simple de seguridad basado en comunidad que se utiliza en SNMPv1.

3.5 SNMP Versión 3

Con el deficiente control de seguridad de SNMPv2 basado únicamente en el nombre de la comunidad, surge la tercera y más reciente versión del protocolo SNMP. Lanzada en 1999, esta nueva versión se desarrolló con el objetivo de corregir inconvenientes de las versiones anteriores, pero principalmente fortalecer la seguridad.

Para fortalecer este aspecto tan importante hoy en día, esta versión de SNMP utiliza dos modelos conocidos el USM y el VCAM. El modelo USM (User Security Model) es el encargado de brindar autenticación y cifrado (Network Working Group, 2002), mientras que el VCAM (View-Based Access Control Model) está orientado hacia el control de accesos, a continuación, analizaremos cada una de estas funciones:

1. Autenticación: La autenticación se aplica con el objetivo de comprobar la identidad de usuarios y dispositivos, además, asegura que los mensajes no hayan sido modificados durante la transmisión.
2. Privacidad: La privacidad se basa en el uso de cifrado para garantizar la confidencialidad de los datos, evitando que sean accedidos por equipos o usuarios no autorizados.

3. Control de acceso: El control de acceso, sirve para supervisar el acceso a los objetos administrados dentro de la red. (Network Working Group, 2002)

3.5.1 Autenticación

La autenticación procura identificar y asegurarse que sólo los usuarios y equipos autorizados tengan acceso a la información. Para asegurar que los mensajes no hayan sido alterados y vengan de fuentes legítimas se utiliza un algoritmo de autenticación, que puede ser SHA o MD5.

3.5.1.1 Algoritmo SHA-1

SHA-1 o Secure Hash Algorithm 1 por sus siglas en inglés, es un algoritmo hash criptográfico que recibe un mensaje de cualquier longitud para producir un mensaje de salida de 160 bits, conocido como resumen de mensaje.

Las funciones hash criptográficas son operaciones matemáticas utilizadas para verificar que un archivo no ha sido alterado, permitiendo garantizar que los datos no hayan sido alterados y provengan de una fuente confiable. ¿Pero cómo verifica que el mensaje no ha sido alterado? SHA-1 produce una suma de comprobación previo a su transmisión, y luego una vez llega a su destino se realiza la misma operación para verificar que resulte igual.

SHA-1 utiliza una función de compresión que trabaja en bloques. El mensaje entrante se secciona en bloques de 512 bits y se procesan uno por uno. El resultado de cada bloque se utiliza como entrada para el siguiente bloque y así continúa hasta finalizar todo el mensaje. El resultado final es un resumen del mensaje con tamaño de 160 bits.

SHA-1 ha sido considerado inseguro desde 2005 debido a la posibilidad de ataques de colisión, por lo que es recomendable usar SHA-2 o SHA-3.

Principales diferencias entre SHA-1, SHA-2 y SHA-3

- Longitud de HASH: SHA-1 genera un mensaje hash de 160 bits que es fijo, mientras que SHA-2 y SHA-3 puede variar entre 224, 256, 384 y 512 bits.
- Velocidad: SHA-1 es más rápido que SHA-2, y SHA-2 es más rápido que SHA-3.
- Seguridad: El más seguro es SHA-3, seguido de SHA-2 y finalmente SHA-1.
- Estructura: SHA-1 y SHA-2 utilizan una estructura similar llamada de Merkle-Damgård, en cambio SHA-3 tiene una estructura basada en el algoritmo de Keccak.

3.5.1.2 Algoritmo MD5

Message Digest Algoritm 5 por sus siglas en inglés, es un algoritmo de reducción criptográfico con objetivo similar al de SHA en cuanto a la generación de códigos Hash para comprobar que un mensaje no ha sido modificado. El algoritmo fue diseñado en 1991 por Ronald Rivest como una propuesta de mejora a MD4. En este caso, MD5 toma el mensaje de entrada de cualquier longitud y lo convierte en un mensaje salida de 32 caracteres conocido como resumen, huella digital o hash.

Como aspectos importantes podemos mencionar:

Propiedades:

- Unidireccional, con el mensaje de entrada se puede obtener el hash de salida, pero con el hash de salida no es posible obtener el mensaje original.
- Determinista, esto quiere decir que, para el mismo mensaje de entrada, siempre se obtendrá el mismo mensaje de salida.
- Rápido de calcular.

Usos comunes:

- Verificación de integridad: Sirve para comprobar si los mensajes transmitidos están intactos y no han sufrido modificación.
- Contraseñas: Aun siendo inseguro, anteriormente se lo utilizaba para almacenamiento de hashes de contraseñas de bases de datos, hoy en día es poco común utilizarlo en este ámbito.

Limitaciones:

- Colisión: Aunque la probabilidad es muy baja, puede darse el caso que dos mensajes de entrada diferentes generen el mismo hash de salida, lo que provocaría una colisión.
- Seguridad: MD5 se considera inseguro por ser vulnerable a ataques de colisión, en su reemplazo se recomienda utilizar SHA256.

¿Cómo funciona MD5?

MD5 se utiliza para autenticar mensajes y verificar que el contenido no haya sido modificado, opera de la siguiente manera:

1. Generación del Hash

MD5 toma un archivo completo y lo procesa a través de un algoritmo matemático de hashing.

El resultado obtenido es un mensaje hash MD5 de 32 caracteres, no importa el tamaño del archivo de entrada, siempre se obtendrá un mensaje de salida del mismo tamaño.

2. Verificación de integridad

Cuando se envía un archivo, el emisor calcula el hash y luego cuando el receptor lo recibe también calcula el hash, si son idénticos se entiende que no ha habido alteración del mensaje.

Basta con modificar un solo bit de todo un archivo para que el hash resultante sea distinto.

3. Usos principales

MD5 se utiliza principalmente para verificar archivos que no hayan sido modificados, aunque también se utilizaba para cifrado.

3.5.2 Privacidad

Apegado a su objetivo de mejorar la seguridad, SNMPv3 agrega la función de cifrado para que los datos sean confidenciales y se evite su modificación durante la transmisión. Para tal efecto, SNMPv3 utiliza algoritmos como: DES o AES

- 3-DES. – Triple Data Encryption Standard.
- AES. - Advanced Encryption Standard.

3.5.2.1 Algoritmo DES

Data Encryption Standard es un algoritmo para proteger la información a través del cifrado por bloques. Es un algoritmo para hacer cifrado simétrico que lo desarrolló IBM en 1976 el cual hace uso de una clave de 56 bits para cifrar o descifrar la información. El cifrado consta de 16 rondas, cada una utiliza una subclave distinta que proviene de la clave inicial o maestra. El proceso se realiza en tres fases.

- Permutación inicial
- Iteraciones de cifrado
- Permutación final

La permutación inicial tiene como función principal reorganizar los bits de entrada para aumentar la confusión y difusión del cifrado, haciendo que sea difícil deducir la clave de cifrado a partir del tex.to cifrado. El algoritmo opera en bloques de 64 bits los cuales se dividen en dos mitades (de 32 bits cada una) y se aplica una función que utiliza la clave simétrica y se obtiene una salida. Posterior a esto, se combina la salida con la otra

mitad del bloque y se repite el proceso hasta cumplir las 16 rondas o iteraciones de cifrado.

Finalmente, para la permutación final se realiza el proceso inverso al de la permutación inicial aplicando una matriz a cada uno de los bits del bloque, restaurando los bits a su estado original.

Anteriormente DES fue muy utilizado, sin embargo, con el pasar de los años ha dejado de utilizarse debido a que su "corta" clave se considera vulnerable para ataques de fuerza bruta.

En atención a esta falencia de seguridad, surge 3-DES, el cual utiliza 3 claves diferentes de 56 bits y aplica el algoritmo DES tres veces seguidas, volviéndolo más seguro, pero más lento también.

Tanto DES como 3-DES han sido reemplazados por algoritmos más modernos y seguros como AES.

3.5.2.1.1 El cifrado simétrico

Es un método criptográfico en el cual emisor y receptor utilizan una misma clave para cifrar y descifrar los datos. Primero ambos participantes se ponen de acuerdo sobre la clave que van a utilizar, y luego, una vez que ambos tienen conocimiento de ella, el remitente cifra el mensaje utilizando la clave, lo envía al receptor, quien procede a descifrarlo valiéndose de la misma clave. La criptografía simétrica está basada principalmente de algoritmos con operaciones booleanas y se considera más eficiente que la criptografía asimétrica (clave para cifrar distinta de clave para descifrar). La seguridad se basa en la confidencialidad de la clave compartida, mas no en el algoritmo. Es decir, para un atacante no serviría de nada conocer el algoritmo que se está utilizando si no conoce la clave, sólo si obtiene la clave serviría saber el algoritmo.

