UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

PROGRAMACION DE REDES IP POR SOFTWARE
PARA LA REDUCCION EN LA COMPLEJIDAD
DE LA INGENIERIA DE TRÁFICO
EN UNA RED DE CAMPUS PARA APLICACIONES MULTIMEDIA

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:

GIANFRANCO TORI DE FLORIO

PROMOCIÓN
2007-II

LIMA-PERÚ
2014

PROGRAMACION DE REDES IP POR SOFTWARE PARA LA REDUCCION EN LA COMPLEJIDAD DE LA INGENIERIA DE TRÁFICO EN UNA RED DE CAMPUS PARA APLICACIONES MULTIMEDIA

A mi familia,
Que con su comprensión y apoyo
Están siempre conmigo

SUMARIO

En el presente informe se explica la aplicación de métodos alternativos a los tradicionales, para reducir la complejidad inherente a la administración de la red ante el aumento de la densidad de su equipamiento. La metodología es ilustrada mediante un caso de estudio consistente de una red de datos de quince equipos de comunicaciones de datos.

De manera extensiva, se presenta como aprovechar los beneficios de esta tecnología, incluso en el caso de que el equipamiento no soporte las metodologías más comerciales, se propone y desarrolla una metodología alternativa: el CLI Adaptado.

La importancia de la metodología presentada, es que los métodos tradicionales de configuración, que en un comienzo sirvieron para poder tener una red robusta, actualmente, debido a la poca escalabilidad de estos métodos y a la dependencia del conocimiento humano, ya no son adecuados para poder soportar nuevos tipos de tráficos y tendencias de virtualización de cómputo.

Este es el caso de la Línea de comandos (CLI), el principal medio para hacer configuraciones en el equipamiento de la red, cuanto mayor el tamaño de la red, más difícil la configuración, documentación y detección de fallas en la misma.

Ambas metodologías son desarrolladas y comparadas para presentar una conclusión de la aplicación de ellas en la administración de la red de datos.

ÍNDICE

INTRODUCCIÓN 1

CAPÍTULO I
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA 3

1.1 Descripción del problema 3

1.2 Objetivos del trabajo 3

1.3 Evaluación del problema 3

1.4 Alcance del trabajo 5

CAPÍTULO II
TEORÍA CONCEPTUAL DE REDES DE DATOS ACTUALES Y MODERNAS 7

2.1 Ingeniería de tráfico de multimedia para campus 7

2.2 Funcionamiento lógico de un equipamiento de red 8

2.2.1 Plano de Control 9

2.2.2 Plano de Datos 10

2.3 Métodos tradicionales de configuración de red 11

2.3.1 Líneas de Comandos - CLI 11

2.3.2 Network Management Systems – NMS 15

2.4 Método actual de Configuración de Red, el SDN 17

2.4.1 Openflow 19

2.4.2 ONE Platform Kit – ONE PK 21

2.5 Calidad de Servicio – QoS 23

2.5.1 Clasificación y Marcado 25

2.5.2 Encolado (queueing) y gestión de la congestión 27

2.6 Listas de Control de Acceso - Aplicaciones 29

CAPÍTULO III
METODOLOGÍA PARA LA SOLUCIÓN DEL PROBLEMA 31

3.1 Caso de estudio 31

3.2 Metodología para el caso de Estudio: CLI adaptado 32

3.3 Solución del problema 34

3.3.1 Solución usando CLI 34

3.3.2 Solución basada en SDN – APIC EM Controller (CLI Adaptado) 39

3.4 Análisis comparativo de ambas soluciones 47

CAPÍTULO IV
ANÁLISIS Y PRESENTACIÓN DE RESULTADOS 48

4.1 Tiempo de Ejecución 48

4.1.1 CLI tradicional 48
4.1.2 CLI adaptado 49
4.2. Costos del proyecto 51
CONCLUSIONES Y RECOMENDACIONES 53
ANEXO A
CONFIGURACIÓN DE NUEVO QOS MAP EN EL APIC-EM 55
BIBLIOGRAFÍA 62

INTRODUCCIÓN

Las metodologías de administración de redes de datos, desarrolladas en el este informe, se basan en la necesidad de reducir la complejidad de la ingeniería de tráfico en una red de campus para aplicaciones multimedia, en la cual el concepto de calidad de servicio es imprescindible.

Estas metodologías se denominan Software Defined Networking (SDN), que ofrecen una manera de rediseñar no solo la forma cómo la red opera sino también cómo se gestiona. Los más comerciales son;

- Openflow.- Considerado como el progenitor de toda la teoría y discusión existente en base a SDN. Este protocolo fue imaginado originalmente en el equipo de investigadores de redes en la Universidad de Standford. Su foco original era el permitir la creación de protocolos experimentales en redes de campus que pueda ser usado para investigación y experimentación,
- Cisco ONE Platform Kit (onePK).-Un paquete de desarrollo de software para programar características específicas de equipamiento Cisco y sistemas operativos de redes que permite acceso y control a un rango amplio de capacidades del equipamiento Cisco. Esto permite a las aplicaciones acceder a las capacidades de los equipos de red mediante el uso de API estándares.

El caso de estudio del presente informe, consiste de una red que posee quince equipos con la topología mostrada.

El informe está organizado en cuatro capítulos principales:

- Capítulo I "Planteamiento de ingeniería del problema".- En este capítulo se explica el problema de ingeniería y se precisa su objetivo. También se hace una evaluación de la problemática y se establecen los alcances del estudio desarrollado.
- Capítulo II "Marco teórico conceptual".- En él se exponen las bases teóricas conceptuales más importantes para la comprensión del sistema descrito en el presente informe. Se desarrollan los siguientes ítems: Ingeniería de tráfico de multimedia para campus, funcionamiento lógico de un equipamiento de red, métodos tradicionales de configuración de red, método actual de configuración de red (SDN), Calidad de Servicio (QoS), Listas de Control de Acceso.
- Capítulo III "Metodología para la solución del problema".- Este capítulo se enfoca en exponer la metodología para la solución del problema. Se procederá a explicar cómo,

mediante un ejemplo, opera el Controlador usando el concepto de CLI Adaptado. Esto permitirá entender las tareas que realiza el Controlador en el background. Luego de esta explicación de la operación, se procederá a mostrar la forma cómo se configura en el escenario de prueba QoS y la búsqueda de ACLs en la red tanto con el método tradicional, así como usando SDN. Finalmente se realiza un análisis comparativo entre el método tradicional y el moderno.

- Capítulo IV "Análisis y presentación de resultados".- Se desarrollan los aspectos relacionados al tiempo de ejecución y a los costos del proyecto.

CAPÍTULO I
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

En este capítulo se explica el problema de ingeniería y se precisa su objetivo. También se hace una evaluación de la problemática y se establecen los alcances del estudio desarrollado.

1.1Descripción del problema

Complejidad en la configuración de la ingeniería de tráfico en una red de campus para aplicaciones multimedia.

Imposibilidad en la aplicación de los métodos actuales de configuración de redes debido a las limitaciones del equipamiento de la red del caso de estudio.

Nota: La ingeniería de tráfico se refiere a todas las técnicas o protocolos que permiten que el tráfico circule por la red de una manera eficiente. Campus se refiere a las tecnologías de redes asociadas a redes empresariales.

1.2 Objetivos del trabajo

Aplicación de métodos alternativos a los tradicionales para reducir la complejidad inherente a la administración de la red ante el aumento de la densidad de su equipamiento.

Los métodos tradicionales (CLI y NMS) ya no son los adecuados para las características actuales de las redes. El método actual es el SDN (Software Defined Networking) en el cual se enfoca el presente informe, sin embargo, debido a una limitación del hardware del caso de estudio para soportar las metodologías más comerciales, se propone una metodología alternativa a ellas.

1.3Evaluación del problema

Los métodos tradicionales de configuración, que en un comienzo sirvieron para poder tener una red robusta, actualmente debido a la poca escalabilidad de estos métodos y a la dependencia del conocimiento humano, ya no son adecuados para poder soportar nuevos tipos de tráficos y tendencias de virtualización de cómputo.

Dado que no se contaba con una red en la cual las nuevas tecnologías para solucionar este problema fueran totalmente probadas, las investigaciones en este campo no tuvieron un progreso durante casi quince años. En sin no existían ambientes que estresen estas tecnologías y permitan así saber si ellas podrían tener aplicabilidad en la

GLOSARIO DE TÉRMINOS

ACL	Listas de Control de Acceso
AFxy	Assured Forwarding PHB
CBWFQ	Class-Based Weighted Fair Queueing
CDPI	Control Data-Plane Interface
CLI	líneas de comando
CoS	Class of Service
DiffServ	Diffentiated Services
DSCP	DiffServ Code Point
EF	Expedited Forwarding
FCAPS	Fault, Configuration, Accounting, Performance, Security
IOS	Internet Operating System
IP ECN	IP Explicit Congestion Notification
LAN	redes de área local
LLQ	Low Latency Queueing
NBI	Northbound Interfaces
NIDB	Network Information Database
NMS	Network Management Systems
ONF	Open Networking Foundation
PHB	Per-Hop Behaviours
QoS	Calidad de Servicio
SDN	Software Defined Networking
SNMP	Simple Network Managent Protocol
ToS	Type of Service
WAN	redes de área amplia
WRED	Weighted Random Early Detection

vida real. Los problemas que se enfrentaron durante las investigaciones fueron:

- El carácter cerrado del sistema operativo con el hardware del equipamiento, por el cual no se pudo acceder a redes que manejen alta densidad de tráfico.
- Las capacidades de hardware de los investigadores se concentraban netamente en equipos de bajo costo y baja densidad de puertos, o en equipamiento híbridos basados en procesamiento de PC, que no estaban preparados y no podían ser usados para el manejo de altos niveles de tráfico.

Desde el punto de los administradores de redes, su travesía empezó en un espacio de desarrollo y manejo de redes "empaquetadas" que se gestionaban de manera distribuida por cada equipo de manera independiente por línea de comandos y que requería un conocimiento a profundidad del equipamiento a nivel de configuración y diseño. Esto no era un problema hace veinte años en donde solo unas pocas empresas tenían el privilegio de tener redes de computadoras conectadas que generaban baja densidad de tráfico y por lo tanto requerían una cantidad de equipamiento mínima.

Todo cambió cuando aparecieron las primeras redes basadas en switches y las primeras tecnologías de movilidad inalámbrica, además de nuevas aplicaciones que comenzaron a estresar la red como lo fue inicialmente la voz, pasando por el video y finalizando en tecnologías de virtualización en el centro de datos. Todos estos cambios hicieron que la densidad de equipamiento en la red aumente considerablemente y por lo tanto la complejidad en la administración basado en el modelo tradicional de líneas de comando (CLI).

Las nuevas tecnologías de redes (calidad de servicio, multicast, seguridad en el control de acceso, etc.) soportaban estos nuevos tipos de tráfico. Estas nuevas tecnologías tenían como base fundamental la de proveer de inteligencia a cada uno de los elementos activos de la red, que desde el punto de vista tecnológico implicaba que cada elemento de red era una isla en sí misma, y desde el punto de vista de quien la opera significaba que la complejidad y conocimiento de cómo habilitar estas nuevas tecnologías se multiplicaba a razón de la cantidad de equipamiento existente en la red.

De la misma manera, la alta densidad de tráfico originada, y las nuevas maneras de cómo el usuario interactúa con la red hicieron que el proceso de resolución de problemas o "troubleshooting" ante fallas de conectividad o de seguridad tome un tiempo muy elevado de respuesta y un elevado conocimiento de la operación del equipamiento del administrador para poder entender en base a la información de logs/eventos originados por cada equipo el origen de dicho problema.

De lograr entender la causa y saber cómo resolverla, se vuelve al mismo paradigma inicial, en donde el administrador tiene que nuevamente entrar a cada uno de los equipos

y configurar de manera independiente los pasos de solución, lo que podría nuevamente agregar un punto de falla que no puede cubrir ningún tipo de tecnología: el error humano.

Se buscaron para ello métodos de gestión más fáciles de entender por los administradores de red como es el caso de los sistemas de gestión de redes o en sus siglas en inglés "Network Management Systems - NMS". Esto hizo que los administradores puedan en un punto centralizado gestionar la red, pero no resuelve todos los problemas adicionales como:

- El tiempo en que una herramienta NMS se actualice para soportar una nueva tecnología o una nueva versión de protocolos existentes en las redes es de meses, y en el durante se vuelve nuevamente a caer al mundo de la gestión por líneas de comando en cada uno de los equipos – Posible error humano.
- Nuevo equipamiento liberado al mercado requiere de una nueva actualización del NMS para poder soportarlo. – Tiempo de ida al mercado versus soporte de nuevas soluciones.
- La mayoría de soluciones NMS del mercado soportan solo una determinada marca de fabricante para la gestión, y de soportar múltiples fabricantes, solo se gestiona características básicas y no avanzadas desarrolladas por dicho fabricante – No interoperabilidad y por lo tanto no se explota la inversión realizada en hardware de red.
- El NMS es solo una máscara, en el "background" el NMS tiene que traducir las acciones creadas por el administrador en la interface gráfica a tareas de línea de comando de manera secuencial en cada uno de los equipos de red. – No es eficiente.

Ante estas problemáticas, nace desde el mundo de la investigación de redes e impulsado por la comunidad de ingenieros abocados a la gestión de las redes el concepto tecnológico llamado "Software Defined Networking" (SDN) como una manera de rediseñar no solo la forma cómo la red opera sino también cómo se gestiona.

Sin embargo, dado que frecuentemente se suelen encontrar redes con equipamiento antiguo, e incapaces de soportar las tecnologías de configuración SDN, es que en el presente informe se desarrolla y presenta una alternativa que compense esta limitación y que provea similares ventajas a la tecnología SDN.

1.4Alcance del trabajo

En este informe se explica cómo, mediante el uso de Controladores bajo el concepto de SDN, se reduce la complejidad en la gestión.

En este informe se comparan los métodos tradicionales de configuración de redes y los métodos basados en SDN mediante un ejemplo de ingeniería de tráfico multimedia usando los siguientes conceptos:

- Configuración de Calidad de Servicio en la red.
- Identificación de cortes de flujo de tráfico debido a listas de control de acceso.

El informe es desarrollado de modo tal que sea un material de consulta para los administradores de redes que deseen tener un primer alcance sobre esta tecnología y les permita conocer las ventajas de la programación de la red basada en software.

Debido a que SDN es una tecnología relativamente nueva y en fase de definición formal, el presente informe busca recoger la información más actualizada liberada en el mercado y basar su análisis en lo que se considera el modelo de SDN: Red – Interfaces Southbound - Controlador – Interfaces Northbound – Aplicaciones.

El alcance general del trabajo y de lo que se va a exponer es el siguiente:

- La problemática de la gestión de la red que cubre SDN es un caso particular de aplicabilidad de SDN. Esta tecnología puede cubrir otras necesidades importantes de campus como es la segmentación de la red, seguridad en el control de acceso, probar nuevos protocolos diferentes al IP, creación de redes experimentales que usen el estrés del tráfico en los equipamientos, etc.
- El caso ejemplo solo considera el tráfico de video para la comparación de las soluciones debido a que es más fácil entender problemas de red que afecten un flujo de video. Esto no implica que no pueda utilizarse otro tipo de tráfico.
- Se ha considerado un caso típico de oficina principal con oficina remota. El diseño de ambas puede variar por empresa. Se ha recogido un diseño estándar que cubra las mejores prácticas de diseño como es el uso de acceso/core para la LAN, doble salida de Internet para la WAN y un único router de oficina remota.
- Se entiende que en el presente informe no se presentará las configuraciones desde el lado del sistema de video. Este sistema para casos del presente informe, se encuentra operativo y funcionando, incluyendo ya el proceso de registro y estando en la fase de envío y recepción de video.
- Se usará en el presente informe como referencia equipamiento y tecnología de la marca Cisco, al ser la marca que tiene mayor presencia y posicionamiento de mercado internacional. Por consiguiente, cualquier problemática que se descubra en el presente documento, es también aplicable a cualquier otro fabricante del mercado que use los conceptos de plano de control residente en cada equipamiento de red.
- La solución se dará en base a desarrollos del fabricante Cisco el cual tiene soluciones bajo el concepto de SDN. Esto no quiere decir que otros fabricantes no puedan tener la misma tecnología, pero la comparación de las ventajas o no de Cisco frente a otros fabricantes no es fin de este informe.

CAPÍTULO II
MARCO TEÓRICO CONCEPTUAL

En este capítulo se exponen las bases teóricas conceptuales más importantes para la comprensión del sistema descrito en el presente informe.

2.1 Ingeniería de tráfico de multimedia para campus

La Ingeniería de Tráfico es definida de acuerdo al RFC 3272 como "el aspecto dentro de la ingeniería de redes que tiene que afrontar la problemática de la evaluación del rendimiento y la optimización del rendimiento de redes operacionales IP". Bajo este concepto formal, el poder mejorar el rendimiento de la red, tanto a nivel de tráfico como de recursos son objetivos fundamentales de la ingeniería de tráfico. Esta definición es general y aplica para casos propios del Internet. El propósito de la definición de Ingeniería de Tráfico para Campus, es adaptar los conceptos usados en Internet a una aplicación de redes empresariales, y más específico aún a tráfico propio multimedia [1].

Las redes en general existen para poder hacer transferir información desde un punto origen hasta un punto destino. En esta definición no solo se debe de contar con el aspecto de cómo lograr comunicar ambos puntos, sino hacerlo de una manera en que entreguemos en ambos casos una correcta calidad en la recepción de la información Desde el punto de vista de la comunicación, la ingeniería de tráfico permite el control y la optimización de las rutas necesarias para el tráfico llegue al destino, pudiendo en determinados casos dirigir el tráfico a rutas alternas que tengan mejores indicadores de retardo y jitter, o que desde la economía del networking haga que sea más económico el tomar una ruta alternativa a la principal. Adicionalmente a ello, el identificar los caminos adecuados y si estos caminos están preparados para permitir el tráfico interesante. Esta capacidad de la ingeniería del tráfico es la más distintiva dentro de las muchas capacidades que se tiene.

Otra capacidad de la ingeniería de tráfico, y que se ha vuelto de gran importancia para estudios y análisis es la ingeniería de tráfico aplicado hacia el rendimiento visto por los usuarios finales. Las características que el usuario final puede percibir son propiedades emergentes de la red. Estas propiedades incluyen ciertos indicadores importantes como puede ser la latencia, el retardo, el jitter, velocidad de transferencia, etc. Estas propiedades se pueden definir de la siguiente manera:

- Retardo: Es el tiempo que tarda una señal para atravesar un conductor o un dispositivo.
- Latencia: Es la suma de retardos temporales dentro de una red. Por ejemplo, una información para llegar a su destino, tiene que ser procesada por el computador, pasar por el stack IP, ser transportado a través de la red, la red tiene múltiples elementos, procesado por el receptor y presentado al usuario final. Todos estos puntos desde donde inicia la comunicación hasta donde termina, agregan de manera independiente retardos. La latencia es la suma de todos los retardos.
- Jitter: Desde el lado del transmisor, los paquetes son enviados en un flujo continuo, con los paquetes uniformemente espaciados. Debido a problemas de red (congestión, errores de configuración, etc), estos paquetes transmitidos llegan al receptor de manera no uniforme, con retardos distintos entre ellos. La variabilidad de esos retardos, se define como jitter.
- Velocidad de transferencia: Es la velocidad con la cual la información es procesada y enviada a la red. Desde el punto de vista de usuario final, es los Mbps de subida o bajada de la información.

Estas propiedades pueden afectar directamente la experiencia del usuario final y son muy evidentes especialmente cuando el usuario final trabaja con aplicaciones de misión críticas como es el caso de voz y video.

Para solucionar estos problemas, la ingeniería de tráfico se concentra en los aspectos de optimización a través de la gestión de la capacidad y la gestión del tráfico. En la parte de gestión de tráfico, se incluye funciones de control de tráfico que está muy ligado a la calidad de servicio - QoS (priorización tráfico, manejo de colas, etc.).

Para el caso del presente documento, se está trabajando en una red empresarial que está pasando tráfico multimedia. Desde el punto de vista de la Ingeniería de Tráfico, aplicaremos la optimización de la red mediante la gestión del tráfico usando Calidad de Servicio y la optimización de rutas mediante la identificación de caminos que puedan interrumpir el flujo de tráfico.

2.2 Funcionamiento lógico de un equipamiento de red

El equipamiento de red es el encargado de poder establecer un camino de comunicación entre dos puntos finales o hosts, usando como protocolo de transporte, en la mayoría de casos, el protocolo IP. Este camino de comunicación se puede separar en redes de área local (LAN) o en redes de área amplia (WAN). Tomando como referencia que el alcance del presente documento es basado en una red Empresarial o Enterprise, se puede tomar en consideración que para las redes LAN y WAN se usa equipamiento de red especializado: switches y routers respectivamente [2].

En general todo equipamiento de red funcionalmente consta de tres partes o planos:

- Control
- Gestión
- Datos

Siendo en la mayoría de los casos el plano de gestión embebido dentro del plano de control. Para simplicidad de este trabajo, cada vez que se haga referencia de la gestión en el plano de control, se estará implícitamente mencionando al plano de gestión. En la figura 2.1 se muestra un diagrama lógico de cómo se compone un equipo que servirá de guía para las definiciones de los Planos.

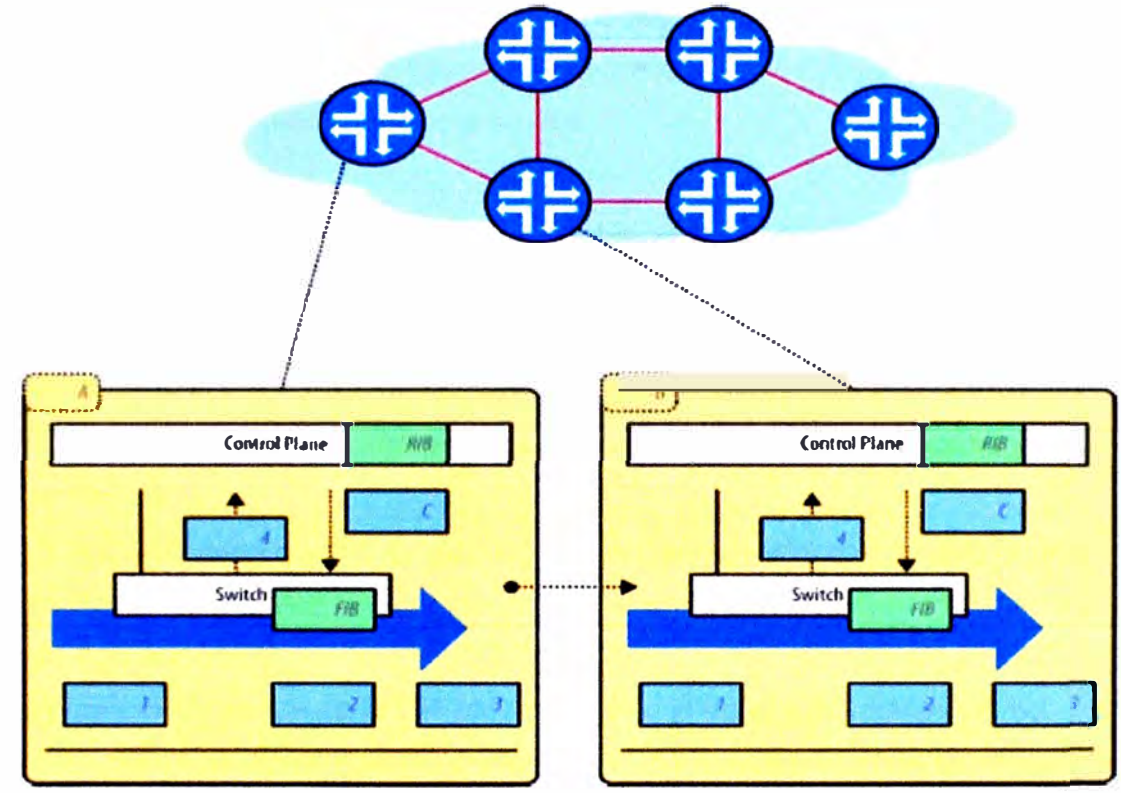


Figura 2.1 Plano de control y de datos en una red típica (Fuente: Ref. [2])

A continuación se definirá el uso de los planos de control y de datos, en el funcionamiento de un equipamiento de red.

2.2.1 Plano de Control

Es un componente que se encarga de cómo un equipamiento particular interactúa con equipamiento vecino mediante el intercambio de estados o señalización dentro de la red. Se encarga también de tener una vista e información del mapa topológico de la red lo cual define qué se hace con los paquetes entrantes a un equipamiento (acciones a realizar en el plano de datos) [2].

Esta información se llama "routing information base - RIB". El RIB siempre busca ser consistente con la información y evita que hayan caminos cerrados o "loops" en la red que podrían generar problemas en el "forwarding" gracias a que otras instancias de plano de control residentes en otros equipamientos comparten también su información de redes

directamente conectadas o redes aprendidas por otros vecinos. La comunicación entre distintos planos de control para el intercambio de información entre diferentes elementos de red se hace a través de protocolos especializados como lo son los protocolos de enrutamiento.

Luego del establecimiento del RIB, las entradas de "forwarding" son colocadas en una tabla, que comúnmente se le llama "forwarding information base - FIB" que es reflejada hacia el plano de datos. Esta FIB contiene información de cómo un paquete debe de ser enviado por la red, las rutas que debe de tomar para llegar a su destino, y las rutas alternas en caso la principal no se encuentre disponible. En el tiempo la información dentro del FIB puede cambiar mediante el intercambio de información entre los distintos planos de control, y la re-convergencia de RIB.

Conclusión:

Desde un punto de vista sencillo de entender, el Plano de Datos es el cerebro en los equipos de red. Desde el inicio de las redes, el Plano de Datos se encuentra en cada equipamiento de red de manera independiente.Esto conlleva a las siguientes problemáticas cuando se habla de redes de campus de gran escala:

- La cantidad de planos de control en una red es la cantidad de equipamiento que exista en la misma.
- Cada plano de control es configurado de manera independiente en cada equipo de red, aumentando la complejidad y el posible error humano en la configuración o actualización de las configuraciones.
- El plano de control reside en el CPU/Memoria propio del equipamiento de red, que suele ser fijo, con posibilidad casi nula de poder hacer una actualización de hardware. En caso existir la actualización, esta es dependiente de cada fabricante, y costosa en el tiempo.
- El plano de control de los equipos solo tiene visibilidad de las redes directamente conectadas y de la información que recibe a través de protocolos de enrutamiento con otros equipos de red. Esto trae como dificultad que tenga que existir una convergencia en el establecimiento del RIB y actualización del FIB entre diferentes protocolos, aumentando la interacción entre ellos, y potencialmente aumentando el tiempo de convergencia, que para tráfico tipo multimedia, podría ser perjudicial.
- Cualquier nueva actualización de software del sistema operativo del equipamiento que pueda cubrir vulnerabilidades o nuevas características tiene que hacerse en cada equipo de manera independiente, aumentando la complejidad en el mantenimiento de la red.

2.2.2 Plano de Datos

El plano de datos maneja los datagramas (forma de encapsulamiento usado en el modelo OSI para la comunicación de la información en redes de datos) que ingresan al

equipo (en el cobre, fibra o inalámbrico) a través de una serie de operaciones a nivel de enlace que recolectan los datagramas y se realiza revisiones de integridad. Un datagrama bien formado es procesado en el plano de data mediante consultas a su tabla FIB que son programadas con anterioridad por el plano de control. Cuando se tienen las decisiones en la tabla de FIB previamente, se le conoce como ruta rápida. Hay casos particulares en donde no se conoce que hacer con el paquete ya que no existe regla en el FIB, como el caso de un destino no conocido. En este caso particular, los paquetes son enviados al plano de control para que haya un mayor análisis usando RIB [2].

El envío de los paquetes al plano de control también se le conoce como ruta lenta, ya que se toma más tiempo en poder hacer el procesamiento de los paquetes debido a que hay que tomar nuevas decisiones que serán colocadas nuevamente en la table FIB.

Las acciones que toma el plano de datos con respecto al tráfico entrante, luego de hacer la revisión en la tabla FIB son las siguientes: reenvío (en casos especiales de tráfico multicast, replicación), drop, re-marcado, contabilizar y encolar. Adicionalmente a estas acciones, el plano de datos también puede realizar ciertos servicios adicionales como es el caso de Listas de Control de Acceso (ACL) y políticas de Calidad de Servicio (QoS).

Conclusión:

Desde un punto de vista sencillo de entender, el plano de datos vendría a ser la gran carretera de alta velocidad para la transferencia de información, y que en determinados casos, recurre al "cerebro – plano de control" para tomar la decisión de qué hacer con determinado tráfico. Esta comunicación, del plano de datos con el plano de control, trae de perse algunas problemáticas como las siguientes:

- Al hacer consultas de manera individual el plano de datos a un plano de control por equipos, la información toma una ruta lenta, lo cual puede llevar a retardos en la red, perjudiciales para tráfico multimedia.
- Al tener de manera local el plano de datos su dependencia con el plano de control, este tiene que esperar una actualización en su tabla de FIB, pudiendo estar esta información de cómo proceder en otro equipo que la tiene en su FIB de su plano de control.

2.3 Métodos tradicionales de configuración de red

A continuación se describirá dos de los métodos tradicionales de configuración: línea de comandos (CLI) y Sistemas de Gestión de Red (NMS – siglas en inglés).

2.3.1 Líneas de Comandos - CLI

La interfaz de la línea de comandos, conocida comúnmente como CLI, es un método que permite a las personas dar instrucciones a algún programa informático por medio de una línea de texto simple. Este tipo de comunicación persona-maquina existe desde hace

mucho tiempo, superada en antigüedad por las tarjetas perforadas [3].

Cabe señalar que la línea de comandos existe para diversos programas, diversos hardware y con diferente funcionalidad. En el ambiente de los administradores de redes, suele ser su principal medio para hacer configuraciones en el equipamiento o poder hacer troubleshooting de fallas en la misma.

Bajo el contexto del presente informe, se estará usando equipamiento Cisco. La estructura de la línea de comandos de Cisco, separa las sesiones en dos niveles de acceso: nivel usuario EXEC y nivel privilegiado EXEC. El nivel usuario EXEC permite el acceso solamente a comandos de monitoreo básico; el nivel privilegiado de EXEC permite acceder a todos los comandos de configuración, y a todos los modos de comando. Existen cinco modos de comando: global, modo configuración, modo de configuración de interface, modo de configuración de sub interface, modo de configuración de router, modo de configuración de línea.

a. Jerarquía de Comandos Cisco IOS

La figura 2.2 [3] provee un diagrama esquemático de la Jerarquía de Comandos Cisco IOS.

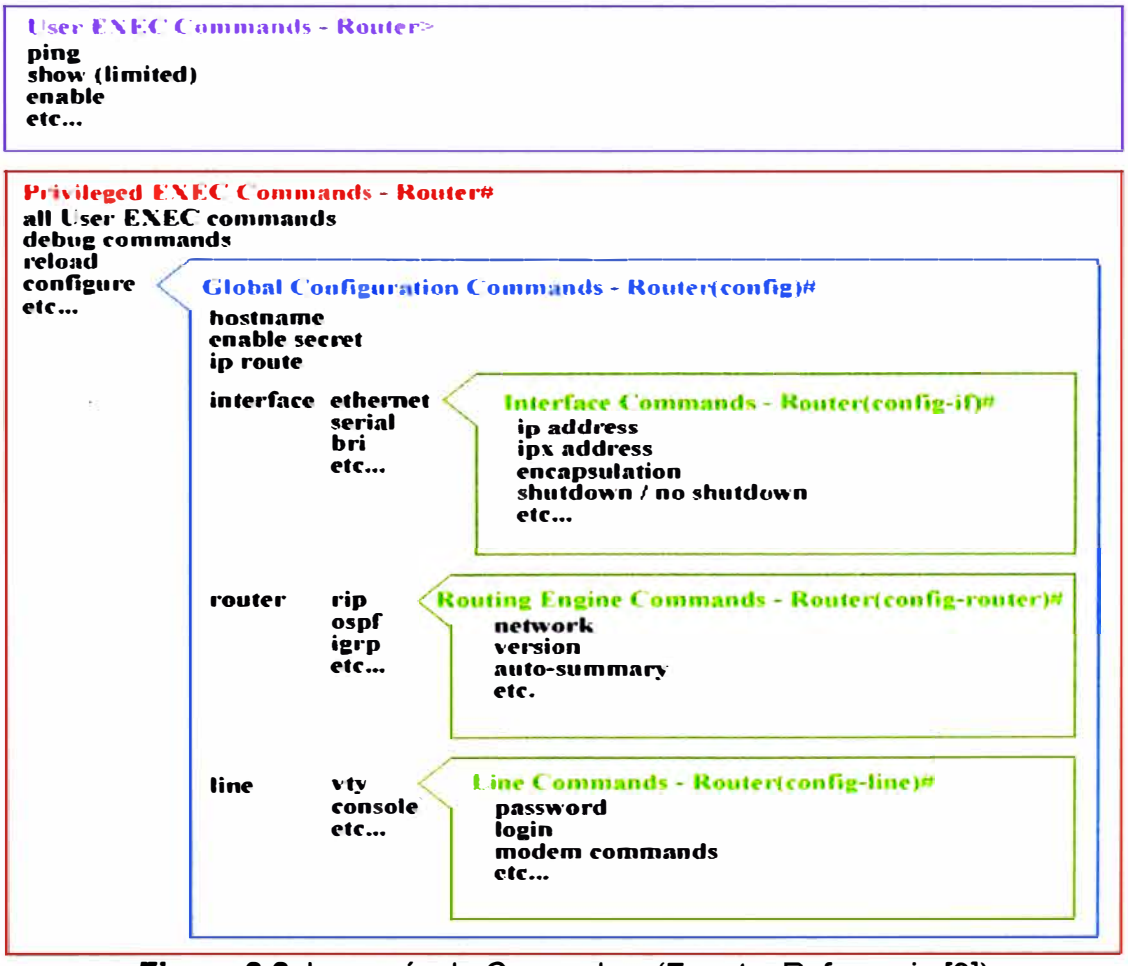


Figura 2.2 Jerarquía de Comandos (Fuente: Referencia [3])

Se observa que cuando una sesión EXEC es establecida, los comandos del IOS de

Cisco tienen una estructura jerárquica. El poder entender esta jerarquía es importante para poder configurar de manera efectiva el equipamiento de red.

Las opciones de los comandos varían de acuerdo a la posición dentro de la jerarquía. Mucho de los comandos no son disponibles hasta que se navegue a la posición jerárquica correspondiente dentro de la estructura de la línea de comandos (CLI). En el modo de configuración global por ejemplo, se tiene configuraciones generales de la plataforma, mientras que en un modo de configuración de interface, se tienen comandos específicos de configuración de interface.

Como guía referencial, la tabla 2.1 [3]muestra un ejemplo de la salida a nivel de línea de comandos versus la posición dentro de la jerarquía.

Tabla 2.1 Ejemplo línea de comandos vs. jerarquía (Fuente: Referencia [3])

Muestra Visual de la Línea de Comandos	**Referencia en la Jerarquía**
Router>	Modo usuario EXEC
Router#	Modo privilegiado EXEC
Router(config)#	Modo de Configuración (el símbolo de # indica que se encuentra este modo dentro del modo privilegiado EXEC)
Router(config-if)#	Nivel de Interface dentro del modo configuración
Router(config-router)#	Nivel de configuración del motor de enrutamiento dentro del modo de configuración. En general el nivel (config-XXXX) corresponde a la tecnología que requiera ser configurada.
Router(config-line)#	Nivel de línea (vty, tty, async) dentro del modo de configuración.

b. Ejemplo de configuración de calidad de servicio

A continuación se muestra una configuración ejemplo de calidad de servicio dentro de un switch Cisco Nexus 5000. Luego de la línea de comandos, se muestra en azul la explicación de su ubicación dentro del modelo jerárquico.

```
Router(config)# class-map type qos cmap-qos-acl
//Modo de Configuración Global
Router(config-cmap-qos)# match access-group ACL-CoS
Router(config-cmap-qos)# exit
//Nivel de configuración de Class-maps dentro del modo de configuración.

Router(config)# policy-map type qos pmap-qos-acl
//Modo de Configuración Global
Router(config-pmap-qos)# class cmap-qos-acl
//Nivel de configuración de policy-maps dentro del modo de configuración.
Router(config-pmap-c-qos)# set qos-group 4
Router(config-pmap-c-qos)# exit
Router(config-pmap-qos)# exit
```

```
//Nivel de configuración de qos dentro del nivel policy-maps en el modo de configuración.
Router(config)# system qos
//Modo de Configuración Global
Router(config-sys-qos)# service-policy type qos input pmap-qos-acl
Router(config-sys-qos)# exit
//Nivel de configuración de service-policy dentro del modo de configuración.

Router(config)# class-map type network-qos cmap-nq-acl
//Modo de Configuración Global
Router(config-cmap-nq)# match qos-group 4
Router(config-cmap-nq)# exit
//Nivel de configuración de qos dentro del nivel policy-maps en el modo de configuración.

Router(config)# system qos
//Modo de Configuración Global
Router(config-sys-qos)# service-policy type network-qos pmap-nq-acl
Router(config-sys-qos)# exit
//Nivel de configuración de service-policy dentro del modo de configuración.

Router(config)# policy-map type network-qos pmap-nq-acl
//Modo de Configuración Global
Router(config-pmap-nq)# class type network-qos cmap-nq-acl
//Nivel de configuración de network-qos dentro del nivel policy-maps en el modo de configuración.
Router(config-pmap-c-nq)# set cos 5
Router(config-pmap-c-nq)# exit
//Nivel de configuración de cos dentro de network-qos dentro del nivel policy-maps en el modo de configuración.
Router(config-pmap-nq)# exit
//Nivel de configuración de policy-maps dentro del modo de configuración.
```

Cada equipo dentro de una red de campus se diferencia de acuerdo a su uso, como de acuerdo a su función, y debido ello existen diferentes características del uso de la línea de comandos.

Enfocándose netamente en el presente documento de acuerdo al alcance, los equipos de redes a configurar Cisco poseen una línea de comandos especializada para su sistema operativo llamado IOS (Internet Operating System). Esta línea de comandos suele ser común para configuración y troubleshooting de características básicas en diversas plataformas que tienen este sistema operativo, y se empieza a diferenciar en sintaxis dependiendo del uso del equipamiento en la red, es decir de su rol dentro de la red. Por ejemplo, un equipo de core de campus, puede tener hasta 8 colas en calidad de servicio por puerto, en cambio un equipo de acceso campus, puede tener 4 colas por puerto. Pese a ser la misma configuración a nivel de tecnología (QoS), la sintaxis del primero incluye la posibilidad de configurar las 8 colas, mientras que del segundo se limitará a configurar solo 4.

De la misma manera, equipamiento Cisco que posee diferentes Sistemas Operativos (Ej: NX-OS, IOS, etc) tienen como base un común formato de configuración para temas básicos, pero difieren en cómo configurar de acuerdo a su función en la red. Por ejemplo,

un equipo con sistema operativo NX-OS, maneja funciones y por lo tanto protocolos especializados para centros de datos. Estos no son comúnmente usados en redes de campus donde el sistema operativo IOS es el predominante.

c. Conclusión

Como se podrá apreciar, el uso de CLI trae algunos de los siguientes inconvenientes:

- Para diferentes equipos de red, el administrador tiene que conocer diferentes formas de configurar los equipos.
- Cada configuración por líneas de comandos es por equipos, es decir, el administrador tiene que entrar a cada uno de los equipos aumentando la complejidad a factor de la cantidad de equipos en la red.
- Un administrador nuevo que desea hacer cambios a los equipos, tendría que entrar a cada uno de ellos para entender lo que se tiene configurado y como esta configuraciones interactúan con los demás equipos de red. Aumenta el tiempo de transferencia de información para nuevos administradores.
- Al tener muchos puntos de configuración, aumenta el tiempo para poner en marcha alguna nueva funcionalidad o nueva característica de red.
- Al tener muchos puntos de configuración, ante algún problema en la red, el hacer troubleshooting por líneas de comando es complejo, lento y dependiente de la experiencia del administrador.

2.3.2 Network Management Systems – NMS

Con el avance en las redes de datos, la gestión de la red entró en un punto de evolución debido a la complejidad en el manejo de la línea de comandos. Con la aparición de los Sistemas de Gestión de la Red (Network Management Systems – NMS) se logró aliviar la complejidad y la visibilidad de lo que sucede en la red. Estos NMS pertenecen a diferentes fabricantes especializados como CA, Solarwinds, Cisco, etc ofreciendo herramientas basadas en Web 2.0 que permiten a los administradores poder gestionar la infraestructura de red de una forma gráfica [11].

La mayor parte de los NMS en el mercado siguen las recomendaciones a nivel de la ITU-T en la ISO "Telecommunication Management Network". El modelo y framework usado se denomina con el acrónimo FCAPS (Fault, Configuration, Accounting, Performance, Security) que define las tareas a realizarse en la gestión de la red. Estas tareas son las siguientes:

- Fault (Falla): Una falla es un evento de efectos negativos. La finalidad de la gestión de las fallas es poder aislar, corregir y poder tener información de fallas (logs) que ocurren en la infraestructura. También, permite predecir errores que puedan suceder en la red. La forma común de comunicación de los dispositivos de red en este caso particular es

usando el protocolo abierto SNMP (Simple Network Managent Protocol) y syslog.

- Configuration (configuración): Son todas las tareas relacionadas a la configuración del equipamiento de red, incluyendo el poder recolectar las configuraciones actuales, simplificar las configuraciones, manejo de cambios, configuración de características avanzadas y planificación para futura expansión o escalabilidad. Esta parte es una de las más críticas ya que debido a la configuración de la red, pueden surgir problemas relacionados, es por ello que la correcta gestión de la configuración es papel importante para el administrador de red. La forma común de configurar es usando una interface GUI que luego traslade le input a CLI directamente al equipo de red.
- Accounting: El fin es recolectar estadísticas de uso de usuarios en la red. Protocolos que se usan para este fin: RADIUS, TACACS.
- Performance (rendimiento): La gestión del rendimiento está enfocado en asegurar que el rendimiento dentro de la red se mantenga en niveles aceptables. Usa como base los siguientes indicadores como: throughput, tiempos de respuesta de red, pérdidas de paquetes, utilización de enlace, etc. El protocolo comúnmente usado es el SNMP.
- Security (Seguridad): La gestión de la seguridad es el proceso de controlar el acceso a los recursos de la red por el lado de los usuarios, es decir, permitir que solamente los usuarios registrados y con permisos de acceso puedan acceder a los recursos que su perfil les permite en la red. Se logra usando autenticación, autorización en muchos casos cifrado.

Desde el punto de vista del presente informe, la comparación a realizar se basa en la parte de Gestión de la Configuración. Pese a que el NMS es una evolución de cómo configurar la red con respecto al CLI, estos están completamente relacionados, y por lo tanto lleva a seguir manteniendo la complejidad pero bajo la máscara de un ambiente de gestión visual/gráfica.

En la figura 2.3 se muestra cómo se logra configurar una característica en la red de manera gráfica usando un NMS, pero que en realidad esconde una serie de CLI, según se muestra en la figura 2.4, que van a ser inyectadas en un equipo determinado.

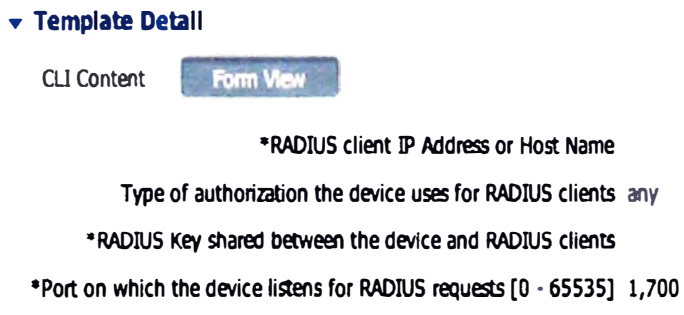


Figura 2.3 Como se ve de manera gráfica usando un NMS (Fuente: Elab. Propia)

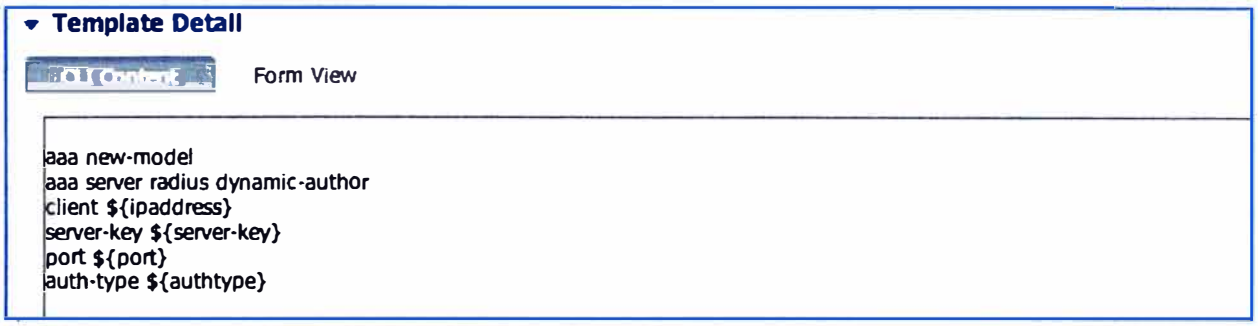


Figura 2.4 Líneas de comando (CLI), resultado del input de la figura 2.3. (Fuente: Propia)

Conclusión:

Con estos gráficos, se puede entender que pese a la mejora en cómo se configura, se sigue arrastrando las limitantes de la línea de comandos y que se reflejan en los siguientes problemas que trae el NMS:

- El tiempo en que una herramienta NMS se actualice para soportar una nueva tecnología o una nueva versión de protocolos existentes en las redes es de meses, y en él durante se vuelve nuevamente a caer al mundo de la gestión por líneas de comando en cada uno de los equipos – Posible error humano.
- Nuevo equipamiento liberado al mercado requiere de una nueva actualización del NMS para poder soportarlo. – Tiempo de ida al mercado versus soporte de nuevas soluciones.
- La mayoría de soluciones NMS del mercado soportan solo una determinada marca de fabricante para la gestión, y de soportar múltiples fabricantes, solo se gestiona características básicas y no avanzadas desarrolladas por dicho fabricante – No interoperabilidad y por lo tanto no se explota la inversión realizada en hardware de red.
- El NMS es solo una máscara, en el "background" el NMS tiene que traducir las acciones creadas por el administrador en la interface gráfica a tareas de línea de comando de manera secuencial en cada uno de los equipos de red. – No es eficiente.

2.4Método actual de Configuración de Red, el SDN

De acuerdo ala Open Networking Foundation (ONF), Software Define Networking (SDN) es una arquitectura de red que desacopla el plano de control del plano de datos de un equipo de red, moviendo el plano de control (encargado de la inteligencia y creación de políticas) hacia una aplicación centralizada llamada Controlador. Con ello, el plano de control es directamente programable y la infraestructura que está debajo (plano de datos) puede ser abstraída para las aplicaciones y los servicios de red. Este concepto simplifica muchas tareas que bajo la arquitectura tradicional de plano de control distribuido son complejas [4].

El punto neurálgico de SDN es el Controlador. Este es encargado de orquestar, mediar y facilitar la comunicación entre las aplicaciones que desean interactuar con los elementos de la red y los elementos de la red que desean transmitir información a esas

aplicaciones. El controlador luego expone y abstrae las funciones y operaciones de la red a través de interfaces de programación modernas y amigables. Con los avances que existen con respecto al Controlador, actualmente muchos investigadores y desarrolladores se están enfocando en lo que más importa en SDN: el desarrollo de aplicaciones.