3.5.2.2 Algoritmo AES

Advanced Encryption Standard, es un algoritmo de cifrado simétrico utilizado para proteger los datos en el proceso de transmisión. Este algoritmo fue desarrollado por dos criptógrafos belgas, Joan Daemen y Vincent Rijmen, quienes utilizaron el principio de diseño conocido como red de sustitución-permutación. Establecido en 2001, es el primer y único cifrado públicamente accesible que está aprobado por la Agencia Nacional de Seguridad para el manejo de información clasificada.

El cifrado AES funciona en tres etapas: expansión clave, cifrado y descifrado.

- En la primera etapa se genera una matriz de contraseñas a partir de una clave "maestra" la cual es conocida por el remitente y el receptor.
- En la segunda etapa se secciona el mensaje original en bloques y se aplican una serie de operaciones criptográficas a cada bloque.
- En la tercera etapa se aplican las mismas operaciones anteriores, pero en orden inverso, permitiendo restablecer el mensaje original.

El algoritmo basado en redes de sustitución-permutación (SPN) realiza un conjunto de cuatro transformaciones fundamentales: reemplazo de bytes mediante S-boxes, reorganización de filas, mezcla de columnas para difundir la información y la incorporación de una clave de ronda en cada iteración. Estas operaciones se ejecutan repetidamente a los bloques del mensaje original durante la etapa de cifrado, lo que brinda la confidencialidad a los datos.

AES es un método de cifrado ágil y seguro que se utiliza en aplicaciones de mensajería instantánea como WhatsApp o programas de compresión como WinZip, siendo así uno de los más utilizados y seguros en la actualidad.

3.5.2.3 Diferencias entre AES y 3-DES

- Fecha de creación: DES fue el precursor, lanzado en 1977 mientras que AES en 2001.
- Longitud de clave: DES tiene una longitud de clave única de 56 bits, mientras que en el caso de AES puede ser de 128, 192 o 256 bits.
- Número de rondas: En el caso de DES la cantidad de rondas es de 16 exclusivamente, en el caso de AES la cantidad varía según la longitud de la clave:
    - 10 rondas en el caso de 128 bits de longitud
    - 12 rondas en el caso de 192 bits de longitud, y
    - 14 rondas en el caso de 256 bits de longitud.
- Estructura: DES está basado en una red Feistel, mientras que AES se basa en sustitución-permutación.
- Velocidad: Como lo es de esperar, AES al ser más reciente, es más rápido también.
- Seguridad: Similar a lo ocurrido con la velocidad, AES tiene ventajas frente a DES en lo que a seguridad concierne.
- AES es el protocolo mayormente utilizado en SNMPv3

3.5.3 Control de Acceso

SNMPv3 implementa un modelo denominado VCAM (View-Based Access Control Model) para gestionar el acceso a los objetos administrados dentro de la red. Este modelo permite definir distintos niveles de visibilidad y operación sobre las MIB, de modo que los agentes pueden limitar qué partes de la MIB son accesibles para cada gestor, así como establecer qué acciones están autorizadas según el perfil o necesidad del solicitante. (Network Working Group, 2002)

El modelo VCAM ofrece varios beneficios relacionados a la administración de acceso a sistemas y redes, entre los que podemos mencionar:

1. Control granular de acceso
    - Permite configurar un control específico sobre qué usuarios pueden acceder a objetos específicos de la MIB. Además, asegura que se asignen los mismos permisos a diferentes usuarios con las mismas responsabilidades.
    - Define roles y permisos previo a su implementación, lo cual facilita el proceso de gestión y asegura una aplicación uniforme de las políticas de acceso.
2. Seguridad mejorada
    - La seguridad se ve mejorada al asociar usuarios con grupos y vistas específicas, lo que le permite al VACM garantizar que sólo aquellos con los permisos adecuados accedan a los datos o realicen operaciones.
    - Esto ayuda a prevenir accesos no autorizados y protege la integridad de la red y facilita la gestión mediante el uso de grupos.
3. Configuración remota
    - Este modelo posibilita la configuración remota de los permisos de acceso a los objetos definidos en la MIB, lo cual resulta fundamental para una administración ágil y eficaz, especialmente en entornos de red distribuidos donde la gestión centralizada no siempre es viable.
4. Cumplimiento de normativas
    - Al implementar el VACM, las organizaciones pueden cumplir con regulaciones de seguridad y privacidad, algo muy importante

especialmente en grandes corporaciones con normas o marcos de seguridad definidos.

5. Flexibilidad

- El VACM es altamente configurable, permitiendo a los administradores adaptarlo a las necesidades específicas de su red. Esto se logra definiendo grupos y niveles de acceso según se lo requiera.

En resumen, el modelo VACM permite:

- Limitar el acceso a partes específicas de la MIB según roles y permisos asignados.
- Definir qué operaciones están permitidas para cada usuario

3.6 Diferencias entre SNMP V1, V2 y V3

Una vez estudiadas las tres versiones existentes de SNMP, vamos a revisar las diferencias entre cada una de ellas:

1. SNMPv1:

- Fecha de lanzamiento: 1988
- Seguridad: Deficiente, utiliza una comunidad “pública” o “privada” como único control. No permite autenticación ni cifrado.
- Funcionalidad: Permite tanto lectura como escritura de datos, pero con estructura de datos más sencilla.
- Conclusión: Vulnerable a ataques, no recomendada para uso.

2. SNMPv2:

- Fecha de lanzamiento: Depende de la versión
- Versiones:
    - SNMPv2c: Es la versión más utilizada, mejora la eficiencia y la capacidad para manejar errores.

    - SNMPv2u: Esta versión utiliza UDP en lugar de TCP para su transmisión.
    - SNMPv2*: Liberada, pero no ampliamente utilizada.
- Seguridad: Mejor que en SNMPv1, pero mantiene la comunidad como método de autenticación.
- Funcionalidad: Ofrece mejoras en la estructura de datos y la capacidad de respuesta. Esta versión agrega la funcionalidad que el administrador reciba mensajes de los agentes SNMP.
- Conclusión: Mejor estructura de datos, más eficiente y mayor aceptación en el mercado, aunque su control de seguridad permanezca limitado.

3. SNMPv3:

- Fecha de lanzamiento: 1998
- Seguridad: Soluciona las deficiencias de seguridad de sus versiones anteriores, incorpora autenticación, cifrado y control de acceso.
- Modelo de vistas: Agrega el modelo VCAM, otorgando diferentes niveles de acceso.
- Privacidad: Garantiza la privacidad de los datos, aun cuando se envían mediante internet.
- Conclusión: Aunque SNMPv3 es la más segura, no ha sido ampliamente utilizada, su mayor complejidad de configuración ha jugado en su contra.

CAPITULO 4: CISCO DISCOVERY PROTOCOL

En el ámbito de las redes, la capacidad de identificar y gestionar dispositivos conectados es fundamental para garantizar un funcionamiento eficiente y seguro. Cisco Discovery Protocol es un protocolo diseñado para el descubrimiento de dispositivos vecinos que se encuentran conectados, identificando algunas de sus características propias.

Este capítulo explorará los conceptos clave de CDP, su funcionamiento y los beneficios que ofrece a los administradores de red. Desde la identificación de dispositivos vecinos hasta la optimización de la gestión de infraestructura, CDP se convierte en una herramienta muy útil para la administración de redes Cisco.

4.1 Definición y propósito

CDP es un protocolo de capa 2, propietario de Cisco, el cual sirve para descubrir y recolectar información de los dispositivos vecinos que se encuentran conectados, permitiendo elaborar y mantener actualizada la topología lógica de la red.

4.2 Funcionamiento y características principales

Todo dispositivo ejecutando CDP envía mensajes periódicos conocidos como publicaciones, estos mensajes se envían cada 60 segundos de forma automática a través de las interfaces donde se encuentre habilitado el protocolo. Aunque este tiempo es predeterminado, puede ser ajustado. Cada equipo Cisco que ejecuta CDP almacena la información recibida de sus vecinos en una tabla, la cual se actualiza con cada mensaje recibido. Si un equipo deja de recibir actualizaciones de un vecino CDP por más de 180 segundos, se elimina la información de ese dispositivo en la tabla de vecinos CDP. Este tiempo se conoce como TTL y también puede ser parametrizado. (Cisco Systems, 2004)

Cuando una interfaz ha sido activada, los paquetes se envían con TTL mayor a cero, y, por el contrario, cuando una interfaz ha caído inmediatamente se envían paquetes CDP con TTL igual a cero, esto permite una rápida identificación del estado de la interfase.