El modelo de bloques de la arquitectura referencial SDN [4] se ilustra en la figura 2.5.. En la arquitectura mostrada se puede observar que el Controlador es la interfaz de comunicación entre las aplicaciones y los elementos de red:

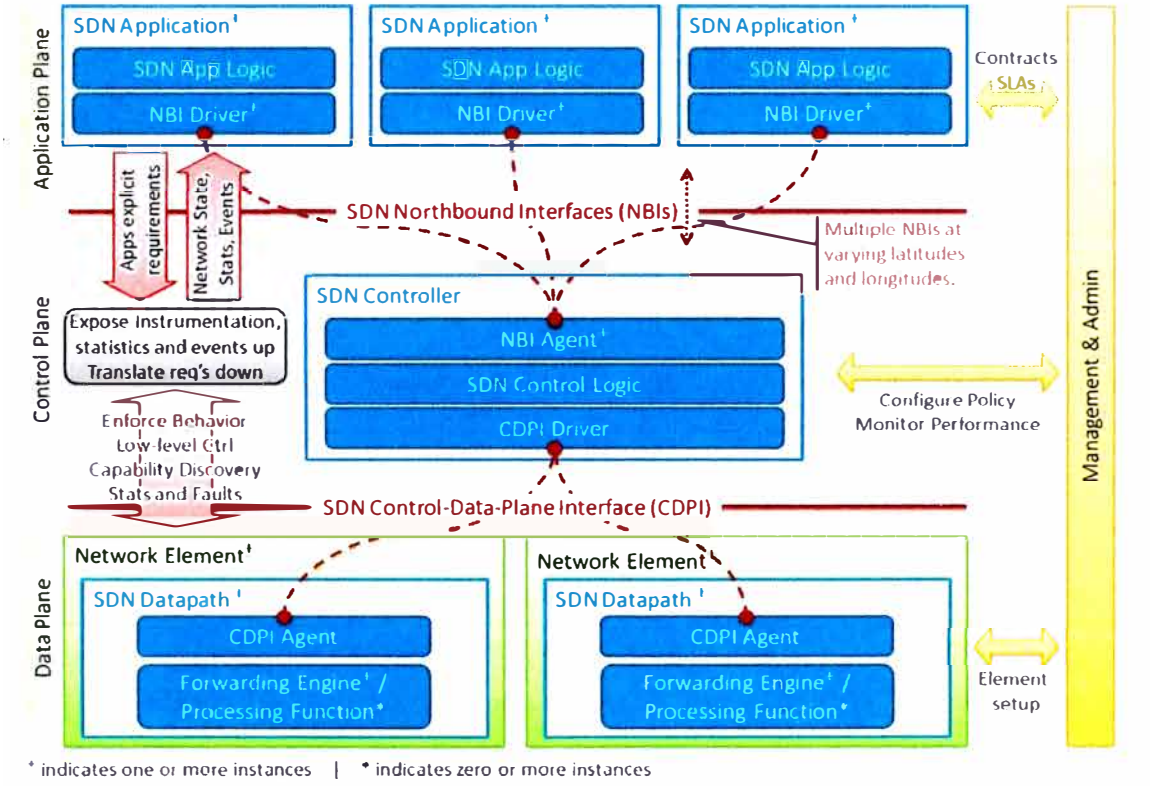


Figura 2.5 Modelo de bloques de la arquitectura referencial SDN(Fuente: Ref. [4])

Los componentes más importantes del modelo son:

- Controlador: el controlador es una entidad lógicamente centralizada encargada de traducir los requerimientos de las Aplicaciones hacia la capa más baja, los elementos de red (SDN datapath), permitiendo que las aplicaciones tengan una vista abstracta de la red (que puede incluir estadísticas y eventos). Un Controlador consiste en uno o más agentes para interfaces Northbound (NBI – Northbound Interfaces), una capa lógica de control, y drivers para la interacción con el plano de data (CDPI – Control Data-Plane Interface).
- SDN Datapath: El SDN Datapath es un dispositivo lógico de red que permite tener visibilidad de sus capacidades de forwarding y procesamiento de data. La representación lógica puede indicar todo o una parte de los recursos físicos (por ejemplo, en un switch, solo los 10 primeros puertos se usan como SDN Datapath, los otros puertos pueden trabajar de manera tradicional). Se conforma de un agente CDPI para interactuar con el

Controlador y un conjunto de uno o más motores de forwarding y funciones de procesamiento. Estos motores y funciones puede incluir reenvío de los datos a través de sus interfaces externas o procesamiento interno de tráfico o funciones de terminación.

- SDN Northbound Interfaces (NBI): SDN NBIs son interfaces entre las Aplicaciones y los Controladores y típicamente provee un abstracto de la vista de la red y permite expresiones directas de los requerimientos y comportamientos de la red. Esto puede ocurrir en todo nivel de abstracción y a través de diferentes conjuntos de funcionalidades. Uno de los valores de SDN es que estas interfaces se implementen en un ambiente abierto y neutral del fabricante. Dentro de las interfaces más comunes se encuentra el uso de JAVA, C++, Python, etc siendo Python la de mayor acogida en el mercado por su simplicidad y sintaxis limpio.
- SDN Controller to Data-Plane Interface (CDPI): El SDN CDPI es la interface entre el Controlador y el SDN Datapath que provee al menos control programático de todas las funciones de forwarding, capacidades de anuncios, reporte de estadísticas y notificación de eventos. Uno de los valores de SDN es que estas interfaces se implementen en un ambiente abierto y neutral del fabricante. Dentro de las CDPI más comunes es OpenFlow, APIs de los fabricantes (en Cisco – ONE PK) y CLI adaptado. No existe aún un convenio de qué tipo de CDPI es el más adecuado, pero por el momento lo más comercial es OpenFlow.

En los siguientes puntos, se procederá a explicar las dos CDPI más comunes: Openflow, ONE PK. Para el caso de estudio, la metodología aplicada como alternativa a las limitaciones del equipamiento para soportar estas dos tecnologías, se desarrolla en el capítulo 3.

2.4.1Openflow

Openflow es considerado como el progenitor de toda la teoría y discusión existente en base a SDN. Este protocolo fue imaginado originalmente en el equipo de investigadores de redes en la Universidad de Standford. Su foco original era el permitir la creación de protocolos experimentales en redes de campus que pueda ser usado para investigación y experimentación, esto debido a que, como se comentó en el capítulo 1, no existía ambientes con tráfico real para poder hacer pruebas de los nuevos protocolos [5].

Los principales componentes del modelo Openflow son esencialmente los que vienen como parte común del modelo SDN.

- Separación del plano de control con el plano de datos donde el plano de control se centraliza de manera lógica a través de un Controlador.
- Uso de un protocolo estándar entre el controlador y un agente dentro de los elementos de red para la creación de instancias de estado (estado de forwarding).

- Proveer programabilidad de la red desde una vista centralizada mediante un moderno y extensible API.

El estándar Openflow, define como modelo de referencia tres partes: el OpenFlow Switch, el protocolo Openflow de comunicación, y el Controlador. De acuerdo a lo visto en el presente informe, el OpenFlow Switch hace referencia al SDN Datapath, el protocolo Openflow sería un CDPI y el Controlador, el Controlador SDN. En la figura 2.6 [5] se puede ver el modelo de referencia.

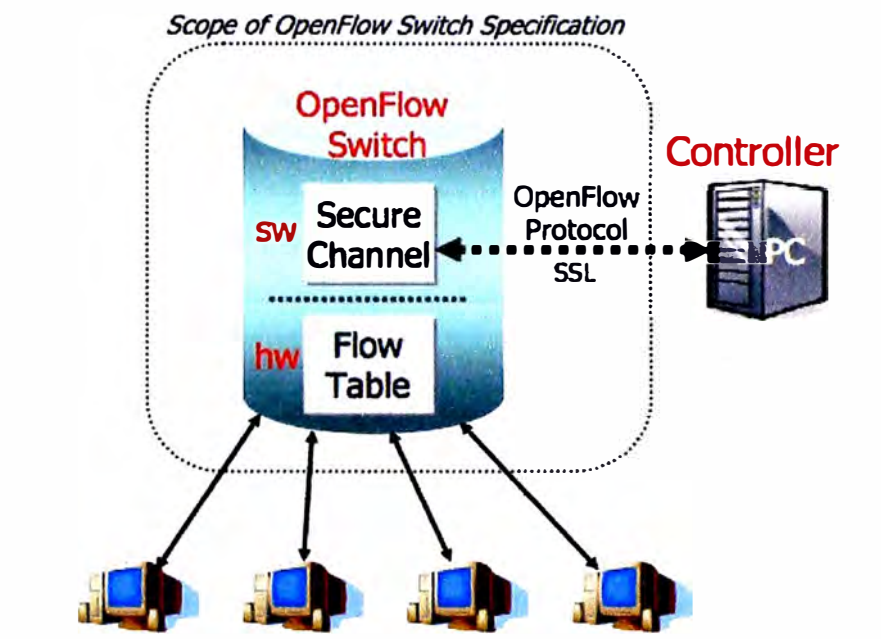


Figura 2.6 Modelo Referencial de OpenFlow (Fuente: referencia [5])

Para entender mejor Openflow, entendamos a más detalle el modelo. El Switch Openflow posee tres partes: una Tabla de Flujos con una acción asociada a cada entrada de flujo, un canal de comunicación seguro que conecta el switch con el Controlador permitiendo que comandos y paquetes viajen de manera segura y el Protocolo Openflow, que provee un estándar abierto de cómo el controlador conversa con el switch. Al especificar una interface estándar (Protocolo Openflow) a través del cual se puede definir de manera externa las entradas en la Tabla de Flujos, se evita el tener que interactuar o configurar directamente el switch.

La Tabla de Flujos tiene tres campos: la cabecera de paquete que define el flujo, la acción cómo los paquetes deben de ser procesados y estadísticas para hacer seguimiento de la cantidad paquetes y bytes generados por un flujo y el tiempo desde el último paquete procesado.

Mediante el uso del Controlador y del protocolo Openflow para programar el switch OpenFlow, se puede lograr las siguientes acciones asociadas a una entrada de flujo en la Tabla de Flujos:

- Reenviar el flujo de paquetes a un puerto físico específico (o puertos). Esto permite que

determinados paquetes sean enrutados a través de la red. En la mayoría de los switches, esta acción se hace a velocidad en línea.

- Encapsular y enviar el flujo de paquetes al controlador a través de un canal seguro. Esto normalmente sucede con el primer paquete de un nuevo flujo, para poder determinar si el flujo debe de ser adicionado a la Tabla de Flujos, o en todo caso si se desea que el controlador tome acciones de procesamiento adicionales.
- "Dropear" el flujo de paquetes.

En switches del mercado que pueden soportar a la vez Openflow como el modelo tradicional, se adiciona una cuarta acción: reenviar hacia el flujo normal del switch.

Las últimas versiones del protocolo Openflow ha introducido algunas mejoras para la simplificación de QoS en la red. Al ser justo el fin de este informe, como podemos configurar QoS en la red de manera sencilla, no podemos usar Openflow como referencia al tener recién una implementación para el manejo de QoS aún no implementada en el mercado.

2.4.2 ONE Platform Kit – ONE PK

Cisco ONE Platform Kit (onePK) es un kit de desarrollo de software para programar características específicas de equipamiento Cisco y sistemas operativos de redes que permite acceso y control a un rango amplio de capacidades del equipamiento Cisco. Esto permite a las aplicaciones acceder a las capacidades de los equipos de red mediante el uso de API estándares [6].

Desde una visión de alto nivel, la arquitectura onePK se compone de tres elementos principales: la capa de presentación, el API onePK y el canal de comunicación. Todos estos elementos se combinan para dar una arquitectura consistente y adaptable que permite a las aplicaciones acceder a múltiples lenguajes de programación y múltiples tipos de despliegues. En la figura 2.7 [6] se muestra la visión en alto nivel de onePK.

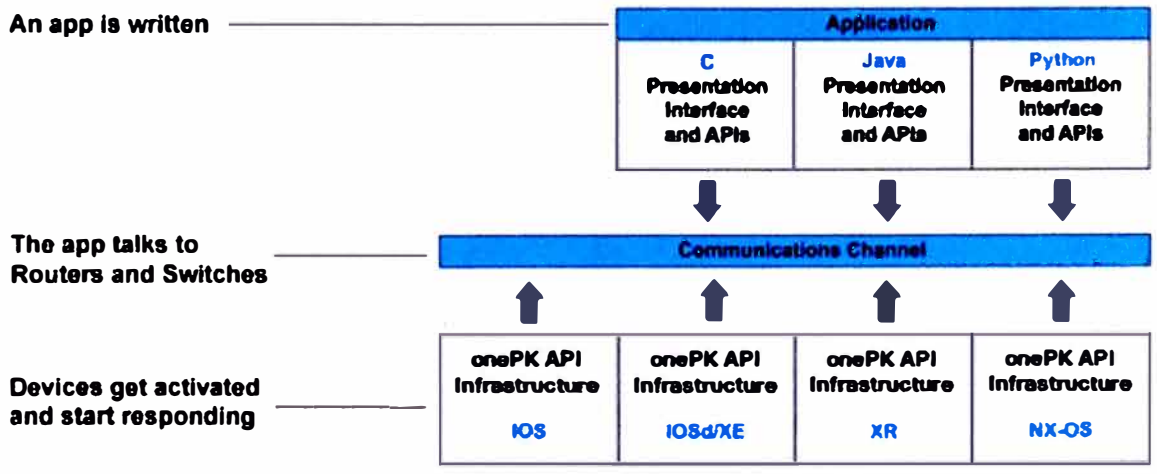


Figura 2.7 Modelo referencial de onePK (Fuente: Referencia [6])

Estos elementos se pueden definir de la siguiente manera:

- Capa de presentación: Consiste en librerías de API que los programadores pueden usar para sus aplicaciones. Con onePK, los programadores acceden a un toolkit universal de programación. Se encuentra librerías para Java, C y Python.
- -onePK API: Provee acceso a las funciones que son internas a un router o a un switch. Uno de sus primeros valores es que abstrae las diferencias fundamentales entre diferentes sistemas operativos y plataformas.
- Canal de Comunicación: el canal de comunicación provee una ruta rápida y segura entre las aplicaciones y los elementos de red.

Los APIs ofrecidos por onePK se organizan en "service sets" de acuerdo a su función. En la figura 2.8 [6] se muestran los "service sets" y los APIs asociados a ellos.

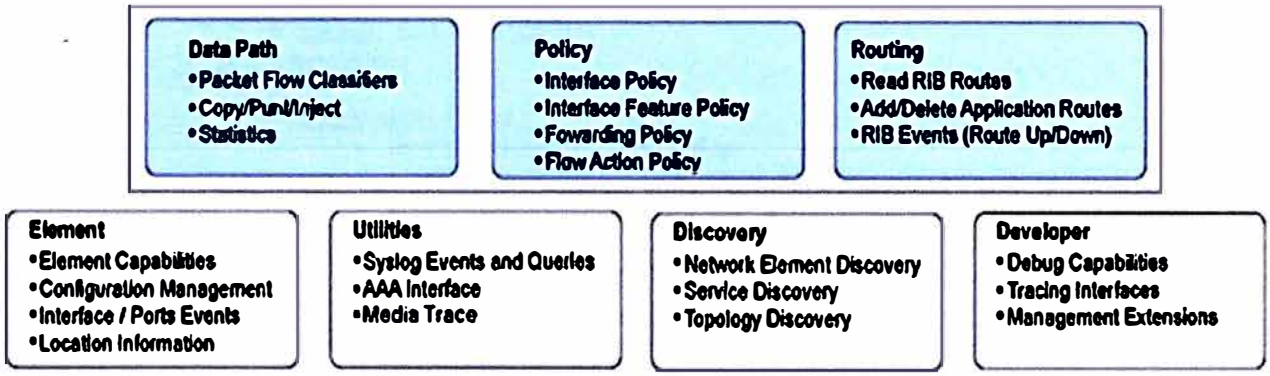


Figura 2.8 Service Sets onePK (Fuente: Referencia [6])

A continuación, se explicará la función de cada service set.

- Data Path: provee locación en la ruta de reenvío para insertar características personalizadas. Estas locaciones permiten a los desarrolladores insertar su propio lógica de procesamiento de paquetes/flujos dentro de la ruta de reenvío.
- Policy: permite a las aplicaciones configurar muchas características de la ruta de reenvío, incluyendo filtrado, ACL y QoS.
- Routing: permite el acceso a la RIB y habilita a los desarrolladores modificar de manera segura la lógica de routing/switching de los elementos de red.
- Elemento: consiste en APIs para configurar y recoger propiedades de las interfaces, estados y estadísticas. En la figura2.9 [6] se muestra parte de la estructura referencial de los API para Python.
- Utilidades: provee acceso a syslog y funciones AAA(autentication, autorization, accounting).
- Descubrimiento: permite tener mecanismos para que una aplicación pueda descubrir redes locales o remotas, la topología de la red y los elementos de la red.
- Desarrollo: permite a los desarrolladores tener servicios adicionales que les permita construir aplicaciones que puedan ser gestionadas, desplegadas y si es necesario tener acceso a información de troubleshooting de bajo nivel (debug).

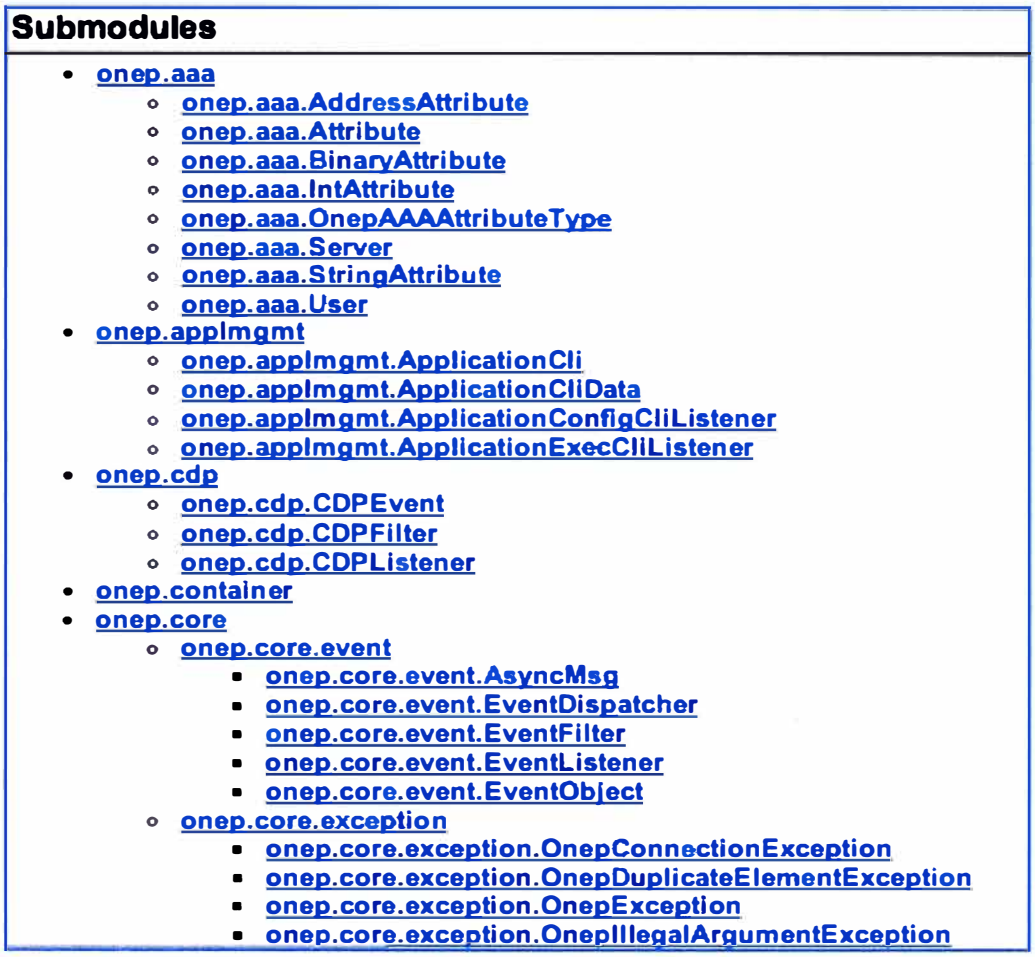


Figura 2.9 Estructura de APIs para Python (Fuente: Referencia [6])

2.5 Calidad de Servicio – QoS

Calidad de Servicio o QoS es la medida de la calidad de transmisión y disponibilidad de un servicio en la red [9].

La disponibilidad del servicio es un elemento fundamental para QoS. La infraestructura de red debe de estar diseñada de tal manera que tenga alta disponibilidad incluso antes de querer implementar QoS. La calidad de la transmisión de la información en la red está determinada por los siguientes factores [9]:

- Pérdida: Una medida relativa del número de paquetes que no fueron recibidos comparado con la cantidad de paquetes transmitidos. La pérdida es típicamente un factor de la disponibilidad. Durante periodos de congestión, los mecanismos de QoS pueden determinar que paquetes pueden ser seleccionados para ser "dropeados" en tiempos de congestión.
- Retardo: Es el tiempo finito que toma a un paquete alcanzar al receptor luego de ser transmitido desde el elemento transmisor.
- Variación del retardo (jitter): Es la diferencia del retardo de extremo a extremo entre paquetes.

Las tecnologías de QoS se refieren a una serie de herramientas y técnicas para

manejar los recursos de la red y son consideradas claves para la convergencia de la red. El objetivo de las tecnologías de QoS es hacer que la voz, video y convergencia de la data sea transparente para los usuarios finales. Las tecnologías de QoS permiten que diferentes tipos de tráficos accedan a recursos de red de manera independiente, tal es el caso de la voz, video y aplicaciones críticas que requieren un mejor trato del lado de la red a diferencia de otras aplicaciones no críticas que puedan degradar el rendimiento de estas.

Las herramientas de QoS no solo son útiles en la protección del tráfico deseable, sino también en proveer servicios diferenciales a tráfico no deseado como posibles gusanos en la red. Se puede usar QoS para monitorear los flujos y proveer reacciones de primer y segundo orden hacia flujos anormales que puedan indicar ataques.

En el caso del presente documento, se toma como referencia a equipamiento Cisco, por lo que nos basaremos en las herramientas que ofrece este fabricante en sus equipos de red. Cisco provee un completo kit de herramientas de QoS para poder preparar la red para tráfico crítico como voz y video (tráfico multimedia).

Se puede de manera efectiva controlar el ancho de banda, retardo, jitter y la pérdida de paquetes con estos mecanismos. Al usar las herramientas de QoS se pueden crear redes empresariales que estén acorde a la arquitectura Diffentiated Services (DiffServ) definida en el RFC 2475.

Dentro de las herramientas que ofrece Cisco para QoS, se pueden ver las siguientes:

- Herramientas de clasificación y marcado.
- Herramientas de encolado y gestión de la congestión.
- Herramientas específicas de enlace
- Herramientas de AutoQoS
- Herramientas de control de admisión de red.

En la figura 2.10 se muestra donde se aplican en un flujo de tráfico las diferentes herramientas.

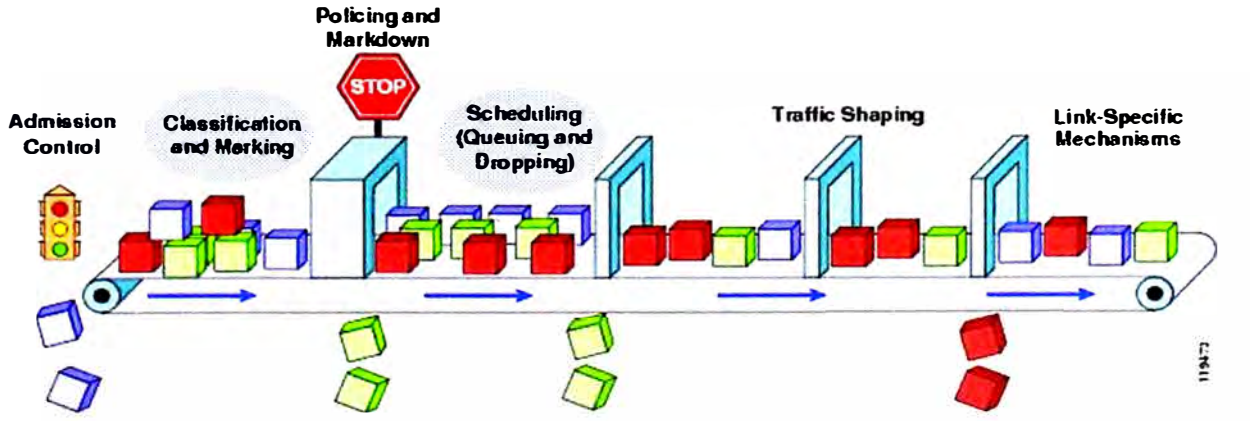


Figura 2.10 Herramientas de QoS de Cisco (Fuente: Referencia [9])

Para el fin del presente informe, es necesario entender las dos primeras herramientas.

2.5.1 Clasificación y Marcado

La primera herramienta de QoS es la clasificación/identificación del tráfico que va a ser tratado de manera diferente (Classification). Luego de la clasificación, las herramientas de marcado permiten que se tenga un valor específico dentro de atributos dentro de un paquete. Estas herramientas usan la inspección de lo siguiente [9]:

- Parámetros de Capa 2: 802.1Q Class of Service (CoS).
- Parámetros de Capa 3: IP Precedence (IPP), Differentiated Services Code Point (DSCP), IP Explicit Congestion Notification (ECN) y IP origen/destino.

a. Marcados de capa 2

Es el 802.1Q/p Class of Service (CoS). En este tipo de marcado, los frames de Ethernet pueden ser marcados a nivel de capa 2 con su importancia relativa configurando los bits de prioridad de usuario 802.1p dentro de la cabecera 802.1Q. Solo se tiene disponible tres bits en el marcado 802.1p, por lo tanto solo se tienen 8 clases de servicio (0-7) para ser marcados a nivel de capa 2.

b. Marcados de capa 3

Solamente se pueden aplicar políticas siempre y cuando el tráfico ha sido completamente clasificado. Las herramientas de marcado pueden ser usadas para agregar información de la prioridad agregando información en campos del paquete para que no sea recurrente el tener que clasificar en cada salto el tráfico. Para ello se usa el byte IP Type of Service (ToS). La media a nivel de capa 2 cambia cada vez que los paquetes pasan de origen a destino. Para ello se tiene una clasificación a nivel de capa 3, en donde el segundo byte dentro de un paquete IPv4 es el byte de ToS.