Los dispositivos Cisco cuando reciben paquetes CDP, enseguida los procesan y almacenan la información recibida, pero nunca la reenvían. Si la información cambia por un nuevo paquete recibido, se almacena y se descarta la más antigua, aun cuando su TTL no haya expirado.

CDP viene habilitado desde fábrica en los equipos, aunque si se requiere, puede deshabilitarse de forma global (para todo el equipo) o parcialmente por interfaces. Cuando un dispositivo Cisco inicia, CDP se pone en marcha automáticamente, permitiendo al dispositivo detectar los equipos vecinos que también están ejecutando CDP.

Entre sus aspectos más relevantes se encuentran:

- CDP funciona únicamente sobre la capa de enlace de datos.
- Los mensajes CDP se envían a la dirección multicast de capa 2 01:00:0C:CC:CC:CC.
- CDP funciona sólo en interfaces directamente conectadas.
- La información de los equipos vecinos se almacena en una tabla llamada *vecinos CDP.*
- CDP solo puede operar en aquellos medios de comunicación que admiten el protocolo SNAP como: Ethernet, PPP, Token Ring, HDLC, FDDI, ATM, y Frame Relay. SNAP se usa para identificar protocolos mediante valores de EtherType, lo que facilita la compatibilidad con distintos estándares de comunicación.

4.3 Versiones de Cisco Discovery Protocol

Existen dos versiones del protocolo CDP:

- CDPv1: Fue la primera versión del protocolo, lanzada en 1994. Compatible con la gran mayoría de los dispositivos de red Cisco, proporciona información básica sobre la topología de la red, nombre y dirección del dispositivo.
- CDPv2: Es una versión mejorada del protocolo, se lanzó en 1997. Esta nueva versión ofrece información adicional sobre la topología de la red como: La capacidad del enlace, la VLAN y la dirección MAC del dispositivo. Siendo la última versión del protocolo, es la más compatible con los equipos y la más utilizada. (Cisco Community, 2019)

Características y diferencias entre las versiones de CDP (Cisco Community, 2019):

Tabla 3. Versiones de CDP

CARACTERISTICA	CDPv1	CDPv2
Fecha de lanzamiento:	1994	1997
Propósito:	Proporciona información básica sobre dispositivos vecinos.	Proporciona información adicional como capacidad de enlace.
Detección de errores:	No tiene mecanismos.	Detecta errores como VLANs nativas no coincidentes y estados de dúplex no coincidentes.

Registro de errores:	No tiene mecanismos.	Puede enviar mensajes de error a la consola o a un servidor de logs.
Uso de unicast / multicast:	Utiliza paquetes multicast para la comunicación.	Puede utilizar multicast o unicast para mejorar la eficiencia de la red.
Direcciones MAC:	Reporta direcciones MAC de dispositivos vecinos	Incluye información más detallada sobre direcciones MAC y su asociación con VLANs.
Período de envío de actualizaciones:	Envía paquetes cada 60 segundos.	Mantiene el mismo intervalo, pero puede modificarse si se requiere
Impacto en la red:	Menos detallado, útil para configuraciones básicas.	Mejora su eficiencia al proporcionar información más precisa.

Nota: Diferencias entre CDPv1 y CDPv2

4.4 Información que podemos obtener con CDP

CDP se utiliza en dispositivos Cisco para obtener información de los equipos adyacentes, aunque los datos que se pueden obtener varían de acuerdo con el modelo de dispositivo y la versión del IOS (sistema operativo) que tiene instalado, algunos que se puede mencionar son:

- La dirección IP.
- El nombre del dispositivo.
- Versión del sistema operativo.

- El tipo de dispositivo.
- El puerto o interfase.
- La plataforma del dispositivo.
- La configuración de la interfase: simplex o dúplex.
- La VLAN nativa.

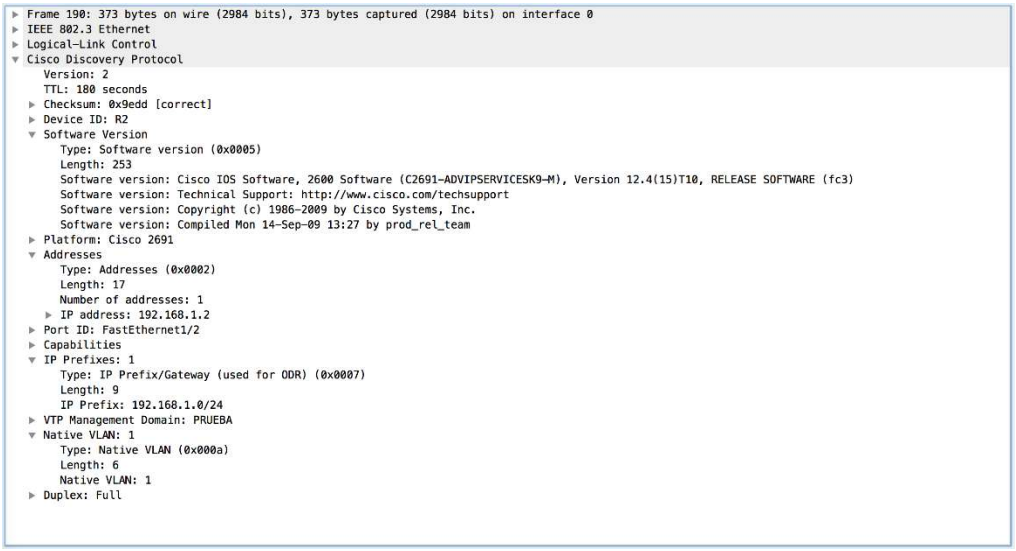


Figura 16. Captura de trama de CDP. Tomado de (W0lf_F4ng, 2020)

4.5 Trama de CDP

La trama de CDP es una estructura de datos que contiene información sobre el equipo que está enviando la trama, así como información sobre los equipos directamente conectados a él.

Los campos de la trama CDP son:

- Encabezado Ethernet. Identifica la dirección MAC del origen y del destino, preámbulo, delimitador de trama y FCS.
- Encabezado CDP. Indica que la trama pertenece a un protocolo propietario de Cisco.
- Versión. Especifica la versión de CDP utilizada.

- TTL. Especifica el tiempo de vida de la información en la tabla de vecinos antes de ser descartada.
- Información de dispositivo:
    - Nombre del equipo
    - Dirección IP
    - Número de puerto desde el que se envía la trama.
    - Versión del sistema operativo.
    - Tipo y modelo del dispositivo.
    - Configuración de VLAN nativa.
    - Consumo energético (en equipos PoE).

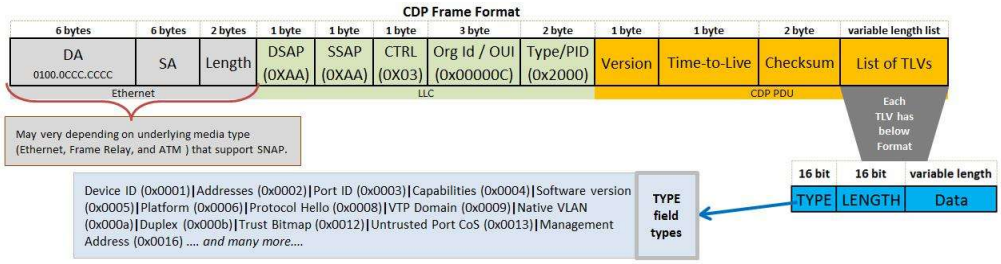


Figura 17. Formato de trama CDP. Tomado de (Bhattarai, 2020)

4.6 Configuración de CDP

CDP viene habilitado desde fábrica y su operación inicia tan pronto se enciende el equipo, sin embargo, es conveniente tomar en consideración algunas buenas prácticas al momento de tenerlo en operación:

- Habilitar CDP sólo en los puertos que se conectan a otros equipos Cisco. Esto evita colocar paquetes en la red que no serán de utilidad, aunque los paquetes de CDP son muy pequeños y no provocan saturación, se evitará tráfico innecesario.

- Configurar un intervalo de tiempo para la publicación de anuncios: CDP envía actualizaciones cada 60 segundos, se puede modificar para ajustar a lo que se requiera.
- Limitar la información de la topología que se entrega. CDP puede enviar información detallada, limitarla reduce el tráfico y la exposición de información sensible.
- Activar CDP sólo en las interfaces que se requiera, esto limita el envío de información por interfaces que no se necesita, evitando exponer información de nuestra red (al router del proveedor de internet, por ejemplo).
- Mantener actualizados los dispositivos de la red. Los dispositivos deben tener la última versión de CDP instalada y así asegurarse de que se están utilizando las funciones más avanzadas.

4.6.1 Comandos para configurar CDP

Los comandos para configurar CDP varían según el dispositivo y la versión del software utilizado, entre los más importantes destacan los siguientes:

Tabla 4. Comandos de CDP

Router# show cdp	Despliega la información global del protocolo.
Router# show cdp neighbors	Sirve para mostrar información resumida de los equipos vecinos.
Router# show cdp neighbors detail	Sirve para mostrar información detallada de los equipos vecinos.

Router# show cdp entry *	Muestra información de todos los equipos.
Router# show cdp entry *equipo*	Muestra información del dispositivo llamado *equipo.*
Router# show cdp traffic	Muestra la información del tráfico, paquetes de entrada / salida / versión.
Router# show cdp interface	Despliega información acerca de las interfaces que están corriendo CDP.
Router# show cdp interface x	Despliega información específica de la interfaz x.
Router# cdp run	Habilita la ejecución de forma global para todo el equipo.
Router# no cdp run	Apaga la ejecución de CDP para todo el dispositivo.
Router# cdp timer	Cambia el tiempo en que los mensajes de actualización se envían.
Router(config-if)# cdp enable	Enciende CDP en la interfaz que se ha ingresado.
Router(config-if)# no cdp enable	Apaga CDP en una determinada interfaz.
Router# clear cdp counters	Reinicia los contadores de tráfico a cero.
Router# debug cdp events	Monitorea los eventos de CDP.
Router# clear cdp table	Borra la tabla CDP.

Router# debug cdp ip	Monitorea eventos CDP específicamente por IP.
Router# debug cdp packets	Monitorea los paquetes de CDP.
Router# debug cdp adjacency	Monitorea información de los vecinos CDP.

4.7 Beneficios y aplicaciones de CDP

CDP descubre y entrega información de los equipos vecinos que se encuentran directamente conectados, esta información puede ser útil en una variedad de situaciones como:

4.7.1 Descubrimiento de dispositivos vecinos

CDP permite identificar los dispositivos conectados directamente a un switch o router Cisco, proporcionando información del equipo.

4.7.2 Diagnóstico de problemas de conectividad

CDP ayuda a detectar discrepancias en la configuración de dispositivos vecinos como VLAN nativas no coincidentes, estados dúplex incorrectos y enlaces con falla, permitiendo la solución de problemas.

4.7.3 Administración de redes grandes

En redes con gran cantidad de equipos, CDP permite a los administradores obtener una vista rápida del diagrama de red sin necesidad de acceder físicamente a cada equipo. Herramientas como Cisco DNA Center, Cisco Prime Infrastructure o Cisco Meraki Dashboard utilizan CDP para generar los mapas de red.

4.7.4 Optimización de redes virtualizadas

CDP puede operar en entornos virtualizados como VMWare, proporcionando información sobre la conectividad en ambientes virtualizados.

4.7.5 Monitoreo de consumo energético en dispositivos PoE

CDP puede reportar el consumo de energía de dispositivos conectados a puertos PoE, ayudando a optimizar la distribución de energía en la red.

4.7.6 Detectar dispositivos intrusos

Aunque CDP no está diseñado para administrar la seguridad, puede aportar información valiosa para mejorarla. Al proporcionar información de dispositivos conectados en la red, permite al administrador identificar dispositivos intrusos que hayan sido conectados sin autorización.

4.8 Análisis de Cisco Discovery Protocol y Simple Network Management Protocol

En el ámbito de la administración de redes, contar con herramientas que permitan tener una amplia visibilidad de equipos y eventos no sólo es necesario, sino fundamental. Utilizar las herramientas adecuadas nos permite recolectar toda la información requerida para una buena administración de la red. CDP y SNMP son esas herramientas clave que un administrador de red necesita, y por eso mismo, son los protocolos de gestión mayormente utilizados. Algunos aspectos importantes con relación a estos dos protocolos:

4.8.1 Diferencias y coincidencias de ambos protocolos.

Tanto CDP como SNMP son protocolos de redes, y aunque poseen algunas similitudes, también destacan algunas diferencias que se mencionan a continuación:

Similitudes:

- Ambos protocolos comparten un mismo objetivo, el de facilitar la administración y monitoreo de las redes de datos.
- Ambos permiten la recopilación de información de los dispositivos en la red, mientras SNMP permite obtener información de forma remota, CDP sólo permite obtener información de los equipos adyacentes.
- Ambos protocolos pueden proporcionar detalles sobre la configuración y estado de los dispositivos.

Diferencias:

- Propósito: CDP es propietario de Cisco y fue diseñado para descubrir dispositivos vecinos en la capa 2, mientras que SNMP es un protocolo estándar utilizado para la gestión y monitoreo desde capa 7.
- Compatibilidad: CDP funciona exclusivamente en equipos Cisco, mientras que SNMP es abierto para cualquier marca.
- Operación: CDP envía anuncios periódicos a dispositivos vecinos, mientras que SNMP permite el envío de mensajes tipo consulta y tipo notificación, pero lo hace hacia una estación central NMS que actúa como el cerebro del sistema.
- Seguridad: CDP no posee mecanismos de seguridad avanzada, pero SNMP en su tercera versión ofrece autenticación y cifrado.

4.8.2 Elección entre CDP y SNMP

Los dos protocolos son buenos en su ámbito, pero por su naturaleza hay escenarios en donde es mejor usar uno que el otro.

Uso de CDP:

- Descubrimiento de dispositivos vecinos: CDP es ideal para redes donde se tiene equipos Cisco, permitiendo obtener su información.
- Solución de problemas: CDP es útil para obtener información rápida sobre la topología de la red, sin necesidad de configuraciones adicionales.
- Telefonía IP: Los teléfonos IP de Cisco usan CDP para obtener información de DHCP y VLAN de voz para su configuración.
- Desde una perspectiva funcional, CDP es preferible en tareas de descubrimiento y documentación inicial de infraestructura donde se está elaborando la topología de la red.

Uso de SNMP:

- Monitoreo y gestión de red: SNMP es recomendado cuando se requiere recopilar métricas de rendimiento, estado de los enlaces, estado de los dispositivos (sin importar la marca). Se recomienda también para el envío de alertas vía correo electrónico.
- Automatización y control: SNMP es mejor cuando se trata no sólo de recopilar información sino también de realizar configuraciones, su trama permite aplicar configuraciones en sus agentes.
- SNMP es ideal para el monitoreo continuo, permitiendo almacenamiento de data histórica del comportamiento de la red para posterior análisis de tendencias de rendimiento

4.8.3 Fortalezas y debilidades

Como es de esperarse, cada protocolo posee sus fortalezas y debilidades que se mencionan a continuación:

Fortalezas de CDP:

- Descubrimiento rápido de dispositivos vecinos.

- No requiere configuración adicional, viene habilitado de fábrica.
- Útil para la solución de problemas y la identificación de topología.

Debilidades de CDP:

- Sólo funciona en equipos Cisco, limitando su uso en redes heterogéneas. Como su rival inmediato, LLDP es el protocolo abierto que puede operar en redes heterogéneas compuestas por dispositivos de otros fabricantes, su ejecución permite obtener similar información que CDP. De la misma manera, trabaja en capa de enlace de datos. (Ali, 2023)
- Protocolo vulnerable a ataques y robo de información, seguridad deficiente.
- Sólo proporciona información de dispositivos directamente conectados.

Fortalezas de SNMP:

- Compatible con múltiples fabricantes, más estandarizado.
- Permite la gestión remota de los dispositivos.
- Permite la recopilación de métricas.
- Permite el envío de notificaciones.
- SNMPv3 ofrece seguridad más avanzada.

Debilidades de SNMP:

- Requiere implementación y configuración más avanzada para una gestión efectiva.
- Genera mayor flujo de datos en la red, pudiendo incluso provocar congestión en enlaces WAN de bajo rendimiento, sobre todo en eventos tipo notificación.
- No proporciona información en tiempo real como lo hace CDP, depende de consultas periódicas.

- Menos eficaz para descubrir automáticamente dispositivos nuevos.