En la figura 2.11 se muestra la ubicación y el uso de las diferentes técnicas de marcado:

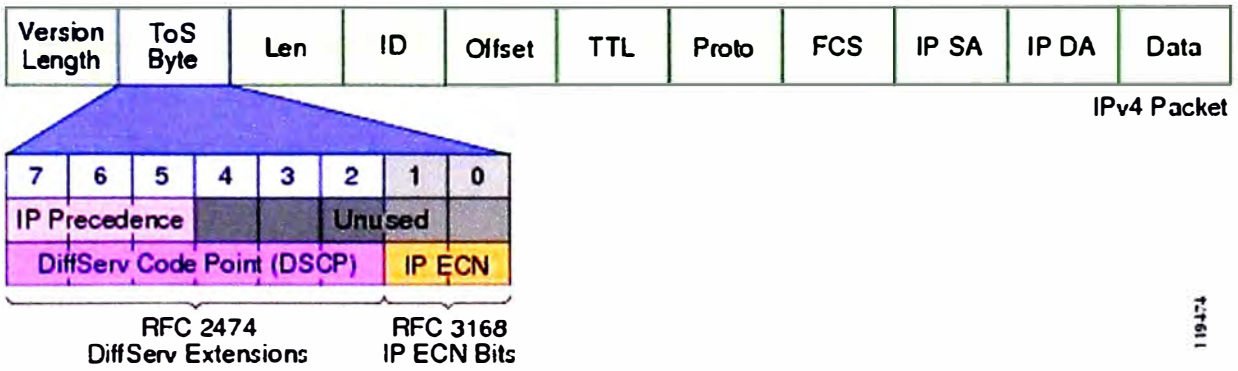


Figura 2.11 El Byte IP ToS (DSCP e IP ECN) (Fuente: Referencia [9])

b.1 IPP (IP Precedence)

Los primeros tres bits del byte ToS son los IPP bits.Los bits de IP Precedence, como

los de 802.1p, permiten solo 8 valores de marcados (0-7):

- IPP 6-7 son reservados comúnmente para tráfico de control como routing
- IPP 5 es recomendado para voz
- IPP 4 es compartido para videoconferencia o video en streaming.
- IPP 3 es para control de voz.
- IPP 1 – 2 para aplicaciones de data.
- IPP 0 es el marcado por defecto.

b.2 DSCP (DiffServ Code Point)

Los primeros tres bits de IP Precedence, combinados con los siguientes tres bits son conocidos como DSCP bits.

Muchas empresas no usan el modelo IP Precedence, comúnmente por ser muy restrictivo y limitante. Para escalar, prefieren usar el modelo DSCP. El marcado DSCP se compone del uso de 6 bits con un total de 64 valores de marcado. Los valores DSCP pueden ser expresados en forma numérica o bajo nombres especiales basados en estándares llamados PHB (Per-Hop Behaviours). Existen cuatro amplias clases de marcado PHB DSCP: Best Effort (BE o DSCP 0), RFC 2474 Class Selectors (CS1-CS7, que son compatibles hacia atrás con los valores de IPP), RFC 2507 Assured Forwarding PHB (AFxy), y el RFC 3268 Expedited Forwarding (EF).

Existen cuatro clases AF, cada uno de ellas empiezan con la letra AF seguido de dos números. El primero corresponde a la clase DiffServ del grupo AF y va de 1 a 4. El segundo número se refiere a Preferencias de Descarte dentro de cada clase AF y va desde 1 (menor preferencia de descarte) a 3 (mayor preferencia de descarte).

Los valores de DSCP se pueden expresar en forma decimal o con sus claves PHB. Por ejemplo, DSCP EF es sinónimo de DSCP 46, y DSCP AF31 es sinónimo de DSCP 26.

b.3 IP ECN (IP Explicit Congestion Notification)

Es definido dentro del RFC 3168. Hace uso de los dos últimos bits del byte IP ToS que no son usados por el marcado DSCP. Estos dos últimos valores son usados para indicar a los transmisores TCP si es que hay congestión o no durante el tránsito. De esta manera los trasmisores pueden adaptar su ventana para no enviar más tráfico que la red no puede servir. El primer bit (sétimo de ToS) sirve para indicar si es que se soporta este servicio, y el segundo (8vo de ToS) se usa para indicar si hay congestión (0= no congestión, 1= congestión).

c. Conclusión

Con el entendimiento de estos métodos de marcado/clasificado, Cisco recomienda un modelo de marcado basado en 12 niveles, como se muestra en la figura 2.12.

Application	L3 Classification		IETF
	PHB	DSCP	RFC
Network Control	CS6	48	RFC 2474
VoIP Telephony	EF	46	RFC 3246
Broadcast Video	CS5	40	RFC 2474
Multimedia Conferencing	AF41	34	RFC 2597
Real-Time Interactive	CS4	32	RFC 2474
Multimedia Streaming	AF31	26	RFC 2597
Call Signaling	CS3	24	RFC 2474
Low-Latency Data	AF21	18	RFC 2597
OAM	CS2	16	RFC 2474
High-Troughput Data	AF11	10	RFC 2597
Best Effort	DF	0	RFC 2474
Low-Priority Data	CS1	8	RFC 3662

Figura 2.12 Modelo de Cisco basado en RFC 4594.(Fuente: Referencia [10])

La aplicabilidad de un modelo de 12 niveles en redes Enterprise puede ser complejo. Cisco recomienda hacer una migración gradual, y recomienda el esquema de migración mostrado en la figura 2.13.

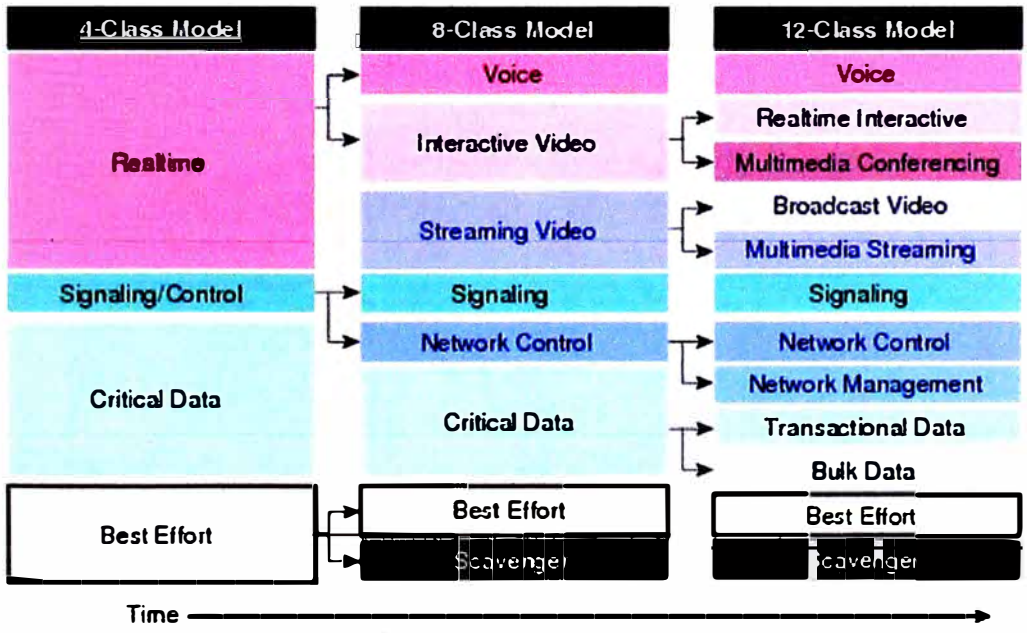


Figura 2.13 Modelo de migración gradual de clases (Fuente: Referencia [10])

2.5.2 Encolado (queueing) y gestión de la congestión

Este tipo de herramientas determinan como un frame/paquete sale de un dispositivo. Siempre que un paquete entre a un dispositivo más rápido de cómo sale, puede existir un punto de congestión o cuello de botella. Los dispositivos de red suelen tener buffers que

permitan encolar paquetes de alta prioridad para que salgan más rápido que los paquetes de baja prioridad [10].

Los algoritmos de encolado son activados siempre y cuando un dispositivo esté experimentando congestión y son desactivados cuando la congestión desaparece. Las principales herramientas de encolado son:

- Low Latency Queueing (LLQ), que permite tener servicios prioridad estricta para tráfico en tiempo real como voz o video.
- Class-Based Weighted Fair Queueing (CBWFQ) que provee garantía de ancho de banda para determinadas clases de tráfico y "fairness" para tráfico discreto dentro de estas clases de tráfico.

Los buffers de encolado tienen un límite, y cuando llega a este punto, los paquetes pueden ser descartados. En este caso particular se usan técnicas para evitar la congestión. Estas técnicas son complementarias a las de encolado.

El principal mecanismo para la gestión de la congestión se denomina WRED (Weighted Random Early Detection), el cual de manera aleatoria descarta paquetes mientras las colas llenan su capacidad. Sin embargo, dentro de lo aleatorio de su selección, se puede aún separar por pesos. El peso puede ser el valor de IP Precedence o el peso puede venir del AF Drop Precedence. WRED también puede ser usado para configurar los bits IP ECN para indicar si hay congestión en tránsito.

En la figura 2.14 se resume laoperación de LLQ/CBWFQ:

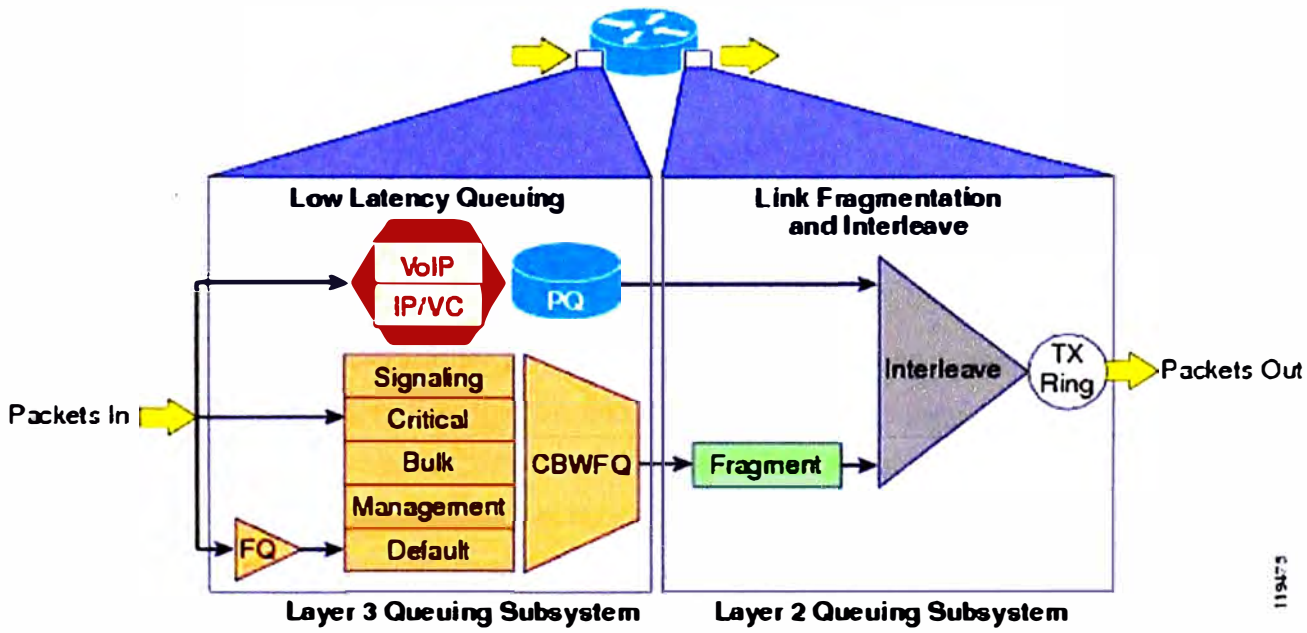
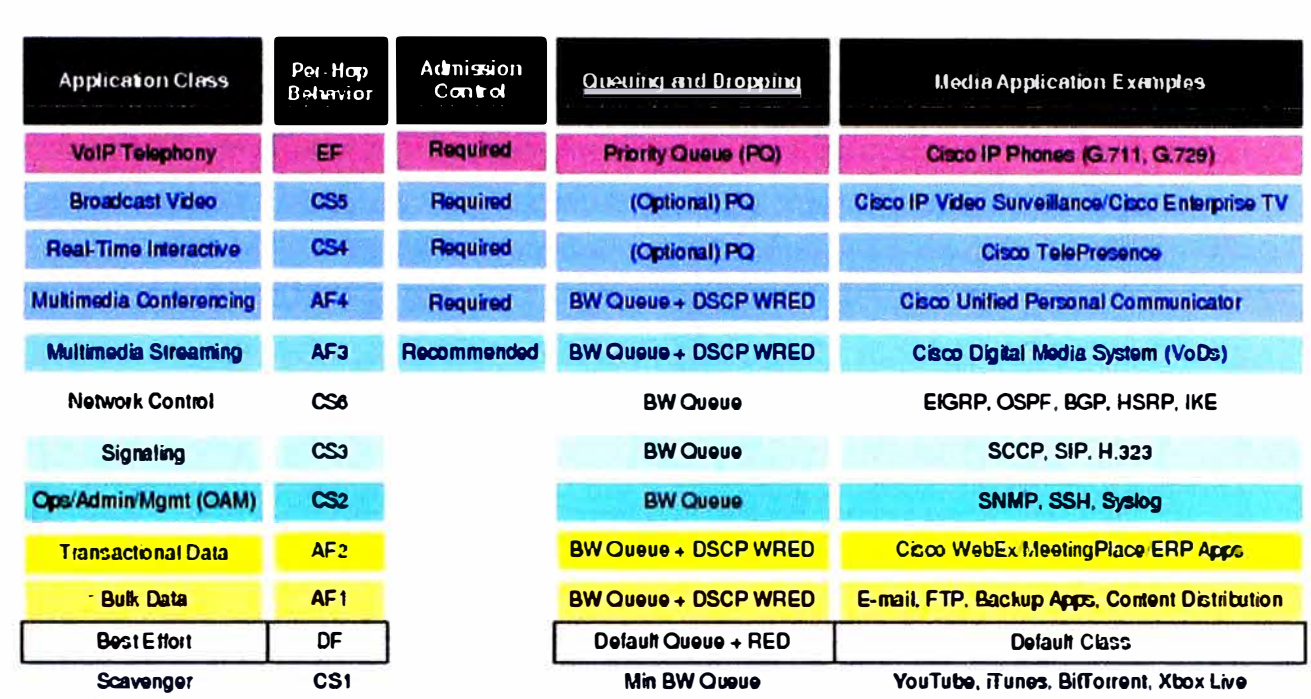


Figura 2.14 Operación LLQ/CBWFQ. (Fuente: Referencia [9])

Las recomendaciones en el caso particular de tráfico multimedia en una red de Campus por parte de Cisco, se resume en la figura 2.15, en donde se hace la asociación del tipo de tráfico, con el marcado, encolado y gestión de la congestión.



Application Class	Per-Hop Behavior	Admission Control	Queuing and Dropping	Media Application Examples
VoIP Telephony	EF	Required	Priority Queue (PQ)	Cisco IP Phones (G.711, G.729)
Broadcast Video	CS5	Required	(Optional) PQ	Cisco IP Video Surveillance/Cisco Enterprise TV
Real-Time Interactive	CS4	Required	(Optional) PQ	Cisco TelePresence
Multimedia Conferencing	AF4	Required	BW Queue + DSCP WRED	Cisco Unified Personal Communicator
Multimedia Streaming	AF3	Recommended	BW Queue + DSCP WRED	Cisco Digital Media System (VoDs)
Network Control	CS6		BW Queue	EIGRP, OSPF, BGP, HSRP, IKE
Signaling	CS3		BW Queue	SCCP, SIP, H.323
Ops/Admin/Mgmt (OAM)	CS2		BW Queue	SNMP, SSH, Syslog
Transactional Data	AF2		BW Queue + DSCP WRED	Cisco WebEx MeetingPlace/ERP Apps
Bulk Data	AF1		BW Queue + DSCP WRED	E-mail, FTP, Backup Apps, Content Distribution
Best Effort	DF		Default Queue + RED	Default Class
Scavenger	CS1		Min BW Queue	YouTube, iTunes, BitTorrent, Xbox Live

Figura 2.15 Recomendaciones Cisco para tráfico. (Fuente: Referencia [10])

2.6 Listas de Control de Acceso - Aplicaciones

En redes de datos, las listas de control de acceso (ACL) se refieren a las reglas que se aplican a determinado número de protocolo en capa 4 o direccionamiento IP que está disponible para un host u otros dispositivos de capa 3, con una lista de host o redes permitidas para usar determinado servicio.Estos ACL son definidos de manera local en cada equipamiento de red [12].

En el campo de las redes, existen aplicaciones para el uso de ACL como las siguientes:

- ACL de Clasificación: Permite clasificar el tráfico basado en la información de capa 2 y capa 3 y es usado para poder tomar decisiones en temas de QoS, enrutamiento, etc.
- ACL de Seguridad: Permite denegar o permitir determinado tráfico hacia determinado servicio dentro de la red. Este tráfico se identifica por sus valor de capa 3 y capa 4. Cada ACL es definido de manera local en cada equipo de red, y es aplicado directamente a interfaces físicas o lógicas. Ejemplo de ello es poder permitir que un usuario corporativo pueda acceder a determinada aplicación en el centro de datos.

Es el segundo tipo de aplicación, el de seguridad, el que puede perjudicar los flujos de tráfico en la red si no se tiene un correcto control de los cambios. Al tener que aplicar los ACL de manera directa a cada equipo de red, esto hace que sea complejo determinar si debido a un ACL el tráfico que se requiere que circule se encuentra bloqueado.

Un ejemplo de ello es en el caso que se colocó un ACL con una IP1 en determinado tiempo. Esta ACL lo hizo el administrador A y no hizo un correcto manejo de cambios, por lo tanto no se tiene conocimiento de quién, dónde y que ACL hay en la red. En el tiempo,

esa IP1 ya no le pertenece a un usuario, sino a un servicio crítico como video. Pese a que se tiene todo configurado a nivel de QoS, el tráfico no pasará debido a este ACL colocado en la red. El administrador para poder identificarlo, va a tener que entrar a cada equipo de red, y si se tiene más de un ACL, la complejidad de ubicar al adecuado es elevada.

CAPÍTULO III
METODOLOGÍA PARA LA SOLUCIÓN DEL PROBLEMA

En este capítulo se explica cómo,mediante un ejemplo, opera el Controlador usando el concepto de CLI Adaptado. Esto permitirá entender las tareas que realiza el Controlador en el background. Luego de esta explicación de la operación, se procederá a mostrar la forma cómo se configura en el escenario de prueba QoS y la búsqueda de ACLs en la red tanto con el método tradicional, así como usando SDN. Finalmente se realiza un análisis comparativo entre el método tradicional y el moderno.

3.1 Caso de estudio

El caso de estudio del presente informe, consiste de una red que posee quince equipos con la topología mostrada en la figura 3.1. Esta red, debido a las limitaciones de la infraestructura, que consistía en no poder soportar las tecnologías SDN (OpenFLow y onePK), se recurre a una metodología alternativa denominada para este informe "CLI Adaptado" el cual es explicado en la siguiente sección.

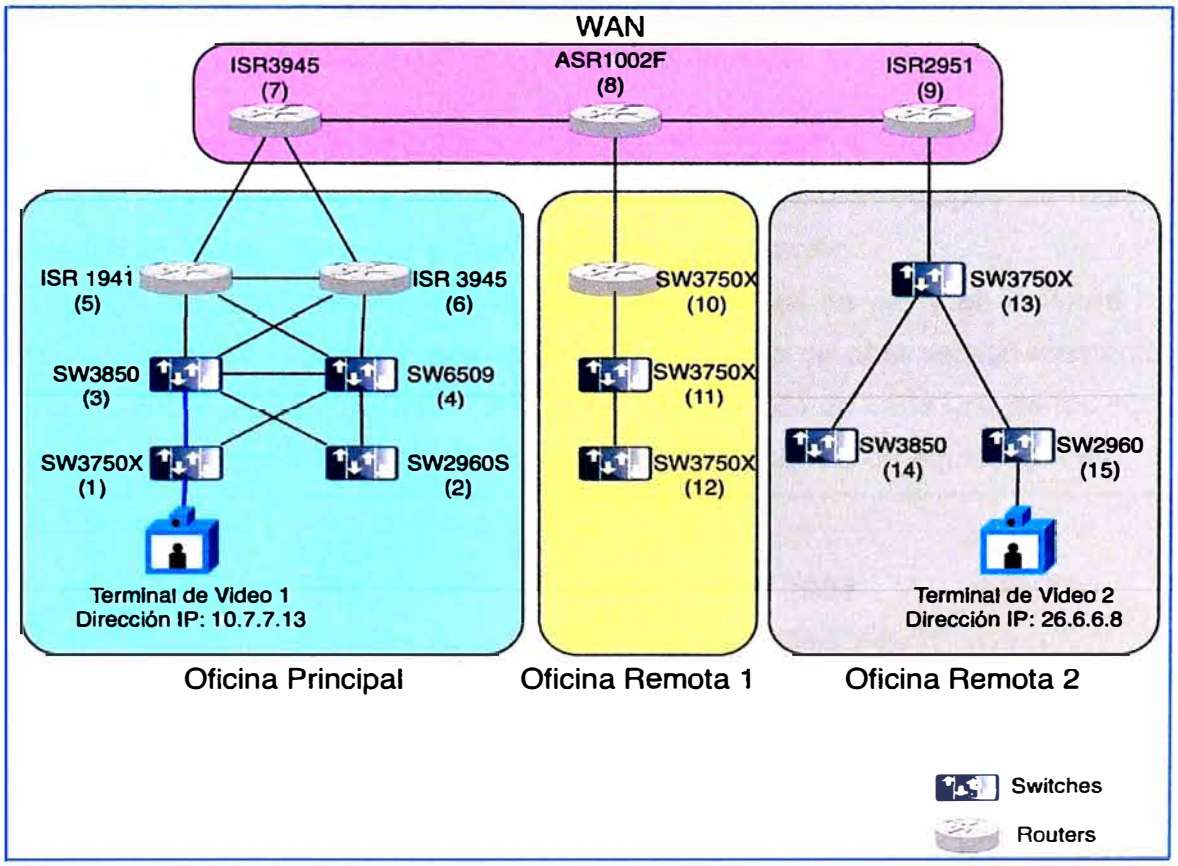


Figura 3.1 Diagrama de red del caso de estudio (Fuente: Elab. Propia)

3.2 Metodología para el caso de Estudio: CLI adaptado

Para la configuración de red del caso de estudio bajo el concepto de SDN, se requiere que la infraestructura a nivel de hardware y software soporte tecnologías tales como OpenFLow y onePK, que como se mencionó, son las más comunes

Sin embargo, en la práctica, se suele encontrar muchas redes que tienen equipamiento tradicional, y no soportan las nuevas tecnologías. La situación se empeora cuando no existen planes de renovación de equipamiento pero se desea comenzar a tener las bondades en la simplificación de la configuración con el uso de SDN.

Para estos casos particulares se tiene que recurrir al esquema tradicional de configuración usando la línea de comandos (CLI). La línea de comandos sigue siendo un medio efectivo para poder configurar a profundidad múltiples características del sistema operativo residente. A diferencia de los otros dos protocolos, se conoce sus grandes debilidades explicadas en puntos anteriores.

Dado que para el caso de estudio, el Controlador utilizado "Cisco APIC Enterprise Module" [13] no soporta las tecnologías OpenFLow y onePK, se aplica una metodología alternativa basada en CLI, a la cual para este estudio se ha denominado "CLI Adaptado", con la cual se logra mejorar el uso de CLI y no se incurre nuevamente en los problemas resultados de su uso.

La clave de la metodología es poder abstraer de manera adecuada cada equipamiento de red y, basado en esta abstracción, adaptar la línea de comandos para su mejor uso.

Nota: La abstracción de un equipamiento de red involucra entender a profundidad las capacidades de hardware y de software que tienen determinado equipos, su relación de dependencia que tiene con otros elementos de red y su función.

En la figura 3.2 se muestra el ejemplo de tres equipos de red y en la figura 3.3 se muestra la abstracción de esos elementos de Red.Luego de abstraer los elementos de red, el controlador puede determinar las líneas de comando de cada uno de los equipos, debido al conocimiento de su sistema operativo y al tipo/modelo de equipo que es.

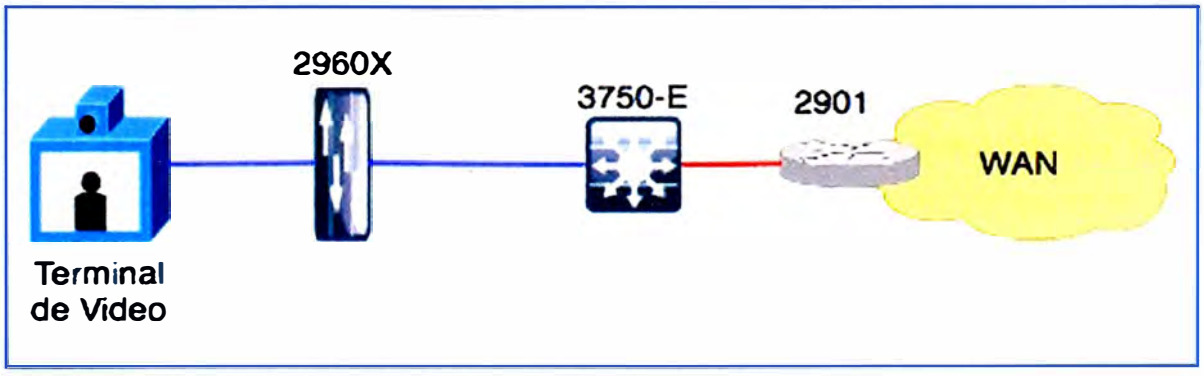
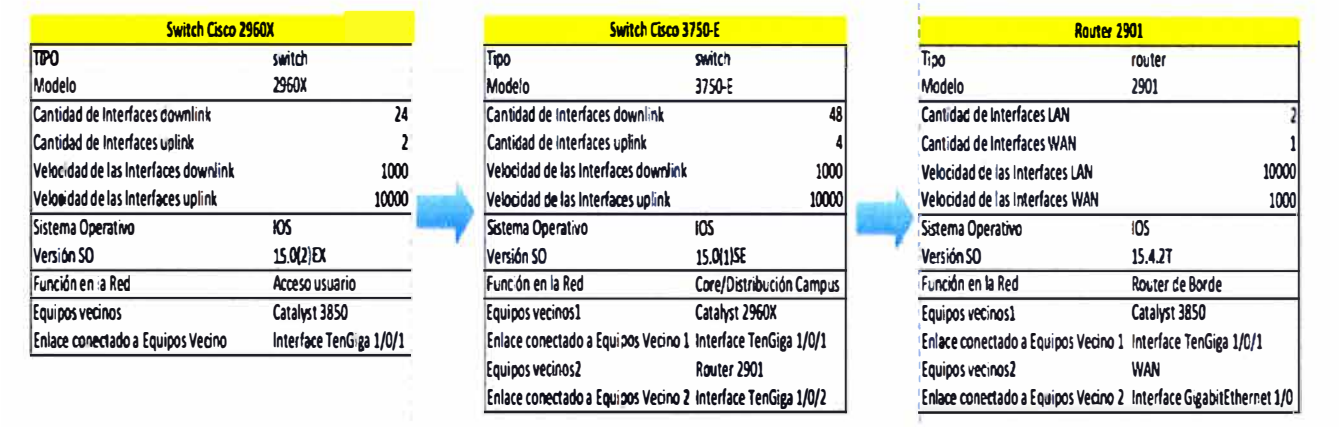


Figura 3.2 Vista de conectividad física de ejemplo en red (Fuente: Elab. Propia)



Switch Cisco 2960X	
TIPO	switch
Modelo	2960X
Cantidad de Interfaces downlink	24
Cantidad de Interfaces uplink	2
Velocidad de las Interfaces downlink	1000
Velocidad de las Interfaces uplink	10000
Sistema Operativo	IOS
Versión SO	15.0(2)EX
Función en la Red	Acceso usuario
Equipos vecinos	Catalyst 3850
Enlace conectado a Equipos Vecino	Interface TenGiga 1/0/1

Switch Cisco 3750-E	
Tipo	switch
Modelo	3750-E
Cantidad de Interfaces downlink	48
Cantidad de Interfaces uplink	4
Velocidad de las Interfaces downlink	1000
Velocidad de las Interfaces uplink	10000
Sistema Operativo	IOS
Versión SO	15.0(1)SE
Función en la Red	Core/Distribución Campus
Equipos vecinos1	Catalyst 2960X
Enlace conectado a Equipos Vecino 1	Interface TenGiga 1/0/1
Equipos vecinos2	Router 2901
Enlace conectado a Equipos Vecino 2	Interface TenGiga 1/0/2

Router 2901	
Tipo	router
Modelo	2901
Cantidad de Interfaces LAN	2
Cantidad de Interfaces WAN	1
Velocidad de las Interfaces LAN	10000
Velocidad de las Interfaces WAN	1000
Sistema Operativo	IOS
Versión SO	15.4.2T
Función en la Red	Router de Borde
Equipos vecinos1	Catalyst 3850
Enlace conectado a Equipos Vecino 1	Interface TenGiga 1/0/1
Equipos vecinos2	WAN
Enlace conectado a Equipos Vecino 2	Interface GigabitEthernet 1/0

Figura 3.3 Abstracción de los elementos de Red (Fuente: Elab. Propia)

Con esto se sabe quélíneas de comando son las adecuadas para cada equipo, pero no brinda la certeza de cuál es la mejor manera de configurarlo. Para el caso en particular de configuración de QoS, se debe recurrir a las respectivas guías de configuración del 2960X [14], del 3750-E [15] y del 2901[16], que usaría en el ejemplo el Controlador.

La siguiente ventaja de la abstracción, es que se puede determinar la función del equipo. Al saber la función, se puede saber cuál es la mejor manera de configurarlo. Para el caso particular, Cisco se basa en sus Guías Validadas de tecnologías, en donde se muestran buenas prácticas de configuración y plantillas de las líneas de comandos específicas para habilitar las funcionalidades dependiendo del uso del equipo en la red. Estas plantillas/guías específicas a las buenas prácticas de QoS están contenidas en el documento Medianet Campus QoS Design 4.0 [8].

De la misma manera, gracias al conocimiento de cada uno de los equipos de red, se puede entender, desde un nivel alto, como se encuentran los ACL configurados en los equipos, y por lo tanto cuál podría estar afectando la comunicación entre dos host.

El análisis de los ACL ya no se harían equipo por equipo de manera manual, tomando tiempo en reconocer la causa, sino que se haría en el controlador, que al tener la configuración de todos los equipos puede hacer ese análisis de forma simultánea y mostrarlo gráficamente.

En general, el CLI adaptado hace uso de la abstracción de los elementos para poder adecuar tanto el tipo de líneas de comando a usar debido a la función, como la mejor manera de configurar el equipo de acuerdo a su uso en la red.

El Controlador para el caso de estudio desarrollado en el presente informe, tiene la base de datos tanto de las guías de configuración como de las guías validadas de Cisco, y al abstraer un equipo de red crea una base de información de red (NIDB – Network Information Database) que sirve como único punto de fuente de información al mantener el inventario de los dispositivos de red y la abstracción de toda la infraestructura IT. El NIDB permite a las aplicaciones ser agnósticos al dispositivo (no preocuparse de que es

o como configurarlo) permitiendo que las diferencias de configuración entre diferentes dispositivos no sea un problema.

3.3 Solución del problema

A continuación se desarrolla la solución del problema, tanto por la metodología clásica de CLI, para entender lo complicado de la configuración, así como por la metodología alterna, el CLI Adaptado, proveyendo las ventajas del SDN.

3.3.1 Solución usando CLI

A continuación se desarrolla la configuración de QoS como la resolución de problemas de ACL.

a. Configuración de QoS

Para el ejemplo en particular, el proceso de configuración de los equipos es manual mediante línea de comandos. A continuación se muestra las líneas de comando mínima necesarias para empezar a configurar los parámetros de Calidad de Servicio. Para ello se toma como ejemplo el mostrado en las figuras 3.1 y 3.2. Estas líneas provienen de la guía de referencia de buenas prácticas de QoS para el switch de acceso 3750-X del caso de estudio.

```
SDN-CAMPUS-C3750X(config)#ip access-list extended MULTIMEDIA-CONFERENCING
SDN-CAMPUS-C3750X (config-ext-nacl)# remark RTP
SDN-CAMPUS-C3750X (config-ext-nacl)# permit udp any any range 16384 32767
 SDN-CAMPUS-C3750X (config)#ip access-list extended SIGNALING
SDN-CAMPUS-C3750X (config-ext-nacl)# remark SCCP
SDN-CAMPUS-C3750X (config-ext-nacl)# permit tcp any any range 2000 2002
SDN-CAMPUS-C3750X(config-ext-nacl)# remark SIP
SDN-CAMPUS-C3750X(config-ext-nacl)# permit tcp any any range 5060 5061
SDN-CAMPUS-C3750X(config-ext-nacl)# permit udp any any range 5060 5061
 SDN-CAMPUS-C3750X(config)#ip access-list extended TRANSACTIONAL-DATA
SDN-CAMPUS-C3750X(config-ext-nacl)# remark HTTPS
SDN-CAMPUS-C3750X(config-ext-nacl)# permit tcp any any eq 443
SDN-CAMPUS-C3750X(config-ext-nacl)# remark ORACLE-SQL*NET
SDN-CAMPUS-C3750X(config-ext-nacl)# permit tcp any any eq 1521
SDN-CAMPUS-C3750X(config-ext-nacl)# permit udp any any eq 1521
SDN-CAMPUS-C3750X(config-ext-nacl)# remark ORACLE
SDN-CAMPUS-C3750X(config-ext-nacl)# permit tcp any any eq 1526
SDN-CAMPUS-C3750X(config-ext-nacl)# permit udp any any eq 1526
SDN-CAMPUS-C3750X(config-ext-nacl)# permit tcp any any eq 1575
SDN-CAMPUS-C3750X(config-ext-nacl)# permit udp any any eq 1575
SDN-CAMPUS-C3750X(config-ext-nacl)# permit tcp any any eq 1630
SDN-CAMPUS-C3750X(config-ext-nacl)# permit udp any any eq 1526
 SDN-CAMPUS-C3750X(config)#ip access-list extended BULK-DATA
SDN-CAMPUS-C3750X(config-ext-nacl)# remark FTP
```

```
SDN-CAMPUS-C3750X(config-ext-nacl)# permit tcp any any eq ftp
SDN-CAMPUS-C3750X(config-ext-nacl)# permit tcp any any eq ftp-data
SDN-CAMPUS-C3750X(config-ext-nacl)# remark SSH/SFTP
SDN-CAMPUS-C3750X(config-ext-nacl)# permit tcp any any eq 22
SDN-CAMPUS-C3750X(config-ext-nacl)# remark SMTP/SECURE SMTP
SDN-CAMPUS-C3750X(config-ext-nacl)# permit tcp any any eq smtp
SDN-CAMPUS-C3750X(config-ext-nacl)# permit tcp any any eq 465
SDN-CAMPUS-C3750X(config-ext-nacl)# remark IMAP/SECURE IMAP
SDN-CAMPUS-C3750X(config-ext-nacl)# permit tcp any any eq 143
SDN-CAMPUS-C3750X(config-ext-nacl)# permit tcp any any eq 993
SDN-CAMPUS-C3750X(config-ext-nacl)# remark POP3/SECURE POP3
SDN-CAMPUS-C3750X(config-ext-nacl)# permit tcp any any eq pop3
SDN-CAMPUS-C3750X(config-ext-nacl)# permit tcp any any eq 995
SDN-CAMPUS-C3750X(config-ext-nacl)# remark CONNECTED PC BACKUP
SDN-CAMPUS-C3750X(config-ext-nacl)# permit tcp any eq 1914 any
SDN-CAMPUS-C3750X(config)#ip access-list extended SCAVENGER
SDN-CAMPUS-C3750X(config-ext-nacl)# remark KAZAA
SDN-CAMPUS-C3750X(config-ext-nacl)# permit tcp any any eq 1214
SDN-CAMPUS-C3750X(config-ext-nacl)# permit udp any any eq 1214
SDN-CAMPUS-C3750X(config-ext-nacl)# remark MICROSOFT DIRECT X GAMING
SDN-CAMPUS-C3750X(config-ext-nacl)# permit tcp any any range 2300 2400
SDN-CAMPUS-C3750X(config-ext-nacl)# permit udp any any range 2300 2400
SDN-CAMPUS-C3750X(config-ext-nacl)# remark APPLE ITUNES MUSIC SHARING
SDN-CAMPUS-C3750X(config-ext-nacl)# permit tcp any any eq 3689
SDN-CAMPUS-C3750X(config-ext-nacl)# permit udp any any eq 3689
SDN-CAMPUS-C3750X(config-ext-nacl)# remark BITTORRENT
SDN-CAMPUS-C3750X(config-ext-nacl)# permit tcp any any range 6881 6999
SDN-CAMPUS-C3750X(config-ext-nacl)# remark YAHOO GAMES
SDN-CAMPUS-C3750X(config-ext-nacl)# permit tcp any any eq 11999
SDN-CAMPUS-C3750X(config-ext-nacl)# remark MSN GAMING ZONE
SDN-CAMPUS-C3750X(config-ext-nacl)# permit tcp any any range 28800 29100
SDN-CAMPUS-C3750X(config)#ip access-list extended DEFAULT
SDN-CAMPUS-C3750X(config-ext-nacl)# remark EXPLICIT CLASS-DEFAULT
SDN-CAMPUS-C3750X(config-ext-nacl)# permit ip any any
SDN-CAMPUS-C3750X(config-cmap)#class-map match-all VVLAN-VOIP
SDN-CAMPUS-C3750X(config-cmap)# match ip dscp ef
SDN-CAMPUS-C3750X(config-cmap)#class-map match-all VVLAN-SIGNALING
SDN-CAMPUS-C3750X(config-cmap)# match ip dscp cs3
SDN-CAMPUS-C3750X(config-cmap)#class-map match-all MULTIMEDIA-CONFERENCING
SDN-CAMPUS-C3750X(config-cmap)# match access-group name MULTIMEDIA-CONFERENCING
SDN-CAMPUS-C3750X(config-cmap)#class-map match-all SIGNALING
SDN-CAMPUS-C3750X(config-cmap)# match access-group name SIGNALING
SDN-CAMPUS-C3750X(config-cmap)#class-map match-all TRANSACTIONAL-DATA
SDN-CAMPUS-C3750X(config-cmap)# match access-group name TRANSACTIONAL-DATA
```

```
SDN-CAMPUS-C3750X(config-cmap)#class-map match-all BULK-DATA
SDN-CAMPUS-C3750X(config-cmap)# match access-group name BULK-DATA
SDN-CAMPUS-C3750X(config-cmap)#class-map match-all SCAVENGER
SDN-CAMPUS-C3750X(config-cmap)# match access-group name SCAVENGER
SDN-CAMPUS-C3750X(config-cmap)#class-map match-all DEFAULT
SDN-CAMPUS-C3750X(config-cmap)# match access-group name DEFAULT
SDN-CAMPUS-C3750X(config-cmap)#policy-map PER-PORT-MARKING
SDN-CAMPUS-C3750X(config-pmap)# class VVLAN-VOIP
SDN-CAMPUS-C3750X(config-pmap-c)# set dscp ef
SDN-CAMPUS-C3750X(config-pmap-c)# class VVLAN-SIGNALING
SDN-CAMPUS-C3750X(config-pmap-c)# set dscp cs3
SDN-CAMPUS-C3750X(config-pmap-c)# class MULTIMEDIA-CONFERENCING
SDN-CAMPUS-C3750X(config-pmap-c)# set dscp af41
SDN-CAMPUS-C3750X(config-pmap-c)# class SIGNALING
SDN-CAMPUS-C3750X(config-pmap-c)# set dscp cs3
SDN-CAMPUS-C3750X(config-pmap-c)# class TRANSACTIONAL-DATA
SDN-CAMPUS-C3750X(config-pmap-c)# set dscp af21
SDN-CAMPUS-C3750X(config-pmap-c)# class BULK-DATA
SDN-CAMPUS-C3750X(config-pmap-c)# set dscp af11
SDN-CAMPUS-C3750X(config-pmap-c)# class SCAVENGER
SDN-CAMPUS-C3750X(config-pmap-c)# set dscp cs1
SDN-CAMPUS-C3750X(config-pmap-c)# class DEFAULT
SDN-CAMPUS-C3750X(config-pmap-c)# set dscp default
SDN-CAMPUS-C3750X(config)#interface range GigabitEthernet 5/0/1-48
SDN-CAMPUS-C3750X(config-if-range)# switchport access vlan 10
SDN-CAMPUS-C3750X(config-if-range)# switchport voice vlan 110
SDN-CAMPUS-C3750X(config-if-range)# spanning-tree portfast
SDN-CAMPUS-C3750X(config-if-range)# mls qos trust device cisco-phone
SDN-CAMPUS-C3750X(config-if-range)# mls qos trust cos
SDN-CAMPUS-C3750X(config-if-range)# service-policy input PER-PORT-MARKING
```

Esta plantilla ha servido para tomar como referencia la cantidad de líneas de comando que un administrador debería conocer y digitar como mínimo por equipo. Se menciona como mínimo, ya que cada equipamiento usado dentro del caso de estudio se tiene agregar más comandos específicos de acuerdo a la plataforma. En total son 98 líneas para el ejemplo, que si se saca un promedio de todas las configuraciones para el caso de estudio (15 equipos), el administrador debe de digitar más de 1470 líneas de comando en toda la red como mínimo.

En el caso de que el administrador desee hacer cambios, por ejemplo, en vez de tráfico de voz que sea otra aplicación, el administrador tiene que editar nuevamente las 1470 líneas de comando en toda la red. Como se puede observar, este proceso se vuelve manual, complejo y propenso a la falla humana.De allí la importancia de utilizar

metodologías SDN.

b. Resolución de problemas de ACL

Mediante el análisis de la configuración de los equipos, se puede identificar si alguna configuración de ACL está ocasionando problemas en el flujo de tráfico multimedia en la red. Lo primero que debe hacerse es mostrar las líneas dentro de la configuración de los equipos que corresponden a los ACL implementados. Este proceso es serial, es decir, hay que hacerlo uno por uno. En la siguiente figura se muestra la identificación de los ACL en un equipo usando el comando "show access-list".

```
SDN-CAMPUS-C3750X#
SDN-CAMPUS-C3750X#show access-lists
Extended IP access list 100
    10 deny udp any range 1235 1236 any
Extended IP access list 101
    10 deny udp any range 1235 1236 any
Extended IP access list 102
    10 permit tcp any any
Extended IP access list 103
    10 deny udp any range 1235 1236 any
Extended IP access list 104
    10 permit ip any any
Extended IP access list 105
    10 deny ip any any
Extended IP access list 108
    10 deny tcp any any
Extended IP access list 111
    10 deny udp any any
Extended IP access list preauth_ipv4_acl (per-user)
    10 permit udp any any eq domain
    20 permit tcp any any eq domain
    30 permit udp any eq bootps any
    40 permit udp any any eq bootpc
    50 permit udp any eq bootpc any
    60 deny ip any any
IPv6 access list preauth_ipv6_acl (per-user)
    permit udp any any eq domain sequence 10
    permit tcp any any eq domain sequence 20
    permit icmp any any nd-ns sequence 30
    permit icmp any any nd-na sequence 40
    permit icmp any any router-solicitation sequence 50
    permit icmp any any router-advertisement sequence 60
    permit icmp any any redirect sequence 70
    permit udp any eq 547 any eq 546 sequence 80
```

```
  permit udp any eq 546 any eq 547 sequence 90
  deny ipv6 any any sequence 100
SDN-CAMPUS-C3750X#
```

Luego se procede a identificar de que dispositivo origen a que dispositivo destino se está haciendo la comunicación multimedia (en el caso de estudio entre la IP Origen 10.7.7.13 a la IP Destino 26.6.6.8) para ver si algún ACL está ejecutándose impidiendo el paso del tráfico. De la información anterior, existen seis ACL que están deteniendo el tráfico de esa comunicación: ACL 100, ACL 101, ACL 103, ACL 105, ACL 108, ACL 111. Al determinar que ACLs pueden afectar el tráfico, se tiene que ver si alguno se está ejecutando en alguna interface de red. Con el comando "show run | begin interface" podemos ver si hay alguno ejecutándose:

```
SDN-CAMPUS-C3750X#sh run | begin interface
interface GigabitEthernet0/0
 vrf forwarding Mgmt-vrf
 no ip address
 negotiation auto
interface GigabitEthernet5/0/1
interface GigabitEthernet5/0/2
interface GigabitEthernet5/0/3
interface GigabitEthernet5/0/4
 ip access-group 100 in
interface GigabitEthernet5/0/5
interface GigabitEthernet5/0/6
interface GigabitEthernet5/0/7
interface GigabitEthernet5/0/8
interface GigabitEthernet5/0/9
interface GigabitEthernet5/0/10
interface GigabitEthernet5/0/11
interface GigabitEthernet5/0/12
interface GigabitEthernet5/0/13
interface GigabitEthernet5/0/14
interface GigabitEthernet5/0/15
interface GigabitEthernet5/0/16
interface GigabitEthernet5/0/17
interface GigabitEthernet5/0/18
interface GigabitEthernet5/0/19
interface GigabitEthernet5/0/20
interface GigabitEthernet5/0/21
interface GigabitEthernet5/0/22
interface GigabitEthernet5/0/23
interface GigabitEthernet5/0/24
```

```
interface GigabitEthernet5/1/1
interface GigabitEthernet5/1/2
interface GigabitEthernet5/1/3
interface GigabitEthernet5/1/4
interface TenGigabitEthernet5/1/1
interface TenGigabitEthernet5/1/2
interface TenGigabitEthernet5/1/3
interface TenGigabitEthernet5/1/4
```

En el caso particular, se encontró que en la interface GigabitEthernet 5/0/4 se encuentra ejecutándose el ACL 100, uno de los que están cortando el tráfico multimedia.

Con la cantidad de dispositivos que hay el ejemplo, el proceso mencionado hay que repetirse hasta encontrar subsiguientes puntos de corte de tráfico. En total se tendría que hacer el proceso 12 veces (la comunicación no pasa por los equipos que se encuentran en la Oficina Remota 1 – en total 3), lo cual toma tiempo y puede afectar la experiencia del usuario final. De allí la importancia de utilizar metodologías SDN.

3.3.2 Solución basada en SDN – APIC EM Controller (CLI Adaptado)

Usando la metodología descrita en 3.2, el controlador SDN Cisco APIC EM, permite poder abstraer la información de la infraestructura de red y crear una base de datos – NIDB. Las figuras 3.4 y 3.5 ilustran cómo es la estructura de esta base de datos.

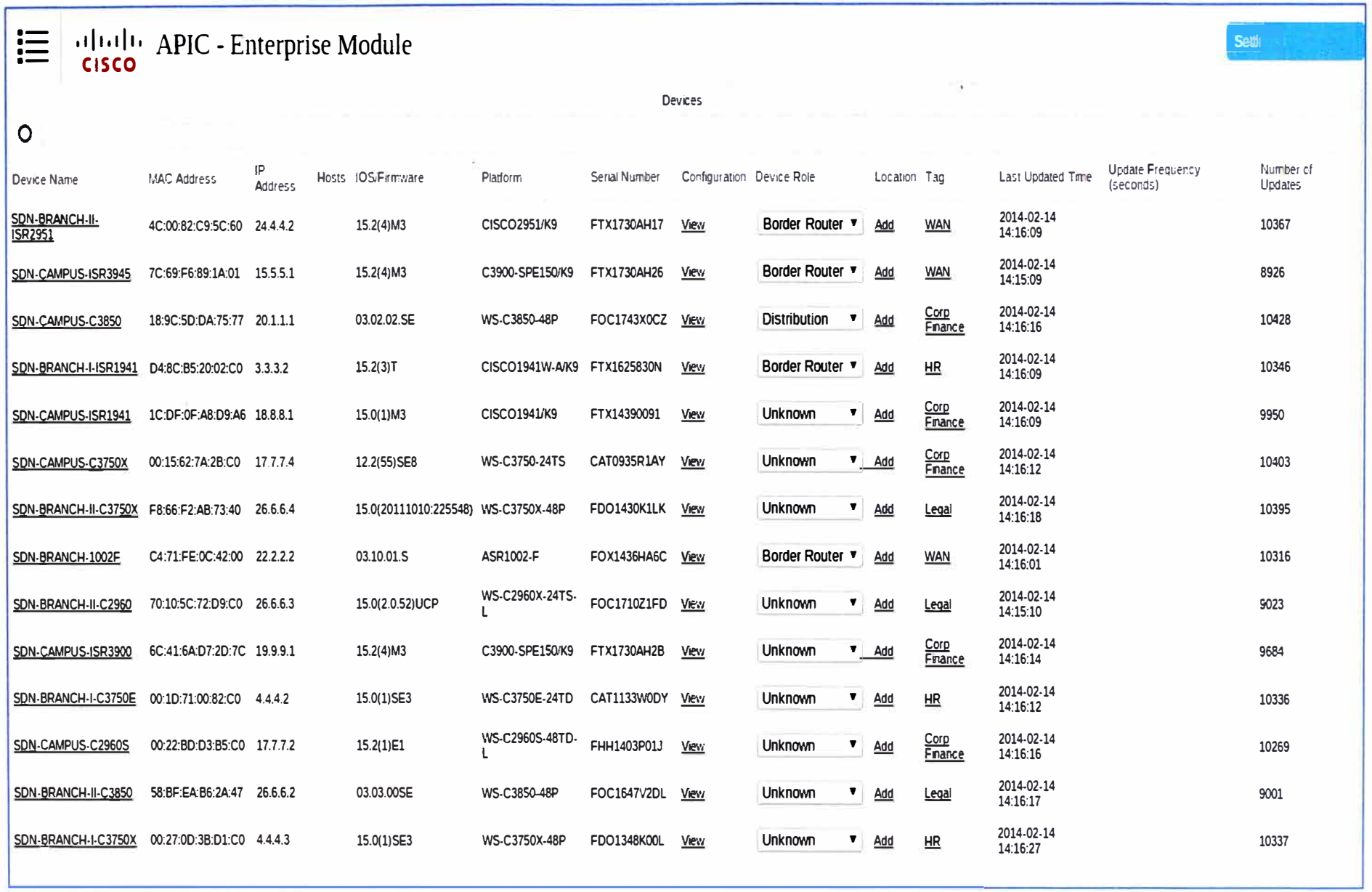
Como se muestra en aquellas figuras, la NIDB se compone de los siguientes campos de abstracción:

- MAC Address
- IP Address
- Host Asociados
- IOS/Firmware
- Plataforma
- Número Serial
- Rol del dispositivo
- Localización
- Detalles específicos de cada equipo (interfaces, estado de las interfaces, relación de los enlaces).