CAPITULO 5: DEMOSTRACION PRACTICA DEL FUNCIONAMIENTO DE SNMP Y CDP

5.1 Descripción del escenario

De forma inicial se planteó la propuesta de realizar un laboratorio simulado en Packet Tracer, sin embargo, para poder tener un enfoque más académico y relevante, se optó por hacer el laboratorio con equipos reales cuyos resultados son más confiables que los obtenidos a través de un simulador.

Para la demostración del funcionamiento de CDP y SNMP se realizará un laboratorio en una red LAN de una empresa mediana. Esta empresa posee algunos departamentos como compras, logística, mantenimiento, entre otros, los cuales están distribuidos en diferentes edificios a lo largo de un campus corporativo. Cada edificio-oficina cuenta con un switch para dar acceso a sus usuarios, y todos los switches del campamento se enlazan al router principal formando la LAN de la empresa.

Debido al crecimiento de la infraestructura y la necesidad de mantener una administración eficiente, se requiere mejorar la visibilidad de los dispositivos de red mediante protocolos de descubrimiento y monitoreo.

Históricamente, la red se ha monitoreado exclusivamente mediante SNMP, lo cual ha limitado la visibilidad topológica, especialmente ante la conexión de dispositivos no autorizados. En este contexto, se propone complementar SNMP con CDP para evaluar si se mejora la visibilidad, detección y la gestión proactiva de la red.

5.2 Topología de red

La red de la empresa está creada formando una topología híbrida, por una parte, tenemos al router a la cabeza y como equipo principal, y en los niveles inferiores se encuentran los switches ramificados hacia abajo (topología jerárquica). Estos switches en

algunos casos actúan como switches de distribución y dan conectividad a otros switches en niveles más inferiores, formando también una topología en estrella. Los equipos que podemos encontrar son principalmente de dos modelos:

- Router: Cisco 4331
- Switches: Catalyst 2960

El diagrama de topología se ilustra a continuación:

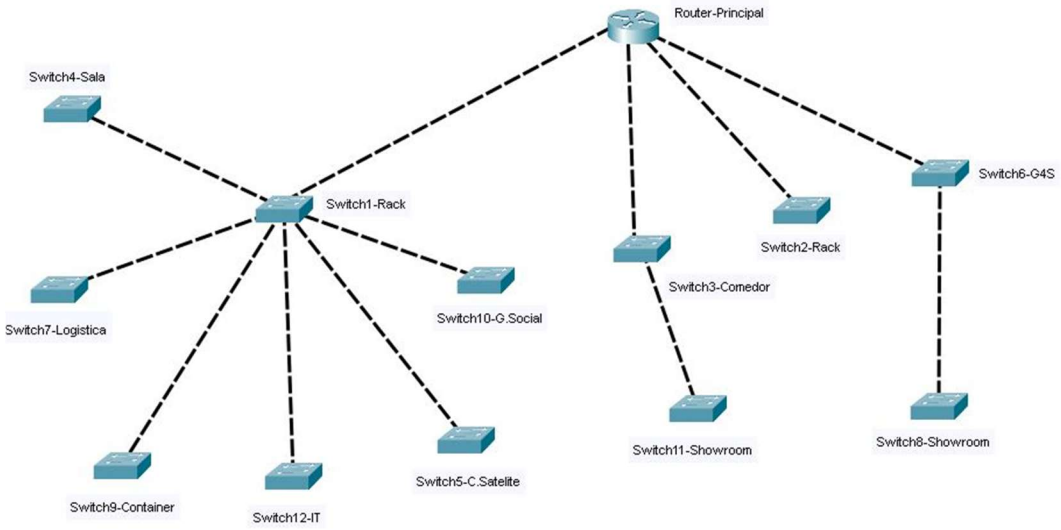


Figura 18. Topología de Red. Elaboración propia

5.3 Ambiente de trabajo

Para ejecutar el monitoreo de la red con SNMP se ha instalado la aplicación PRTG Network Monitor. PRTG es un software de monitoreo de redes, diseñado para supervisar de forma centralizada toda la infraestructura de TI. Aunque el aplicativo es pagado, posee también una versión gratuita que permite tener hasta 100 sensores de monitoreo de por vida. El software ha sido instalado en una estación de trabajo y cumple el rol de NMS, si bien PRTG soporta todas las versiones de SNMP, se ha configurado SNMPv2c ya que es la más utilizada en todo el mundo.

El entorno cuenta con un router Cisco 4331 y 12 switches Catalyst 2960, y da servicios a 120 usuarios directos y 20 visitantes. La red se encuentra segmentada en VLANs para seccionar el tráfico por servicios. Los equipos tienen una VLAN nativa, que es la 1 que viene por defecto, misma que se utiliza en los enlaces troncales.

Los enlaces troncales sirven para interconectar los switches, y el router se encarga del enrutamiento inter-VLAN. Todas las interfaces de los switches y el router han sido configurados con CDP habilitado.

5.4 Conjunto de pruebas planteado

Una vez que la red ya se encuentra configurada y en funcionamiento, vamos a realizar las pruebas de operación de ambos protocolos:

5.4.1 Comprobación de activación y funcionamiento

Para verificar que SNMP se encuentra operando, en el software de PRTG se debe realizar algunas validaciones:

- Primero, ingresamos a la configuración de PRTG y revisaremos el “Log de inicio de sistema”, asegurándonos que no haya alertas o mensajes de error.

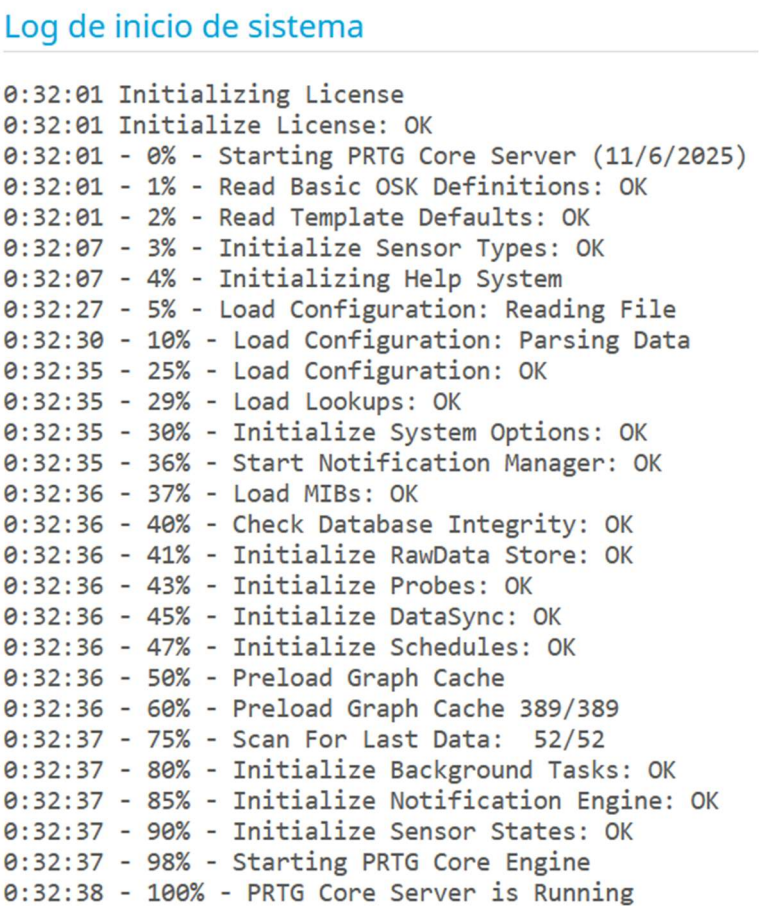


Figura 19. Inicio de SNMP y PRTG. Obtenido de PRTG Network Monitor

- Luego, revisamos que el nombre de comunidad se encuentre correctamente configurado. En este caso utilizaremos “altichama” con SNMPv2c.

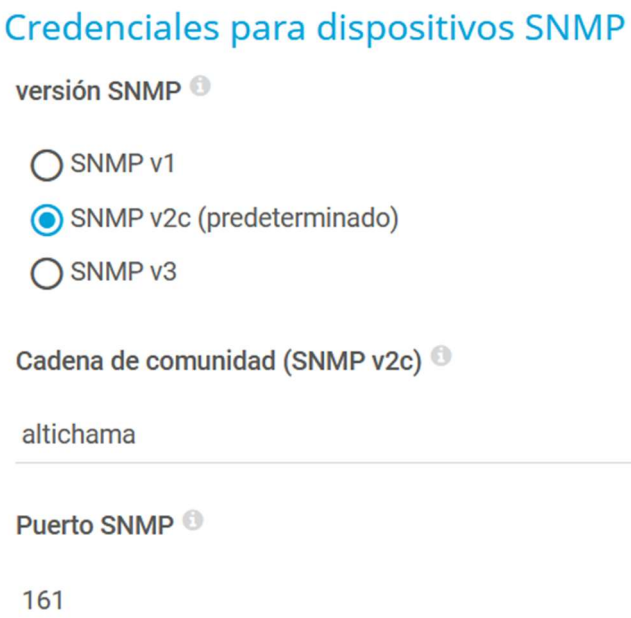


Figura 20. Configuración de comunidad y puerto de SNMP. Obtenido de PRTG Network Monitor

- Una vez que se ha realizado las configuraciones más básicas, podemos ver que el servidor Raíz de PRTG y la Sonda local se encuentran en verde, indicando su correcto funcionamiento.

Figura 21. Comprobación de SNMP activo. Obtenido de PRTG Network Monitor

- Finalmente, comprobamos que SNMP se encuentra operativo porque ya comenzamos a recibir datos de nuestros equipos.

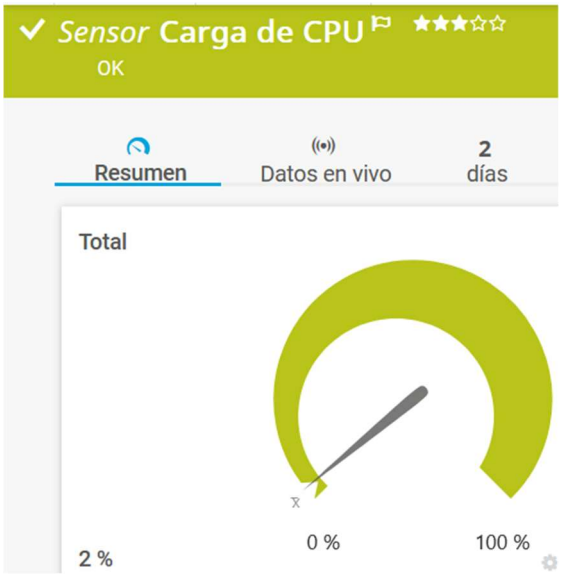


Figura 22. Sensor de SNMP de consumo de CPU. Obtenido de PRTG Network Monitor

Aunque CDP viene habilitado de fábrica e inicia tan pronto se encienden los equipos, para comprobar que se encuentra activo es necesario ingresar a la configuración de cada uno de los equipos y verificarlo manualmente. Para ingresar a los equipos utilizaremos el software putty, a través de una conexión SSH.

```
Router-Principal#show cdp
Global CDP information:
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is enabled
Router-Principal#
```

Figura 23. Captura que muestra a CDP activado. Elaboración propia

En la Figura 23 podemos ver que CDP se encuentra activo en el Router-Principal, enviando paquetes CDP cada 60 segundos y con un TTL de 180 segundos. Además, se aprecia que la versión que está ejecutando es CDPv2.

5.4.2 Propagación e información obtenida

Luego de comprobar que SNMP y CDP se encuentran activos y en funcionamiento, vamos a revisar la información que podemos obtener de ellos.

SNMP es un protocolo muy completo que permite el monitoreo de una amplia gama de variables (OIDs) de los equipos. Algunos ejemplos a continuación:

- Monitoreo del ancho de banda

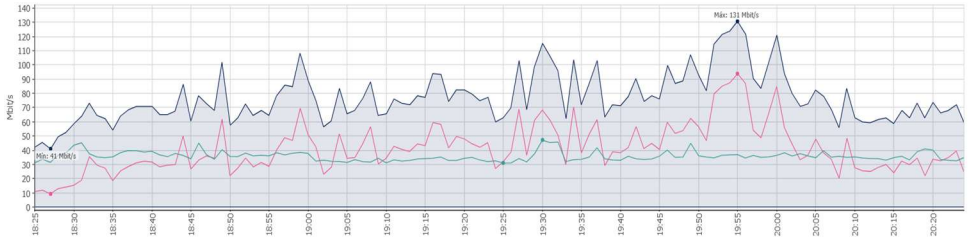


Figura 24. Monitoreo de ancho de banda. Obtenido de PRTG Network Monitor

- Monitoreo de ping

Figura 25. Monitoreo de ping. Obtenido de PRTG Network Monitor

- Monitoreo de almacenamiento en disco

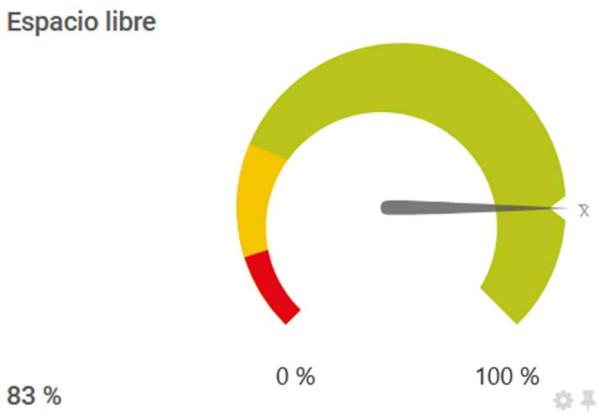


Figura 26. Monitoreo del almacenamiento. Obtenido de PRTG Network Monitor

- Monitoreo de consumo de memoria RAM

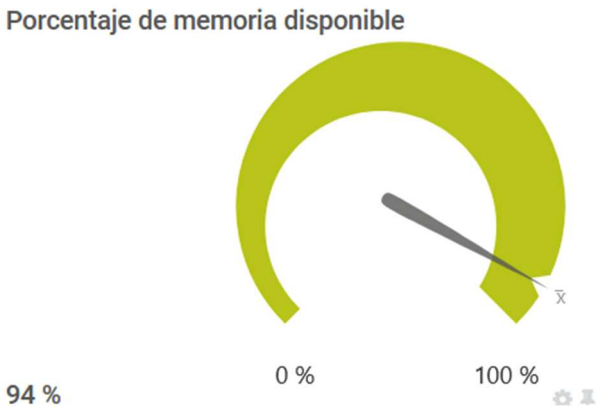


Figura 27. Monitoreo de memoria. Obtenido de PRTG Network Monitor

- Monitoreo del tiempo de actividad

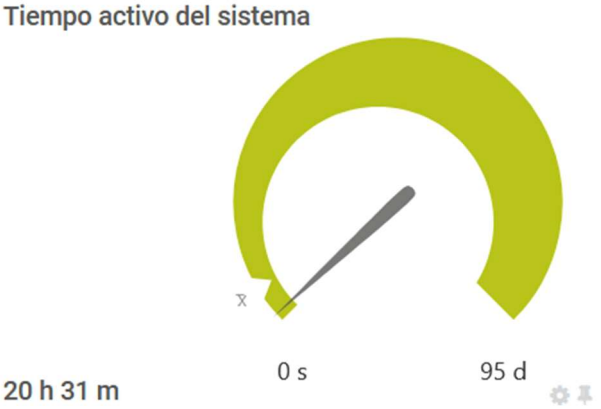


Figura 28. Monitoreo de tiempo de actividad. Obtenido de PRTG Network Monitor

Ahora vamos a revisar la propagación de CDP y la información que nos muestra.

```
Switch1-Rack#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID     Local Intrfce   Holdtme    Capability   Platform     Port ID
Switch5-C.Satelite
              Fas 0/7         159            S       2960         Fas 0/1
Switch9-Container
              Fas 0/4         159            S       2960         Fas 0/1
Switch7-Logistica
              Fas 0/3         159            S       2960         Fas 0/1
Switch12-IT   Fas 0/5         159            S       2960         Fas 0/1
Switch4-Sala
              Fas 0/2         159            S       2960         Fas 0/1
Switch10-G.Social
              Fas 0/6         159            S       2960         Fas 0/1
Router-Principal
              Fas 0/8         159            R       ISR4300      Gig 0/1/2
Switch1-Rack#
```

Figura 29. Dispositivos vecinos CDP. Elaboración propia

En la Figura 29 podemos ver que para el equipo Switch1-Rack hay varios vecinos CDP registrados, lo cual es correcto si lo revisamos en la imagen de la topología de red (Figura 18). Además, en esta imagen podemos encontrar la siguiente información:

- El equipo Switch5-C.Satelite es un equipo de plataforma 2960, y se lo puede alcanzar por la interfaz Fas 0/7.
- El equipo Switch9-Container es un equipo de plataforma 2960, y se lo puede alcanzar por la interfaz Fas 0/4.
- El equipo Switch7-Logistica es un equipo de plataforma 2960, y se lo puede alcanzar por la interfaz Fas 0/3.
- El equipo Switch12-IT es un equipo de plataforma 2960, y se lo puede alcanzar por la interfaz Fas 0/5.
- El equipo Switch4-Sala es un equipo de plataforma 2960, y se lo puede alcanzar por la interfaz Fas 0/2.
- El equipo Switch10-G.Social es un equipo de plataforma 2960, y se lo puede alcanzar por la interfaz Fas 0/6.
- El equipo Router-Principal es un equipo de plataforma ISR4300, y se lo puede alcanzar por la interfaz Fas0/8.