Con ello, el APIC-EM puede determinar la línea de comandos específica para cada equipamiento y las buenas prácticas necesarias de configuración para cada equipo.

De la misma manera, con la abstracción, APIC EM puede mostrar el diagrama topológico de la solución a nivel de conectividad, como se observa en la figura 3.6.

Esto permite tener una vista más clara de cómo está la red y el rol del equipamiento en la misma.



Device Name	MAC Address	IP Address	Hosts	IOS/Firmware	Platform	Serial Number	Configuration	Device Role	Location	Tag	Last Updated Time	Update Frequency (seconds)	Number of Updates
SDN-BRANCH-II-ISR2951	4C:00:82:C9:5C:60	24.4.4.2		15.2(4)M3	CISCO2951/K9	FTX1730AH17	View	Border Router	Add	WAN	2014-02-14 14:16:09		10367
SDN-CAMPUS-ISR3945	7C:69:F6:89:1A:01	15.5.5.1		15.2(4)M3	C3900-SPE150/K9	FTX1730AH26	View	Border Router	Add	WAN	2014-02-14 14:15:09		8926
SDN-CAMPUS-C3850	18:9C:5D:DA:75:77	20.1.1.1		03.02.02.SE	WS-C3850-48P	FOC1743X0CZ	View	Distribution	Add	Corp Finance	2014-02-14 14:16:16		10428
SDN-BRANCH-I-ISR1941	D4:8C:B5:20:02:C0	3.3.3.2		15.2(3)T	CISCO1941W-A/K9	FTX1625830N	View	Border Router	Add	HR	2014-02-14 14:16:09		10346
SDN-CAMPUS-ISR1941	1C:DF:0F:A8:D9:A6	18.8.8.1		15.0(1)M3	CISCO1941/K9	FTX14390091	View	Unknown	Add	Corp Finance	2014-02-14 14:16:09		9950
SDN-CAMPUS-C3750X	00:15:62:7A:2B:C0	17.7.7.4		12.2(55)SE8	WS-C3750-24TS	CAT0935R1AY	View	Unknown	Add	Corp Finance	2014-02-14 14:16:12		10403
SDN-BRANCH-II-C3750X	F8:66:F2:AB:73:40	26.6.6.4		15.0(20111010:225548)	WS-C3750X-48P	FDO1430K1LK	View	Unknown	Add	Legal	2014-02-14 14:16:18		10395
SDN-BRANCH-1002F	C4:71:FE:0C:42:00	22.2.2.2		03.10.01.S	ASR1002-F	FOX1436HA6C	View	Border Router	Add	WAN	2014-02-14 14:16:01		10316
SDN-BRANCH-II-C2960	70:10:5C:72:D9:C0	26.6.6.3		15.0(2.0.52)UCP	WS-C2960X-24TS-L	FOC1710Z1FD	View	Unknown	Add	Legal	2014-02-14 14:15:10		9023
SDN-CAMPUS-ISR3900	6C:41:6A:D7:2D:7C	19.9.9.1		15.2(4)M3	C3900-SPE150/K9	FTX1730AH2B	View	Unknown	Add	Corp Finance	2014-02-14 14:16:14		9684
SDN-BRANCH-I-C3750E	00:1D:71:00:82:C0	4.4.4.2		15.0(1)SE3	WS-C3750E-24TD	CAT1133W0DY	View	Unknown	Add	HR	2014-02-14 14:16:12		10336
SDN-CAMPUS-C2960S	00:22:BD:D3:B5:C0	17.7.7.2		15.2(1)E1	WS-C2960S-48TD-L	FHH1403P01J	View	Unknown	Add	Corp Finance	2014-02-14 14:16:16		10269
SDN-BRANCH-II-C3850	58:BF:EA:B6:2A:47	26.6.6.2		03.03.00SE	WS-C3850-48P	FOC1647V2DL	View	Unknown	Add	Legal	2014-02-14 14:16:17		9001
SDN-BRANCH-I-C3750X	00:27:0D:3B:D1:C0	4.4.4.3		15.0(1)SE3	WS-C3750X-48P	FDO1348K00L	View	Unknown	Add	HR	2014-02-14 14:16:27		10337

Figura 3.4 Base de datos de abstracción del APIC-EM (NIDB).(Fuente: Cisco Systems).

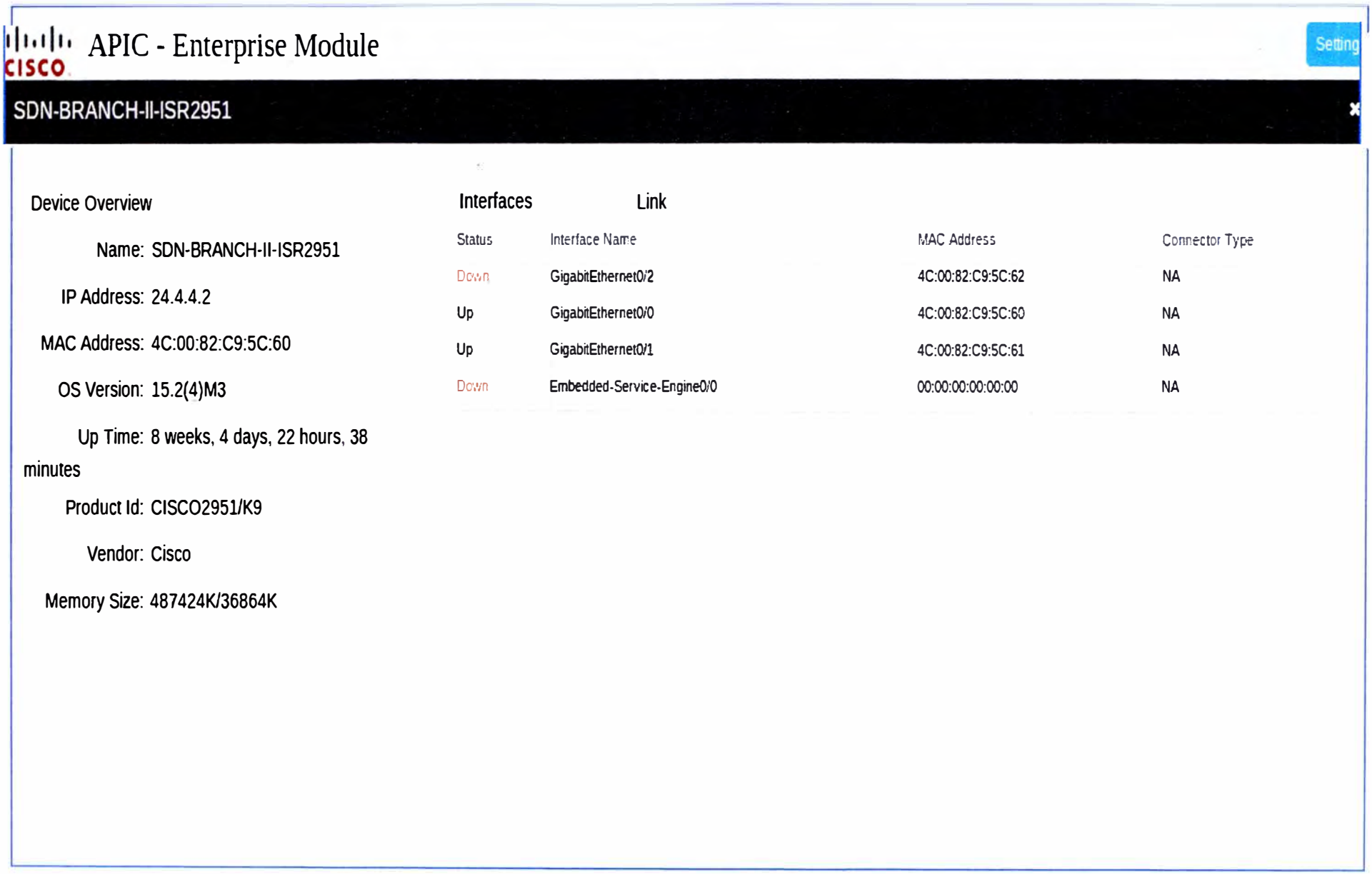


Figura 3.5 Detalles específicos abstraídos por APIC-EM para tener más información del equipamiento de la red (Fuente: Cisco Systems).

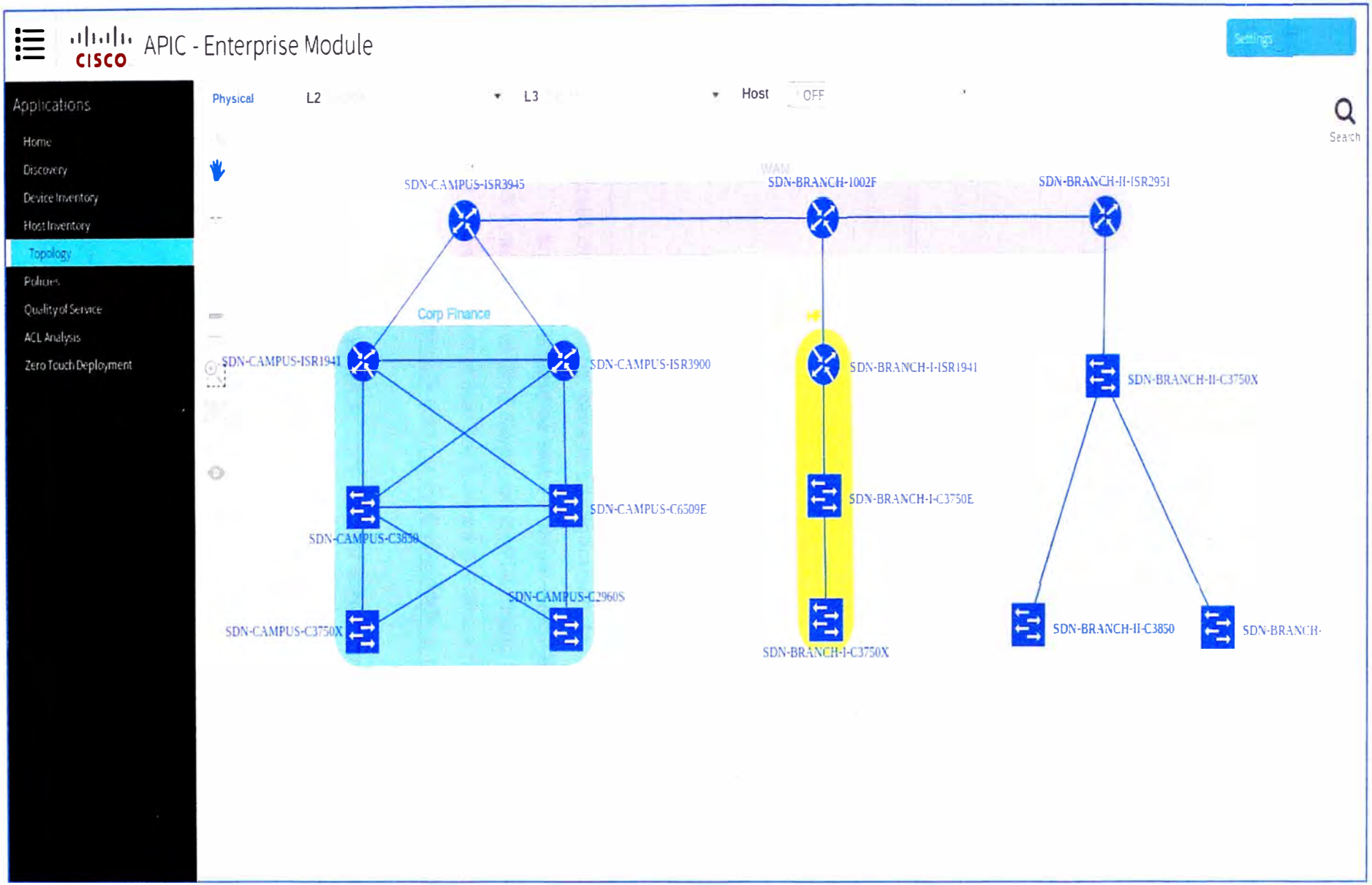


Figura 3.6 Diagrama Topológico abstraído por APIC-EM.(Fuente: Cisco Systems).

a. Configuración de QoS.

APIC-EM viene con una aplicación llamada Quality of Service. En las figuras 3.7 a 3.9, se muestra el proceso de configuración de la red basado en las buenas prácticas de Cisco en un GUI amigable, y mediante clicks, cómo la red se configura usando CLI adaptado.

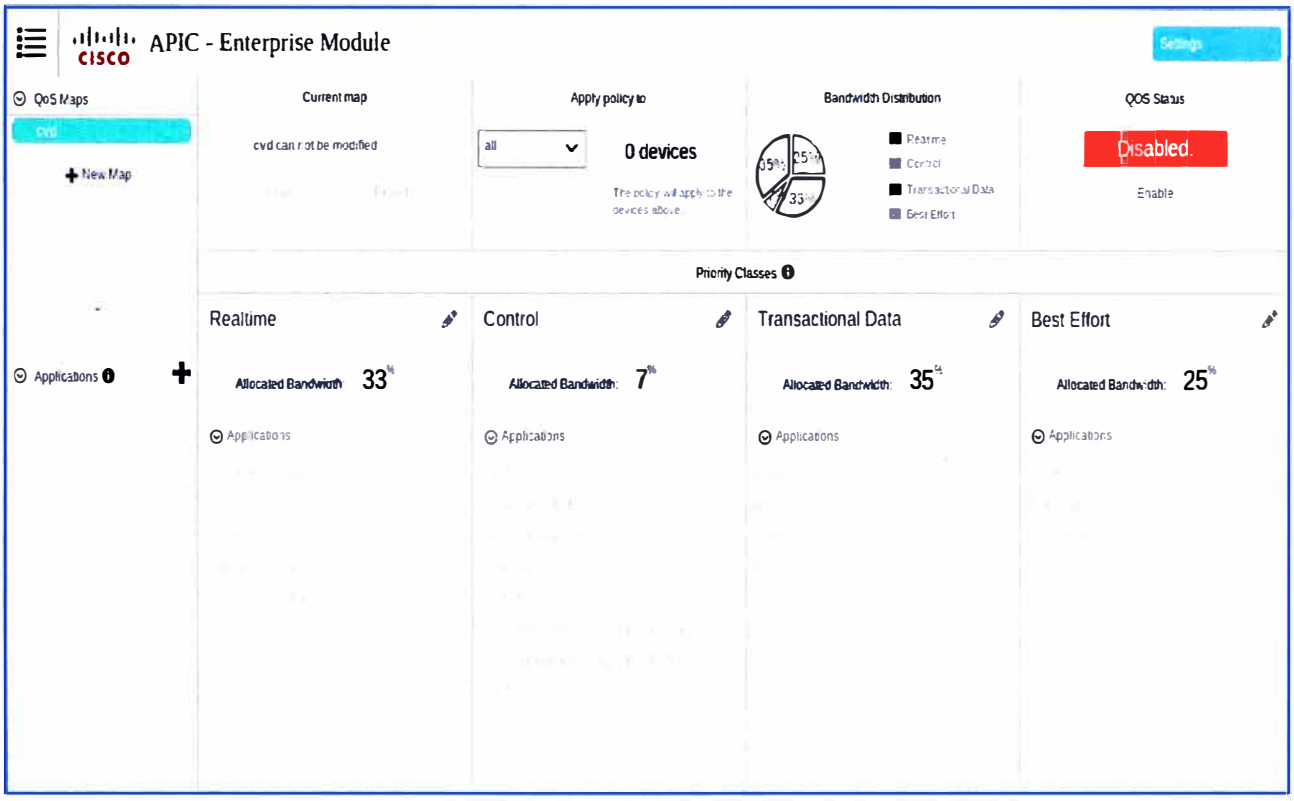


Figura 3.7 Pantalla de QoS Maps, para la configuración de QoS.Política no asignada aún a ningún equipo de red. (Fuente: Cisco Systems).

En la figura 3.7, se ve en el QoS Maps, un perfil llamado CVD que viene del acrónimo Cisco Validated Design, que traduce las buenas prácticas de Cisco en la red. Como se puede apreciar, la política de QoS aún no está asignada a ningún equipo, y por lo tanto aún no está habilitada.

Al seleccionar el perfil CVD, en la parte inferior automáticamente se asocian los tipos de tráfico a las clases de prioridad que vienen bajo la recomendación de mejores prácticas. El administrador no tuvo que intervenir en la asignación de las aplicaciones por cola.

Los parámetros pre-asignados por la recomendación son el tipo de cola que le corresponde a cada aplicación, así como también el ancho de banda asignado por cada cola.

En la figura 3.8, se escoge los 15 dispositivos del diagrama referencial a los cuales se desea aplicar las políticas de QoS recomendadas. Este proceso toma un click.

Finalmente el administrador habilita el QoS Map – CVD en toda la red. (Figura 3.9)

Figura 3.8 Pantalla de QoS Maps, para la configuración de QoS.Se seleccionan los dispositivos a configurar QoS.(Fuente: Cisco Systems).

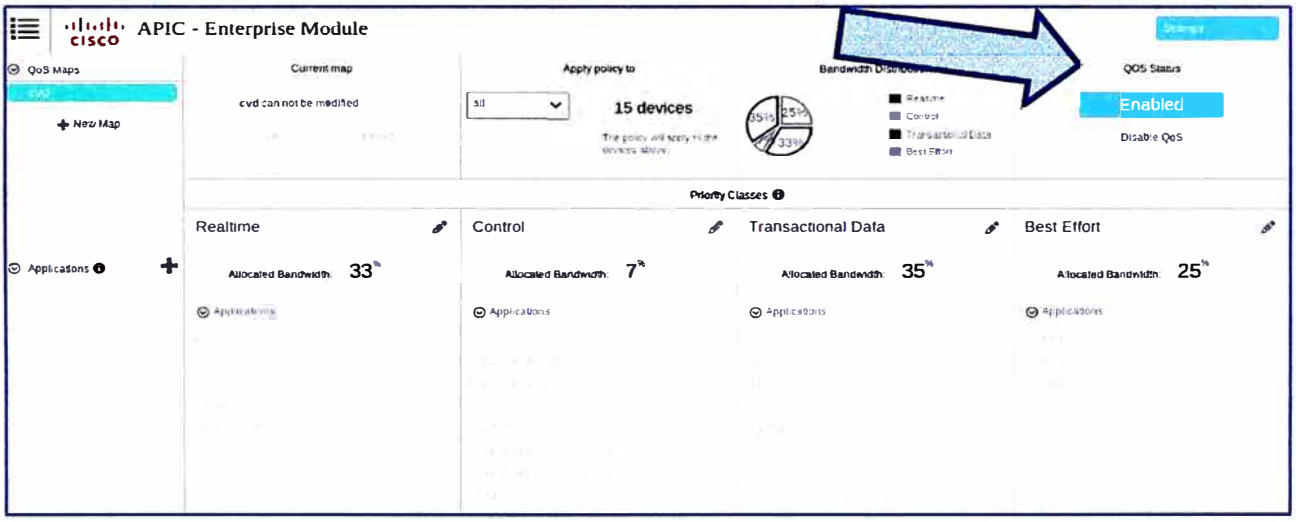


Figura 3.9 Pantalla de QoS Maps, paraconfiguración QoS. Habilitación de QoS.

De requerir una asignación de prioridades en otras clases de QoS, o asignar una aplicación no conocida a una cola determinada, el administrador puede agregar un nuevo Mapa y asignarlos mediante el proceso de "drag and drop". En el Anexo A, las figuras A.1 a A.6, ilustran el proceso de creación de un nuevo QoS Map.

b. Resolución de problemas de ACL

APIC-EM viene con una aplicación llamada ACL Analysis. En ella se puede colocar el origen y el destino de la comunicación multimedia, y mediante el uso del diagrama topológico abstraído, se puede lograr hacer el análisis del impacto de los ACL de la red en este flujo. En la figura 3.10 se muestra este proceso.

Luego de hacer la selección de los dispositivos origen y destino, mediante el uso de la función Trace, se puede visualizar donde está el flujo de tráfico, donde se encuentra el ACL que está bloqueando la comunicación y la sentencia de ACL específica. En la figura 3.11 se muestra el resultado arrojado por APIC-EM.

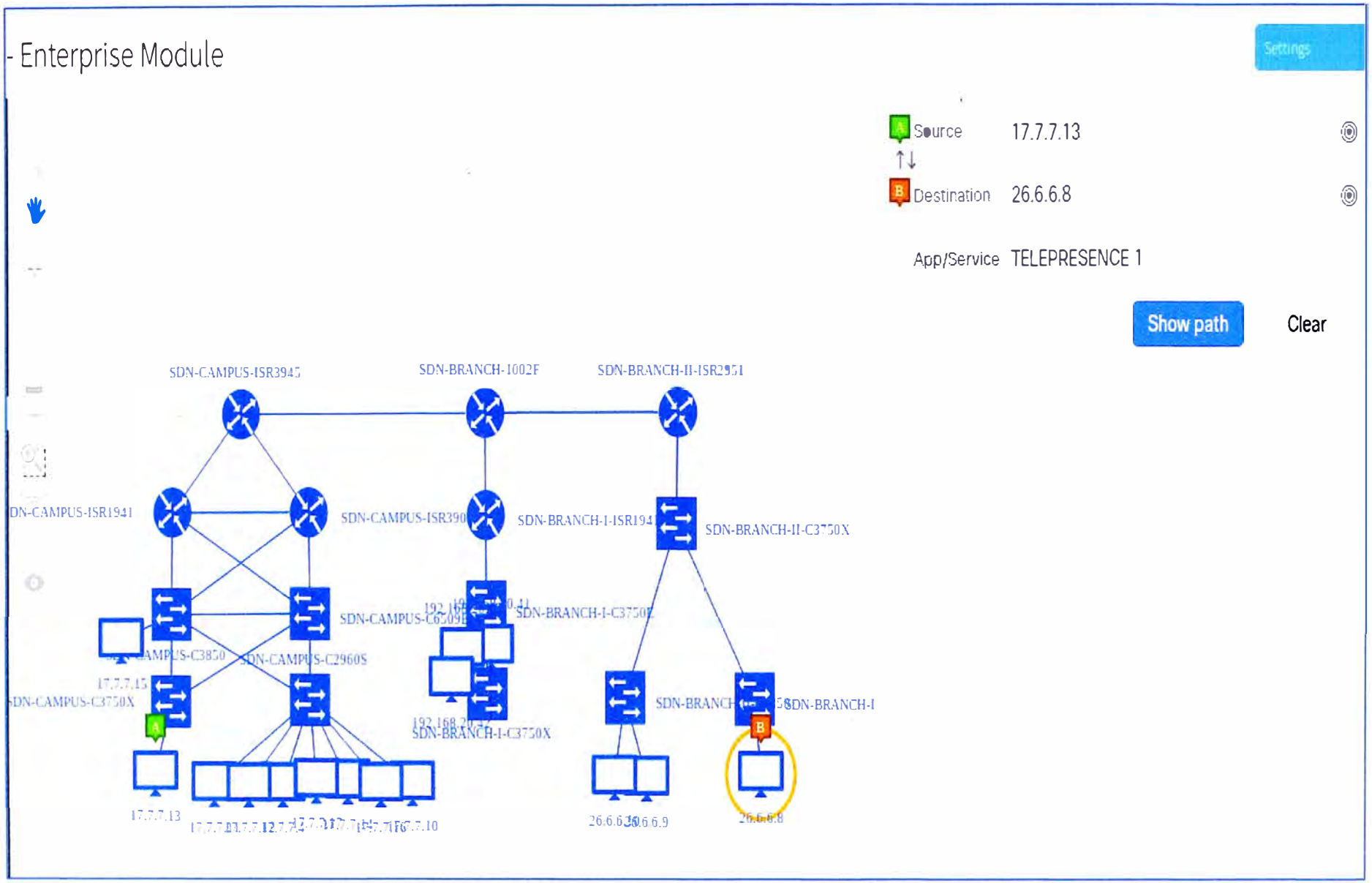


Figura 3.10ACL Analysis APIC-EM - Selección de Dispositivo Origen y Dispositivo Destino.(Fuente: Cisco Systems).

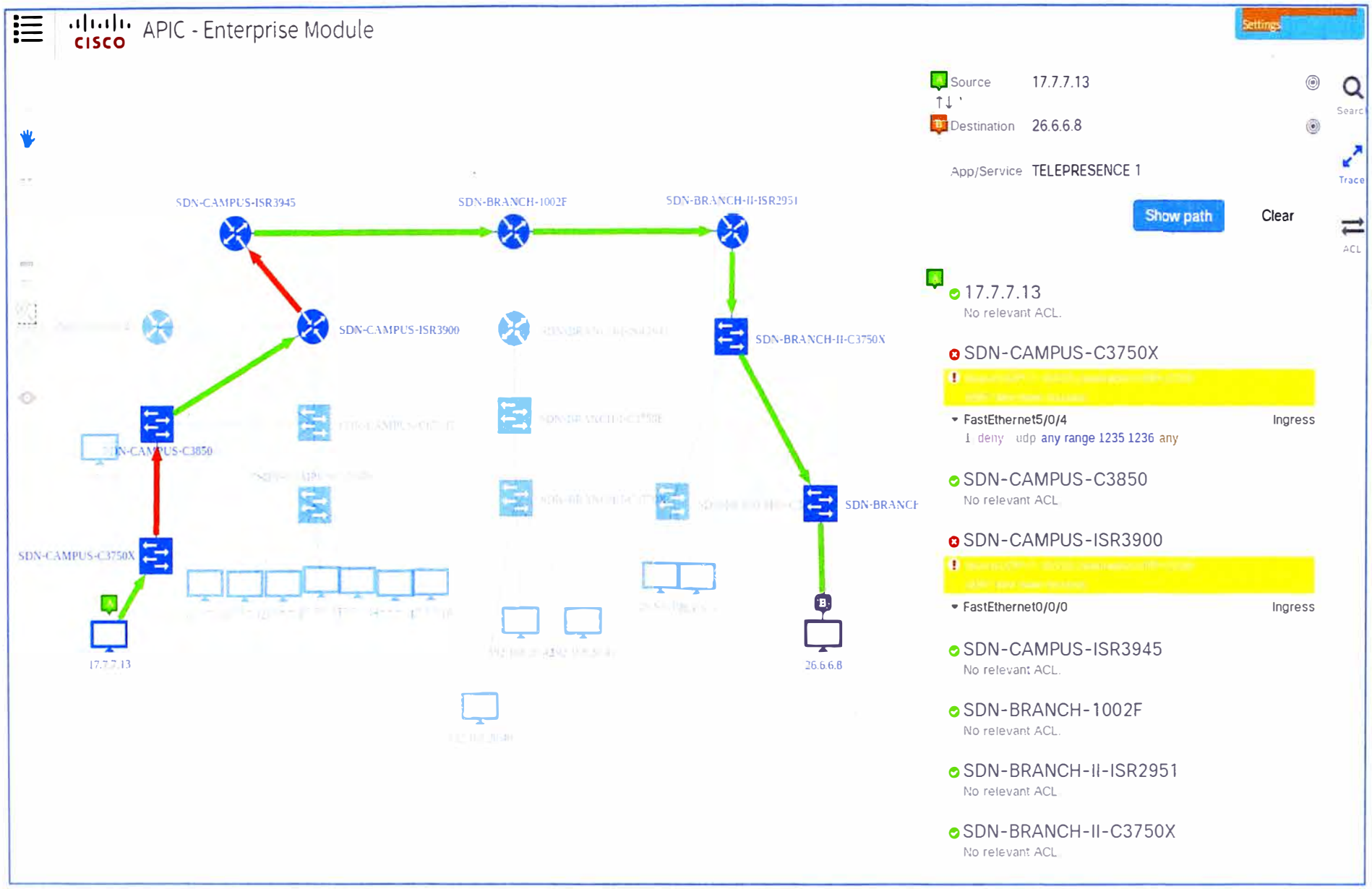


Figura 3.11 ACL Analysis APIC-EM-Flujo del tráfico multimedia e identificación de ACL que bloquean el flujo en flechas rojas.(Cisco).

En general, tanto en la configuración de QoS como en la problemática de ACL mediante el APIC-EM se sigue usando la metodología explicada en el punto 3.2 – CLI Adaptado.

3.4Análisis comparativo de ambas soluciones

A continuación se muestra, en la tabla 3.1, el cuadro comparativo del resultado de ambas soluciones.

Tabla 3.1 Cuadro Comparativo del resultado de ambas soluciones (Elab. Propia)

Características	**Método Tradicional (CLI)**	**Método Actual (SDN)**
Facilidad de Configuración	Difícil	Sencillo
Experiencia del Administrador	Requiere conocimientos avanzados de configuración de líneas de comando y troubleshooting para QoS y ACL.	Requiere conocimientos básicos en el funcionamiento de QoS y ACL.
Cantidad de pasos a seguir para Configuración de ACL	Elevada. En el caso de estudio, se llegó a más de mil líneas de comando.	Baja. Con unos cuantos clicks se puede configurar la red del caso de estudio.
Complejidad ante el aumento de equipamiento en la red	Alta. Mayor cantidad de equipamiento, más complejo el mantenimiento de las configuraciones y el troubleshooting.	Baja. El Controlador sigue redescubriendo la red ante nuevo equipamiento y mantiene actualizada su NIDB constantemente.
Tiempo de Configuración	Elevado. Configuración en 15 equipos del caso de estudio.	Bajo. Configuración directamente en el Controlador.
Simplicidad en la gestión	No es simple. La interface del sistema operativo en donde se coloca la línea de comandos no es simple.	Simple. Basado en un GUI por Web 2.0 de fácil entendimiento y simple.
Interpretación de resultados en Troubleshooting	Troubleshooting de manera individual por equipo, haciendo la interpretación más difícil.	Troubleshooting de manera centralizada y gráfica.

CAPÍTULO IV
ANÁLISIS Y PRESENTACIÓN DE RESULTADOS

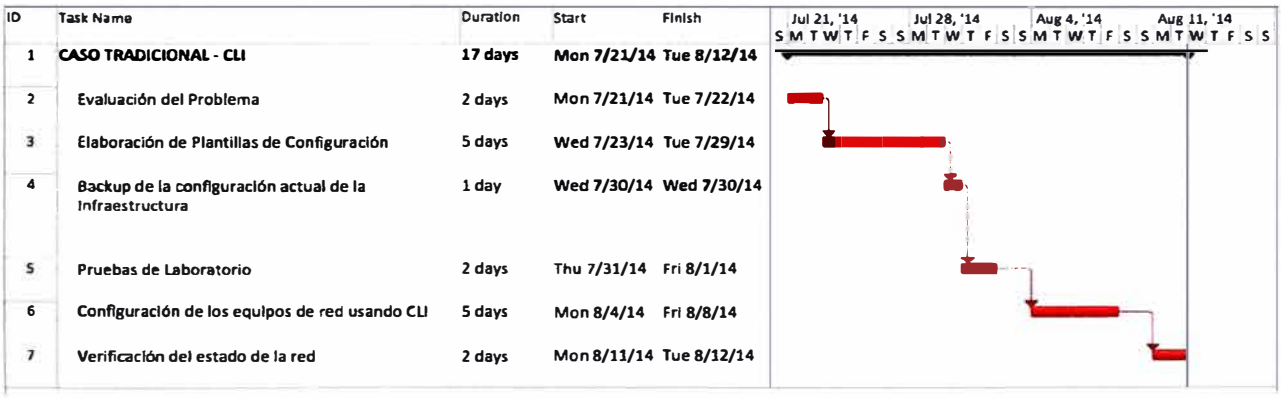
En este capítulo se desarrollan los aspectos relacionados al tiempo de ejecución y a los costos del proyecto.

4.1 Tiempo de Ejecución

En este punto se hace un análisis de los tiempos de ejecución de la implementación de QoS en la red ejemplo. Para este caso particular, se tiene que entender que la red se encuentra en producción, y por lo tanto no es equipamiento nuevo el que se agrega a la infraestructura, por lo tanto el proceso de implementación es más crítico y de no hacerse una correcta implementación, esta puede llevar a impactar el tráfico multimedia en la red.

4.1.1 CLI tradicional

En la figura 4.1, se muestran las tareas y los tiempos que se tomaría el encargado de la implementación en realizar las configuraciones de QoS para tráfico multimedia en la red usando el método tradicional por líneas de comando (CLI).



ID	Task Name	Duration	Start	Finish
1	**CASO TRADICIONAL - CLI**	**17 days**	**Mon 7/21/14**	**Tue 8/12/14**
2	Evaluación del Problema	2 days	Mon 7/21/14	Tue 7/22/14
3	Elaboración de Plantillas de Configuración	5 days	Wed 7/23/14	Tue 7/29/14
4	Backup de la configuración actual de la Infraestructura	1 day	Wed 7/30/14	Wed 7/30/14
5	Pruebas de Laboratorio	2 days	Thu 7/31/14	Fri 8/1/14
6	Configuración de los equipos de red usando CLI	5 days	Mon 8/4/14	Fri 8/8/14
7	Verificación del estado de la red	2 days	Mon 8/11/14	Tue 8/12/14

Figura 4.1 Diagrama de Gantt - CLI tradicional (Fuente: Elab. propia)

Para la configuración con el método tradicional mediante líneas de comando, se tiene que tener en consideración las siguientes tareas de implementación:

1. Evaluación del Problema: El encargado de la implementación tiene que entender los objetivos de la implementación, los contactos o responsables de la red, pre-requisitos del sistema, entender el equipamiento que existe, el sistema operativo, el tipo de aplicaciones que se debe de priorizar, el posible impacto en la red ante los cambios previstos, posibles métodos de rollback en caso de falla, los niveles de escalación en caso falle la implementación, etc. En esta etapa el encargado de la implementación tiene que crear un documento de alto nivel detallando lo encontrado en la red, y esperar la

aceptación del cliente final.

2. Elaboración de Plantillas de Configuración: En esta etapa, el encargado de la implementación con la información de la primera etapa, tiene que investigar las guías de configuración de los equipos, la compatibilidad en los sisitemas operativos presentes en la red y el rol de los equipos. De la misma manera, determinar las mejores prácticas de configuración de los equipos de la red. Con ello procede a la creación de plantillas de configuración, con las líneas de comando a implementar en los equipos de red, esto con el fin de poder realizar los cambios de manera más eficiente. En esta etapa el encargado de la implementación tiene que crear un documento de bajo nivel detallando las configuraciones, plantillas y procedimientos a tomar para la implementación de QoS en la red, luego tiene que esperar la aceptación del cliente final.

3. Backup de la configuración actual de la infraestructura: El encargado de la implementación tiene que hacer backup de la configuración actual de la infraestructura para poder lograr dos cosas: en un laboratorio replicar a menor escala la red actual del cliente y probar las plantillas creadas en el punto anterior y también permite tener las configuraciones con la cual la red está operando correctamente para casos de rollback.

4. Pruebas de Laboratorio: Con las configuraciones de backup y las plantillas creadas, se recrea la red del cliente a menor escala para determinar si existió alguna falla en la sintaxis de las plantillas, si estas plantillas al ser aplicadas logran el fin de dar prioridad a las aplicaciones multimedia, y poder anticipar algún problema que pueda existir durante la implementación. En esta etapa, el encargado de la implementación crea un documento de protocolo de pruebas que se usará para probar la red luego de la implementación. Se espera la aceptación del cliente al protocolo de pruebas.

5. Configuración de los equipos de red usando CLI: Lo probado en las pruebas de laboratorio, se implementa en la red en producción, en un espacio de tiempo muerto o de poco tráfico para impactar al mínimo la red.

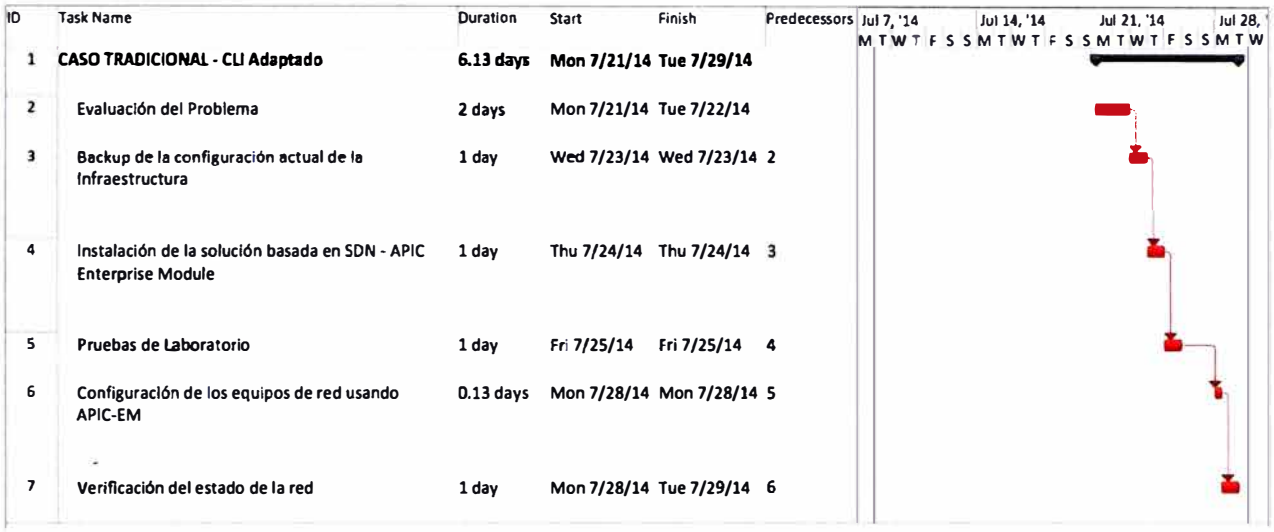
6. Verificación del estado de la red: Luego de la configuración de los equipos, se procede a ejecutar el protocolo de pruebas para determinar si la red sigue operando como lo esperado, determinar si no hay disrupción de servicios en la red, y probar en tráfico con mayor demanda si la implementación cubre los objetivos inciales del proyecto. En esta etapa el encargado de la implementación procede a firmar un acta de conformidad ante la implementación.

Todo el proceso usando el método tradicional de líneas de comando toma un total de 17 días a 8 horas por día de trabajo.

4.1.2 CLI adaptado

En la figura 4.2, se muestran las tareas y los tiempos que se tomaría el encargado de

la implementación en realizar las configuraciones de QoS para tráfico multimedia en la red usando el método tradicional por líneas de comando (CLI).



ID	Task Name	Duration	Start	Finish	Predecessors
1	**CASO TRADICIONAL - CLI Adaptado**	**6.13 days**	**Mon 7/21/14**	**Tue 7/29/14**	
2	Evaluación del Problema	2 days	Mon 7/21/14	Tue 7/22/14	
3	Backup de la configuración actual de la Infraestructura	1 day	Wed 7/23/14	Wed 7/23/14	2
4	Instalación de la solución basada en SDN - APIC Enterprise Module	1 day	Thu 7/24/14	Thu 7/24/14	3
5	Pruebas de Laboratorio	1 day	Fri 7/25/14	Fri 7/25/14	4
6	Configuración de los equipos de red usando APIC-EM	0.13 days	Mon 7/28/14	Mon 7/28/14	5
7	Verificación del estado de la red	1 day	Mon 7/28/14	Tue 7/29/14	6

Figura 4.2 Diagrama de Gantt - CLI adaptado (Fuente: Elab. propia)

Para la configuración con el método CLI adaptado, se tiene que tener en consideración las siguientes tareas de implementación:

1. Evaluación del Problema: El encargado de la implementación tiene que entender los objetivos de la implementación, los contactos o responsables de la red, pre-requisitos del sistema, el posible impacto en la red ante los cambios previstos, posibles métodos de rollback en caso de falla, los niveles de escalación en caso falle la implementaciolos etc. En esta etapa el encargado de la implementación tiene que crear un documento de alto nivel detallando lo encontrado en la red, y esperar la aceptación del cliente final.
2. Backup de la configuración actual de la infraestructura: El encargado de la implementación tiene que hacer backup de la configuración actual de la infraestructura para poder tener las configuraciones con la cual la red está operando correctamente y usarlos en caso de rollback ante fallas. También se usará estas configuraciones para replicar la red en menor escala en el laboratorio. En esta etapa el encargado de la implementación tiene que crear un documento de bajo nivel detallando el procedimiento a tomar para la implementación de QoS en la red mediante el uso de SDN CLI adaptado, luego tiene que esperar la aceptación del cliente final.
3. Instalación de la Solución de Software basado en SDN – CLI Adaptado: Se instala el software con los parámetros necesarios para integrarlo a la red (direccionamiento IP, DNS, nombre de dominio, etc). Se determina si el software fue instalado correctamente para luego ser usado en las pruebas de laboratorio.
4. Pruebas de Laboratorio: Con las configuraciones de backup se recrea la red del cliente a menor escala y se coloca el Software SDN en la red piloto. El software descubre el equipamiento en la red y realiza la tarea de abstracción. Luego se configura el Software

para que pueda habilitar QoS bajo las buenas prácticas de configuración en la red. Con esto se determina el posible impacto de los cambios hechos por el software y anticipar si existen problemas luego de la configuración. En esta etapa, el encargado de la implementación crea un documento de protocolo de pruebas que se usará para probar la red luego de la implementación. Se espera la aceptación del cliente al protocolo de pruebas.

5. Configuración de los equipos usando el Software SDN CLI Adaptado: Se lleva el software que fue instalado con los parámetros de red previos y se inserta en la red de producción en un espacio de tiempo muerto o de poco tráfico para impactar al mínimo la red. Se ejecuta desde el software el descubrimiento de la red y este hace el proceso de abstracción. Luego se escoge el perfil de CVD (Cisco Validated Designs), se escoge los equipos de la red y se ejecuta la orden de configuración usando CLI Adaptado.

6. Verificación del estado de la red: Luego de la configuración de los equipos usando CLI Adaptado, se procede a ejecutar el protocolo de pruebas para determinar si la red sigue operando como lo esperado, determinar si no hay disrupción de servicios en la red, y probar en tráfico con mayor demanda si la implementación cubre los objetivos inciales del proyecto. En esta etapa el encargado de la implementación procede a firmar un acta de conformidad ante la implementación.

Todo el proceso usando el método SDN de CLI Adaptado toma un total de 6.13 días a 8 horas por día de trabajo.

Se concluye que el tiempo de implementación usando el método tradicional es mayor que el tiempo de implementación del método usando SDN.

4.2. Costos del proyecto

Debido a que es una red en producción, no se requiere equipamiento adicional para el método tradicional. Solo se emplea horas hombre para la implementación. En el caso del método SDN, se tiene que incluir el costo del licenciamiento del software SDN y también las horas-hombre de implementación. En la tabla 4.1 se muestran los resultados del análisis de costo del proyecto para ambos casos.

Tabla 4.1 Análisis de Costos (Fuente: Elab. propia)

Método	Cantidad de días	Horas trabajadas por día	Horas totales	Costo de Hora Hombre (soles)	Costo total Servicio de Implementación (soles)	Costo de Equipamiento (soles)	Total de Costo del Proyecto
Tradicional - CLI	17	8	136	35	4760	0	4760
SDN - CLI Adaptado	6.13	8	49.04	35	1716.4	5560	7276.4

De la tabla 4.1, se puede apreciar que el costo de implementación en el método tradicional es 2.7 veces el costo de implementación usando el método SDN. Por el contrario, el costo de comprar el software para SDN es mayor, pero no es un costo recurrente, permitiendo al administrador realizar otras tareas relacionadas a la priorización del tráfico multimedia.

En general en el tiempo, si el administrador desea hacer más cambios en la red con respecto al tráfico multimedia, recurría en mayores costos. Esto se puede apreciar en la tabla 4.2 en donde se simula tres cambios en la red de la misma naturaleza analizada:

Tabla 4.2 Análisis de Costos de cambios en la red (Fuente: Elab. propia)

Método	Implementación 1 (soles)	Implementación 2 (soles)	Implementación 3 (soles)	Costo Total
Tradicional - CLI	4760	4760	4760	14280
SDN - CLI Adaptado	7276.4	1716.4	1716.4	10709.2

Se puede apreciar, que a partir del tercer cambio, el método tradicional sobrepasa los costos de usar el método SDN.

Nota:

- Costos de hora hombre en base a datos de empresas de tecnología de redes Cisco.
- Costo del software basado en la cantidad de equipamiento en la red.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Se concluye que la aplicación delos métodos alternativos a los tradicionales si reducen la complejidad inherente a la administración de la red ante el aumento de la densidad de su equipamiento, como fue el del caso de estudio presentado
2. En el presente informe se compararon los métodos tradicionales de configuración, específicamente el uso de CLI y los métodos actuales de configuración usando SDN – CLI Adaptado.
3. Se concluye, basado en el caso de estudio, que existe complejidad en los métodos tradicionales basados en CLI y que puede ser propenso a errores humanos y a lentitud en la resolución de problemas del tráfico multimedia.
4. Se concluye, basado en el caso de estudio, que el uso de SDN mediante una de sus formas de configuración (CLI Adaptado) también se obtienen los beneficios de reducción de la complejidad de sobremanera, permitiendo al administrador configurar la red de manera sencilla y poder resolver problemas de tráfico multimedia de forma rápida y eficiente.

Recomendaciones

1. Se recomienda empezar a adoptar infraestructura que soporte ya métodos de configuración basado en SDN (Openflow y onePK) debido a que es una gran tendencia en el mercado el poder hacer la centralización del plano de control.
2. Se recomienda que en el caso de redes tradicionales, en donde aún no se tiene pensado una modernización de la misma, se pueda empezar a usar métodos de SDN basado en CLI adaptado. Esto permitirá poder sacar provecho a la inversión que se tiene y el empezar a disfrutar las bondades de la configuración de SDN.
3. Se recomienda la evaluación de controladores que están bajo el soporte de fabricantes reconocidos. Esto asegura que exista interoperabilidad de la plataforma de red y la resolución de problemas que puedan existir en el Controlador.
4. Se recomienda comenzar a evaluar aplicaciones que usen las interfaces northbound de los Controladores más allá de solo ACL Analysis y QoS. En el mercado existen

muchos startups que desarrollan aplicaciones para mejorar la gestión de la infraestructura.

5. Se recomienda que en caso de redes críticas y con información sensible, se comience a analizar la alta disponibilidad del controlador, sin el cual toda la inteligencia de la infraestructura se perdería. De la misma manera, una opción a ello es poder tener infraestructura que trabaje de manera híbrida, es decir, que todavía mantenga ciertas capacidades de control en caso falle el Controlador.