Además de lo mencionado, también podemos observar en la Figura 29 que el TTL (HoldTime) para los equipos es de 159 segundos restantes, sus capacidades son de switch (S) o router (R) y también vemos la interfaz con la que cada equipo se conecta hacia el Switch1-Rack (Port ID).

Para obtener información más detallada de un equipo vecino ejecutamos el comando *show cdp neighbors detail* como se muestra a continuación:

```
Switch8-showroom#show cdp neighbors detail

Device ID: Switch6-G4S
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: FastEthernet0/1, Port ID (outgoing port): FastEthernet0/2
Holdtime: 145

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen

advertisement version: 2
Duplex: full

Switch8-showroom#
```

Figura 30. Información detallada de vecinos. Elaborado por el autor

En este caso se ejecutó el comando en el Switch8-Showroom, y nos muestra la información adicional de su único vecino, el Switch6-G4S. Los datos que se agregan en esta vista son: Versión del sistema operativo, versión de CDP y tipo de dúplex.

En este punto es importante resaltar que, aunque SNMP puede monitorear una gran cantidad de variables y obtener información importante de ellas, los datos obtenidos con CDP son únicos, y no se los puede extraer con SNMP, siendo ésta una ventaja del uso conjunto de ambas herramientas.

5.4.3 Pruebas realizadas

Para comprobar la efectividad y el valor agregado que ofrece CDP en este laboratorio, se ha procedido a conectar un switch adicional, simulando un equipo intruso.

```
Switch11-Showroom#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
Switch3-Comedor
             Fas 0/1          120            S       2960        Fas 0/2
Switch       Fas 0/2          164            S       2950        Fas 0/1
Switch11-Showroom#
```

Figura 31. Dispositivo intruso. Elaborado por el autor

En la Figura 31 podemos ver cómo CDP "detecta" de forma inmediata al equipo no autorizado, el cual es de Plataforma 2950 y ha sido conectado al Switch11-Showroom. Este es una ventaja de CDP, permitiendo identificar el nuevo equipo conectado, dando

alerta al administrador y a la vez permitiendo actualizar la topología de la red si así lo amerita. Este descubrimiento de un nuevo equipo conectado, no es posible realizarlo con SNMP.

Otra prueba realizada, ha sido la desconexión intencional de un dispositivo, simulando la caída del enlace o fallas propias del equipo. Los resultados que se obtuvieron con esta prueba son los siguientes:

En el caso de SNMP se ha detectado la falla de forma inmediata, y se envía un paquete tipo trap notificando el evento al NMS con el PRTG instalado. La falla se puede visualizar enseguida en el tablero de control como se observa en la imagen a continuación:

Figura 32. Equipo caído - SNMP. Obtenido de PRTG Network Monitor

Como valor adicional de SNMP se resalta el envío de alertas/notificaciones por correo electrónico si se lo configura.

En el caso de CDP la caída se puede visualizar una vez que el tiempo restante de TTL finalice.

```
Switch1-Rack#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID     Local Intrfce   Holdtme    Capability   Platform     Port ID
Switch5-C.Satelite
              Fas 0/7         173            S       2960         Fas 0/1
Switch9-Container
              Fas 0/4         173            S       2960         Fas 0/1
Switch7-Logistica
              Fas 0/3         173            S       2960         Fas 0/1
Switch12-IT   Fas 0/5         113            S       2960         Fas 0/1
Switch4-Sala
              Fas 0/2         173            S       2960         Fas 0/1
Switch10-G.Social
              Fas 0/6         173            S       2960         Fas 0/1
Router-Principal
              Fas 0/8         159            R       ISR4300      Gig 0/1/2
Switch1-Rack#
```

Figura 33. Dispositivos vecinos CDP 2. Elaborado por el autor

En la Figura 33 vemos que el Switch12-IT pese a que ha sido desconectado, todavía se encuentra en la tabla de vecinos con un TTL restante de 113 segundos. Luego de transcurrido ese tiempo el equipo ya no aparece registrado:

```
Switch1-Rack#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
Switch5-C.Satelite
             Fas 0/7         120            S       2960        Fas 0/1
Switch9-Container
             Fas 0/4         120            S       2960        Fas 0/1
Switch7-Logistica
             Fas 0/3         120            S       2960        Fas 0/1
Switch4-Sala
             Fas 0/2         120            S       2960        Fas 0/1
Switch10-G.Social
             Fas 0/6         120            S       2960        Fas 0/1
Router-Principal
             Fas 0/8         166            R       ISR4300     Gig 0/1/2
Switch1-Rack#
```

Figura 34. Dispositivos vecinos CDP 3. Elaborado por el autor

5.5 Análisis de resultados

Los hallazgos clave del laboratorio son:

- SNMP permite el monitoreo remoto de dispositivos, mientras que CDP sólo puede ver información de los dispositivos vecinos.
- SNMP permite realizar monitoreo y obtener métricas de rendimiento de los equipos, para CDP estas tareas están fuera de su alcance.
- A través del uso de una estación central de monitoreo, SNMP puede almacenar información histórica y elaborar indicadores de desempeño, CDP en cambio sólo puede obtener la información en vivo.
- CDP permitió una detección inmediata de vecinos directamente conectados, facilitando la construcción de una topología precisa, incluso si no estaban configurados para ser monitoreados por SNMP.
- SNMP mostró limitaciones en detección de nuevos nodos, a menos que se conociera previamente su dirección IP.

- El retardo promedio de descubrimiento (delay) fue de 60 segundos para CDP, gracias a su frecuencia de anuncios por defecto. En contraste, SNMP presentó un delay de 5 minutos, equivalente al intervalo de sondeo por defecto.
- Al simular fallas, CDP dejó de recibir anuncios de dispositivos caídos de forma inmediata, lo que permitió identificar rápidamente cambios en la red sin depender de alertas externas.
- Se identificaron riesgos de seguridad al utilizar ambos protocolos: CDP, al ser un protocolo propietario sin cifrado, expone detalles técnicos de cada dispositivo; y SNMPv2c, al utilizar comunidades de texto plano, puede ser explotado, en especial si se usa el valor “public” que viene por defecto en los equipos.

CONCLUSIONES

- Cisco Discovery Protocol es un protocolo que permite obtener información muy útil de los dispositivos, pero, al tratarse de un protocolo propietario, tiene la desventaja que funciona únicamente en equipos de marca Cisco. SNMP, por el contrario, es un protocolo abierto, lo que le da la ventaja de operar con dispositivos de cualquier marca.
- Aunque ambos protocolos están orientados a la gestión de la red, su aplicación específica puede diferir un poco. Mientras CDP está enfocado en el descubrimiento y compartición de la información de los dispositivos, SNMP, en cambio, está enfocado en monitorear y generar indicadores del desempeño de la red. Además, permite la configuración de alertas al administrador, algo que está fuera del alcance de CDP.
- CDP puede mostrar información un tanto más estática y que no cambia con frecuencia, información intrínseca del dispositivo como: Versión del sistema, direccionamiento IP, tipo de dispositivo, etc. SNMP, por el contrario, está en capacidad de mostrar información que puede cambiar según el uso de la red, condiciones que varían en el tiempo como: Uso del procesador, uso de memoria, consumo de ancho de banda, estado de una interfaz, etc.
- La información de CDP se obtiene en vivo y no se almacena por sí sola, mientras que los datos de SNMP si son almacenados, lo que permite generar KPIs para el administrador de la red.
- CDP se vuelve particularmente útil y posee una ventaja frente a SNMP en la elaboración de la topología de la red, ya que, a través de sus funciones de descubrimiento e identificación de dispositivos, permite a los

administradores elaborar la topología y mantenerla actualizada con cada cambio que pueda presentarse en la red.