ANEXO A
CONFIGURACIÓN DE NUEVO QOS MAP EN EL APIC-EM

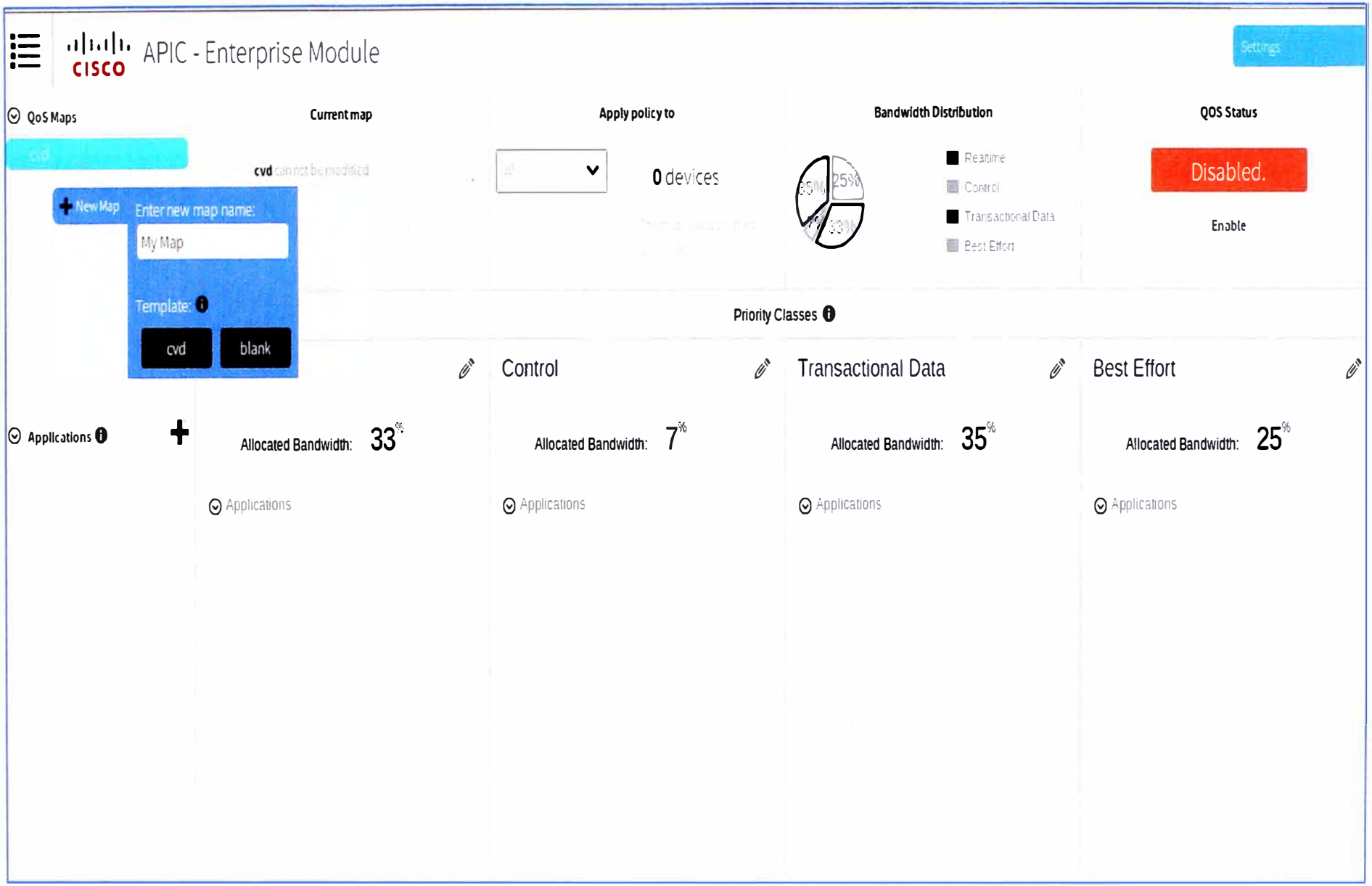


Figura A.1 Creación de nuevo QoS Map: MyMap.(Fuente: Cisco APIC Enterprise Module).

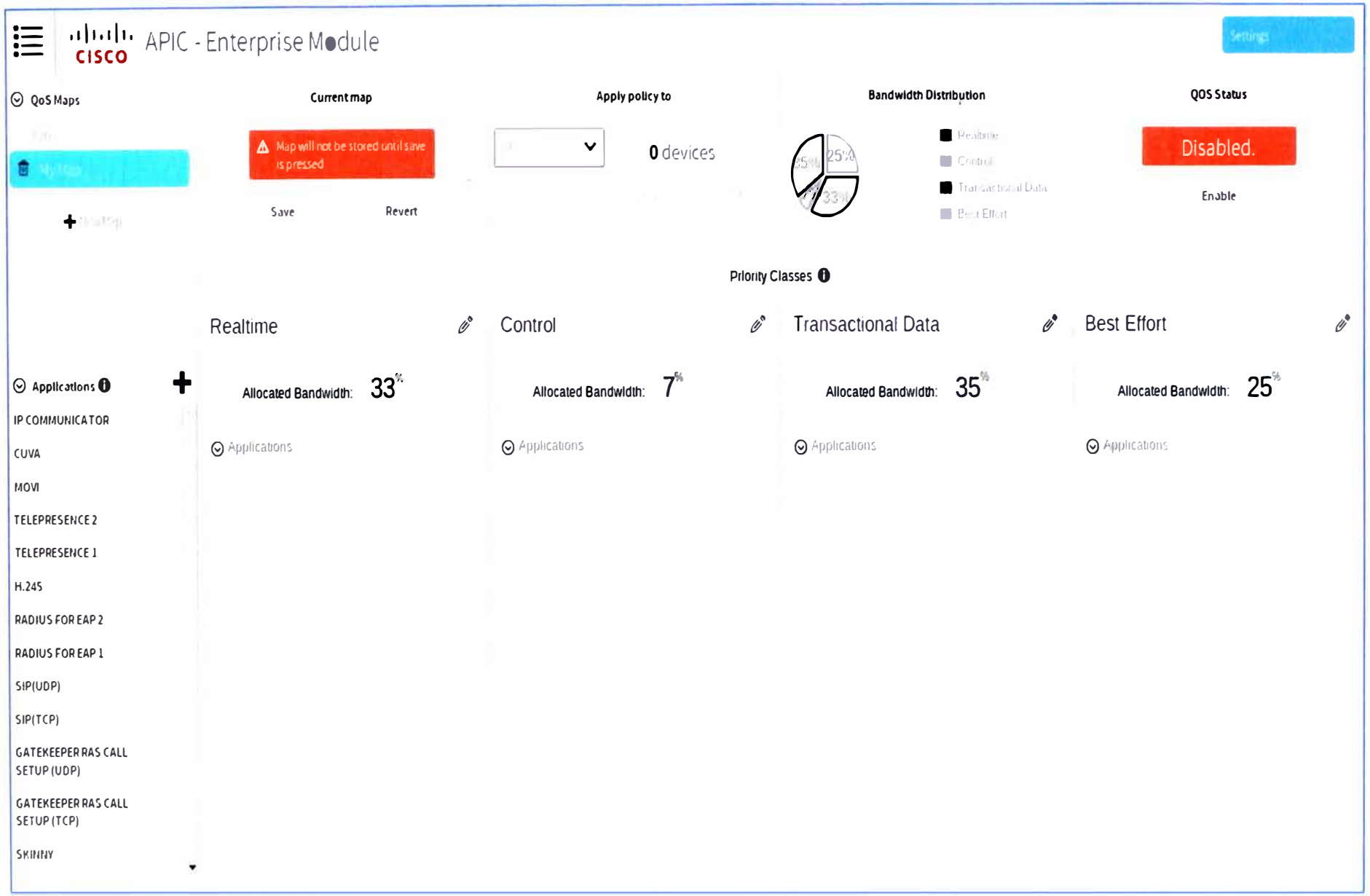


Figura A.2 MyMap creado, se observa que ya no hay aplicaciones por defecto en ninguna cola.(Fuente: Cisco APIC Enterprise Module).

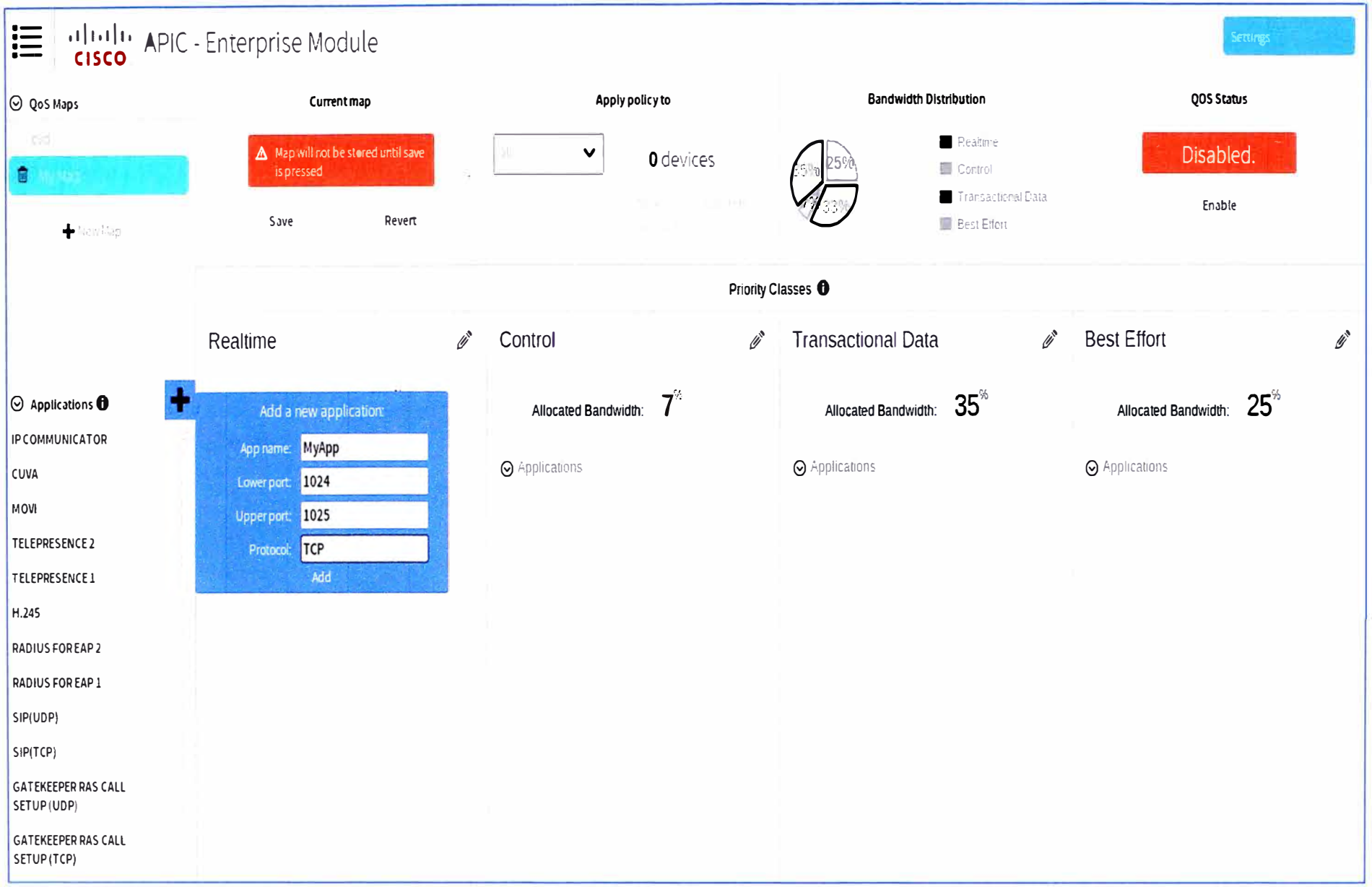


Figura A.3 Creación de nueva aplicación personalizada MyApp(Fuente: Cisco APIC Enterprise Module).

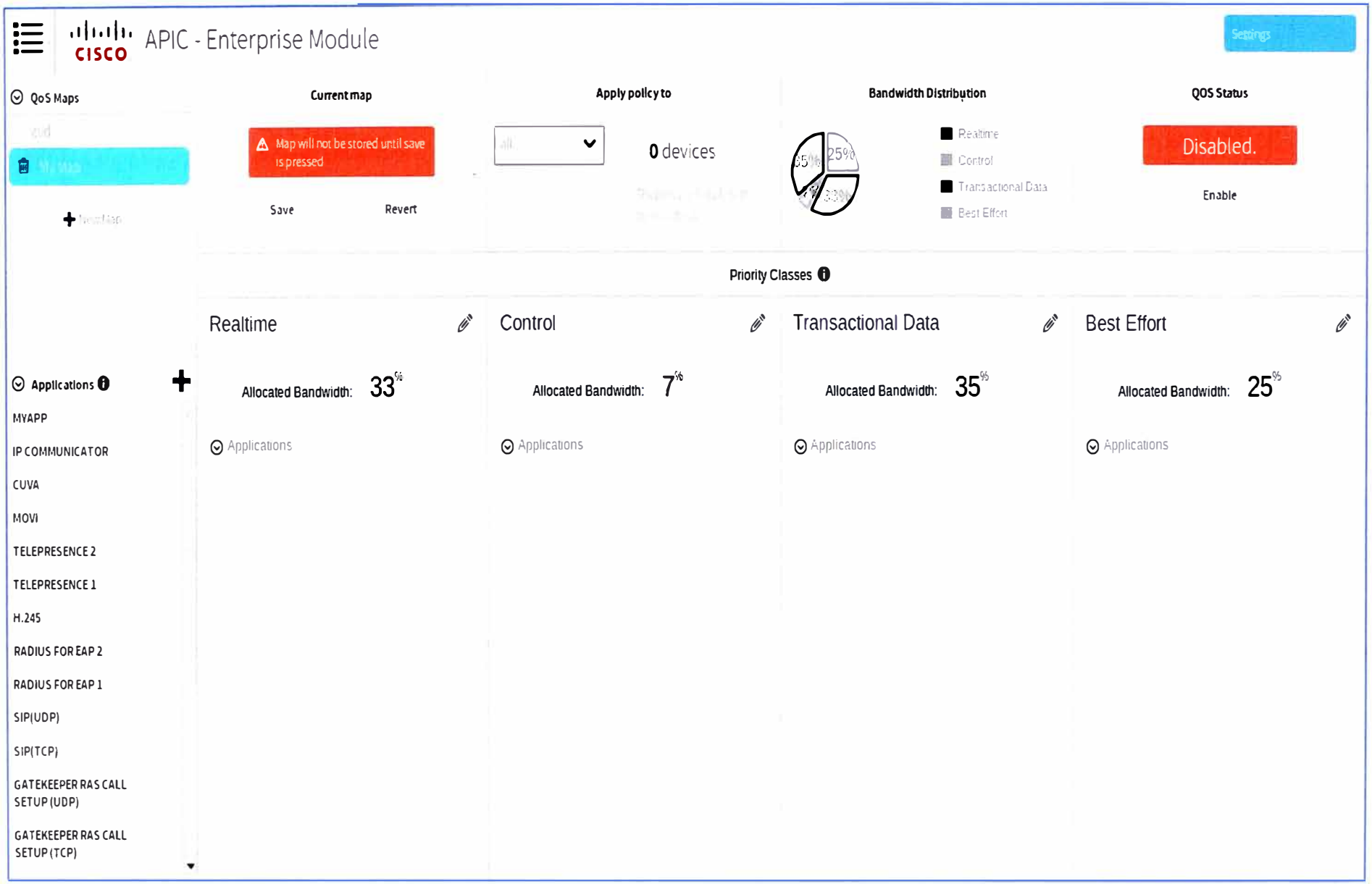


Figura A.4 MyApp se encuentra en la lista de aplicaciones del APIC-EM.(Fuente: Cisco APIC Enterprise Module).

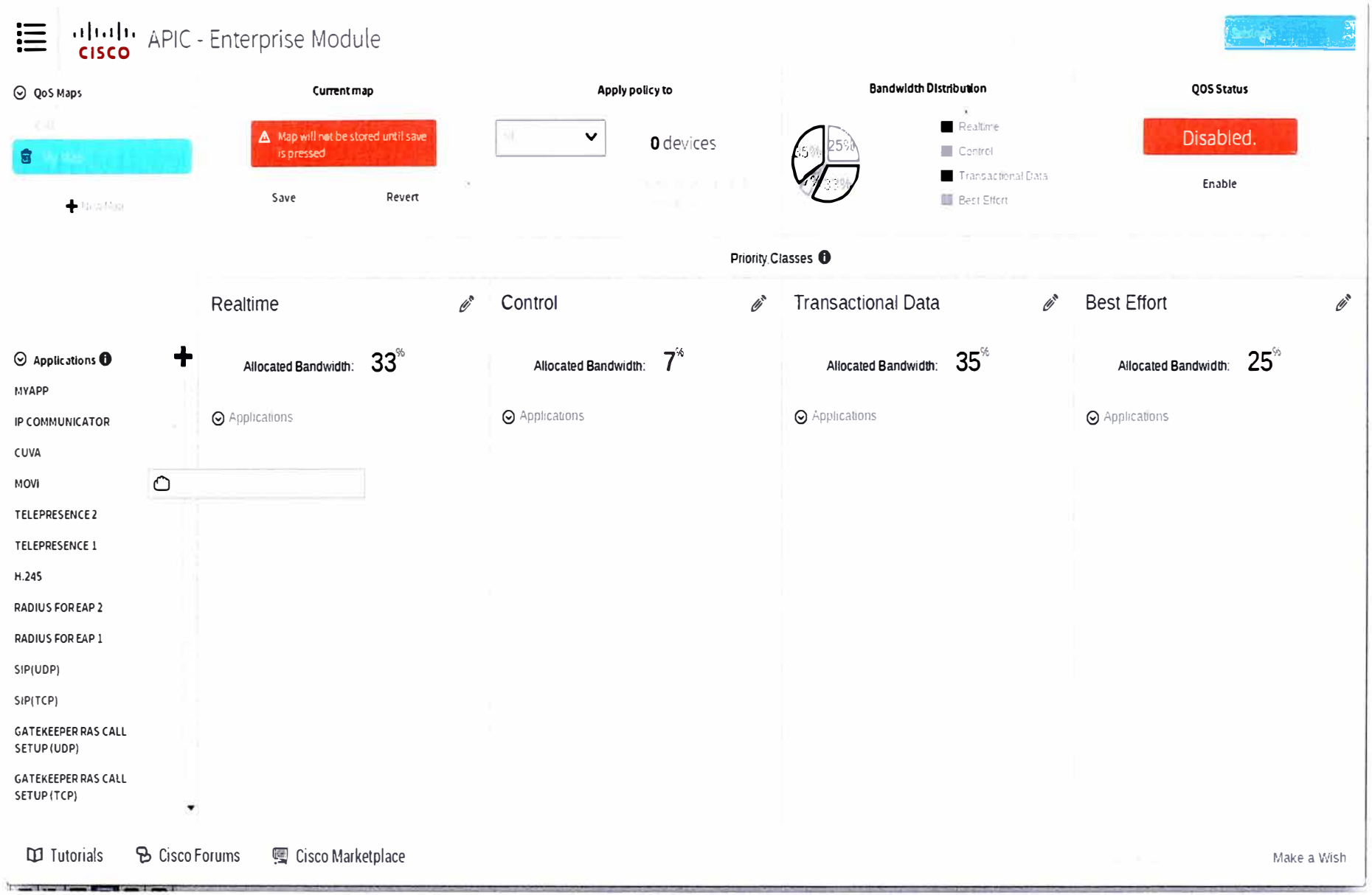


Figura A.5"Drag and Drop" de MyApp a la cola de QoS esperada.(Fuente: Cisco APIC Enterprise Module).

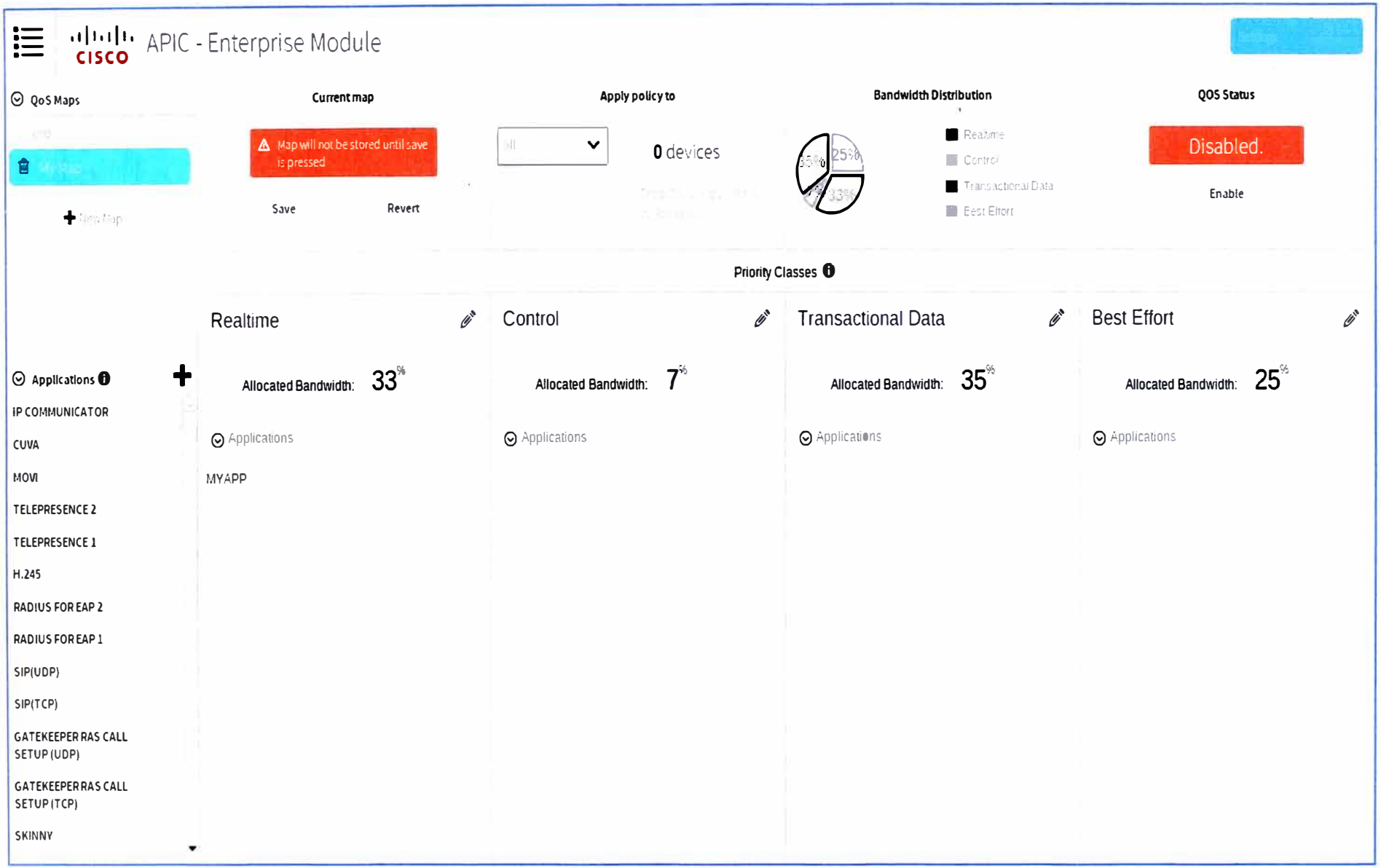


Figura A.6 Se muestra MyApp en la cola de QoS esperada. Luego se habilita.(Fuente: Cisco APIC Enterprise Module).

BIBLIOGRAFÍA

[1] RFC 3272 D. Awduche - "Overview and Principles of Internet Traffic Engineering". http://tools.ietf.org/html/rfc3272

[2] D' Nadeau, Thomas. "SDN – Software Defined Networks", O'Reilly Media, 2013.

[3] Cisco IOS Command Hierarchy – Cisco TAC Training.

[4] Open Network Foundation, "SDN Architecture Overview- V1.0", Diciembre-2013 http://goo.gl/i7svts

[5] Nick McKeown, et. al. "OpenFlow White Paper: Enabling Innovation in Campus Networks" http://archive.openflow.org/documents/openflow-wp-latest.pdf, 2008

[6] Cisco Systems, "Cisco onePK Developer Program-Technical Overview", https://developer.cisco.com/site/networking/one/onepk/discover/overview/

[7] Cisco Systems, Cisco onePK Developer Program- API Reference"http://goo.gl/ywpRhy

[8] Cisco, "Design Guides: Medianet Campus QoS Design 4.0", http://goo.gl/VOmK4F

[9] Cisco Systems, "Enterprise QoS Solution Reference Network Design Guide- Quality of Service Design Overview Cap.", http://goo.gl/PrF8Vf

[10] Cisco Systems, "Enterprise Medianet Quality of Service Design 4.0—Overview", http://goo.gl/dBNnUO

[11] ITU-T, X.701 : "Information technology - Open Systems Interconnection - Systems management overview" http://www.itu.int/rec/T-REC-X.701-199708-I

[12] IETF RFC 4949 "Internet Security Glossary, Version 2" R. Shirey http://tools.ietf.org/html/rfc4949

[13] Cisco, "Data Sheet: Cisco Application Policy Infrastructure Controller Enterprise Module" (Cisco APIC). http://goo.gl/ynmYVJ

[14] Cisco, Guía de configuración Qos del 2960X: "Catalyst 2960-X Switch QoS Configuration Guide, Cisco IOS Release 15.0(2)EX", http://goo.gl/TrrWpQ

[15] Cisco, Guía de configuración Qos del 3750-E: "Catalyst 3750 Switch Software Configuration Guide, Cisco IOS Release 15.0(1)SE", http://goo.gl/un8cj1

[16] Cisco, Guía de configuración Qos del 2901: "QoS: AutoQoS Configuration Guide, Cisco IOS Release 15M&T", http://goo.gl/RKNiX9