- A través de este laboratorio se ha comprobado que CDP complementa eficazmente a SNMP al ofrecer descubrimiento inmediato de vecinos y visibilidad topológica sin configuración adicional. Aunque SNMP sigue siendo vital para el monitoreo detallado del rendimiento, CDP ofrece ventajas significativas para la administración de redes complejas. Combinar ambos protocolos potencia la capacidad de gestión y diagnóstico de redes en ambientes corporativos.
- La experimentación demostró que el uso de CDP como complemento a SNMP mejora significativamente la visibilidad y trazabilidad física de los dispositivos en una red administrada. Si bien ambos protocolos tienen debilidades propias, su combinación estratégica resulta en una solución robusta que reduce los tiempos de detección, incrementa la capacidad de respuesta ante fallas y optimiza el monitoreo general de la infraestructura. La implementación de estas tecnologías, acompañada de buenas prácticas de configuración y seguridad, contribuye a una buena administración proactiva y eficiente en entornos empresariales en crecimiento.
- Se destaca el potencial del uso conjunto de CDP y SNMP para generar mapas de red mediante herramientas especializadas como Cisco Network Assistant o Cisco Meraki, lo que agiliza tareas como auditoría, inventario o mantenimiento preventivo.

RECOMENDACIONES

- Todas las redes empresariales, sin importar su tamaño, deben ser monitoreadas. Una adecuada gestión de la red permite asegurar su correcto funcionamiento.
- CDP es ideal para redes donde predominan los dispositivos Cisco, para redes de otras marcas se puede utilizar SNMP con LLDP por su apertura para diferentes fabricantes.
- Aunque SNMPv2c es la versión mayormente utilizada para la administración y monitoreo de redes, en un mundo donde la seguridad informática es cada vez más vulnerable, SNMPv3 puede ser una mejor alternativa a considerar, ya que ofrece controles de seguridad superiores a los de cualquier otra versión de SNMP.
- En toda implementación de SNMP que se realice, es conveniente cambiar el nombre de la comunidad “public” por otro diferente, ya que representa un riesgo para la seguridad.
- Implementar SNMP puede ser una mejor alternativa, ya que su campo de acción puede resultar más amplio que CDP. SNMP no sólo se enfoca en la administración y monitoreo de la red, sino que también puede monitorear aplicaciones, páginas web, servidores, sistemas operativos y otros usos más.
- Aunque los costos podrían incrementarse, puede ser muy útil para una empresa optar por un despliegue distribuido de SNMP, ya que la información puede ser más precisa, con menor latencia y con mayor redundancia.

BIBLIOGRAFIA

- Ali, H. (18 de 04 de 2023). *Protocolo de descubrimiento LLDP VS CDP: Comprensión de las Diferencias*. Obtenido de FIBERROAD: https://fiberroad.com/es/resources/glossary/lldp-vs-cdp-understanding-the-differences/
- Arciniega, F. (2023). *¿Qué son las Topologías de Red?* Obtenido de Mtro. Fernando Arciniega.com: https://fernandoarciniega.com/que-son-las-topologias-de-red/
- Bhattarai, D. (13 de February de 2020). *Cisco Discovery Protocol (CDP)*. Obtenido de The Cisco Learning Network: https://learningnetwork.cisco.com/s/article/cisco-discovery-protocol-cdp-x
- Bilbao, A. (21 de Abril de 2015). *Instalar red LAN con Fibra Óptica*. Obtenido de https://asierbilbaoibarguen.wordpress.com/2015/04/21/instalar-red-lan-con-fibra-optica/
- *Blog Altare | Tendencias Tecnológicas Y Digitalización*. (20 de Diciembre de 2022). Obtenido de Importancia De La Administración De Redes: https://altaresp.es/importancia-de-la-administracion-de-redes/
- CCNADESDECERO.es. (s.f.). *CCNA desde Cero*. Obtenido de Que es Cisco Discovery Protocol: https://ccnadesdecero.es/cisco-discovery-protocol-cdp/
- Cisco Community. (02 de 03 de 2019). *What is the difference between CDP versions 1 and 2?* Obtenido de https://community.cisco.com/t5/other-network-architecture-subjects/what-is-the-difference-between-cdp-versions-1-and-2/td-p/193318

- Cisco Systems. (2004). *Academia de Networking de Cisco Systems Guía del primer año CCNA 1 y 2 Tercera edición.* Madrid: PEARSON EDUCACION S.A.
- Cisco Systems. (17 de Julio de 2015). *Prácticas recomendadas para los switches Catalyst serie 6500/6000 y Catalyst serie 4500/4000 que ejecutan el software Cisco IOS*. Obtenido de Switches Cisco Catalyst de la serie 6500: https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-6500-series-switches/24330-185.html
- Creative Commons. (Mayo de 2009). *1.3 CABLE COAXIAL*. Obtenido de Guimi.net: https://guimi.net/monograficos/G-Cableado_estructurado/G-CEnode5.html
- ESCUELA DE EDUCACIÓN TÉCNICA NUMERO 2 LANUS. (s.f.). *TOPOLOGÍAS*. Obtenido de APLICACIONES ESPECIFICAS - REDES: https://eet2lanus.tripod.com/R_2.htm
- Fandom. (2012). *Network Operations and Control Wiki*. Obtenido de Fandom: https://tele9752.fandom.com/wiki/Xx5R
- FMUSER International Group INC. (18 de 10 de 2021). *¿Qué es la topología de bus? Trabajo y sus ejemplos*. Obtenido de Fmuser: https://es.fmuser.net/content/?20976.html
- NETWORK ENGINEERING. (Jan de 2017). *SNMP protocol MIBs & OIDs*. Obtenido de StackExchange: https://networkengineering.stackexchange.com/questions/36333/snmp-protocol-mibs-oids

- Network Working Group. (Mayo de 1990). *Request for Comments: 1157*. Obtenido de A Simple Network Management Protocol (SNMP): https://datatracker.ietf.org/doc/html/rfc1157
- Network Working Group. (December de 2002). *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*. Obtenido de Datatracker.ietf.org: https://datatracker.ietf.org/doc/html/rfc3418
- Network Working Group. (December de 2002). *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*. Obtenido de Datatracker.ietf.org: https://datatracker.ietf.org/doc/html/rfc3412
- Network Working Group. (December de 2002). *SNMP Applications*. Obtenido de Datatracker.ietf.org: https://datatracker.ietf.org/doc/html/rfc3413
- Network Working Group. (December de 2002). *Transport Mappings for the Simple Network Management Protocol (SNMP)*. Obtenido de Datatracker.ietf.org: https://datatracker.ietf.org/doc/html/rfc3417
- Network Working Group. (December de 2002). *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*. Obtenido de Datatracker.ietf.org: https://datatracker.ietf.org/doc/html/rfc3414
- Network Working Group. (December de 2002). *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*. Obtenido de Datatracker.ietf.org: https://datatracker.ietf.org/doc/html/rfc3416
- Network Working Group. (December de 2002). *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*. Obtenido de Datatracker.ietf.org: https://datatracker.ietf.org/doc/html/rfc3415
- Oracle. (2025). *SNMP MIB*. Obtenido de docs.oracle.com: https://docs.oracle.com/cd/E13203_01/tuxedo/tux91/snmpmref/1tmib.htm

- O'Reilly & Associates. (2002). *NMS Architectures*. Obtenido de https://docstore.mik.ua/orelly/networking_2ndEd/snmp/ch03_02.htm
- Ortiz, C. (s.f.). *Tipos de IP's y clases, A, B, C, D y E*. Obtenido de Cecomart: https://cecomart.com/tipos-ip-que-son-ventajas-clases/
- Pandora FMS. (s.f.). *¿Qué es SNMP? - Protocolo simple de gestión de redes*. Obtenido de Pandora FMS: https://pandorafms.com/es/it-topics/introduccion-a-snmp/
- SpringerNature. (01 de October de 2023). Obtenido de SpringerNature Link: https://link.springer.com/chapter/10.1007/978-981-99-5648-7_9
- Stallings, W. (2000). *Comunicaciones y Redes de Computadores* (Sexta ed.). New York: MacMillan.
- W0lf_F4ng. (12 de Apr de 2020). *Cisco Discovery Protocol (CDP)*. Obtenido de https://www.w0lff4ng.org/cisco-discovery-protocol-cdp/
- www.blogspot.com. (14 de Diciembre de 2015). *Comparación de cables*. Obtenido de www.blogspot.com: https://comparaciondecables.blogspot.com/2015/12/cable-stp.html