ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

INSTITUTO DE POSGRADO Y EDUCACIÓN CONTINUA

MAESTRÍA EN INTERCONECTIVIDAD DE REDES

"EVALUACIÓN DEL PROTOCOLO 802.1Q EN LA IMPLEMENTACIÓN DE VLANS EN ENTORNOS WIRELESS MEDIANTE LA APLICACIÓN DE SOFTWARE LIBRE"

Proyecto de investigación, presentado ante el Instituto de Postgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado académico de:

MAGISTER EN INTERCONECTIVIDAD DE REDES

AUTOR: JUAN CARLOS YUNGÁN CAZAR

TUTOR: ING. JOSÉ JAVIER HARO MENDOZA

Riobamba – Ecuador

2016

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
INSTITUTO DE POSGRADO Y EDUCACIÓN CONTINUA

El Tribunal de Trabajo de Titulación certifica que:

El Proyecto de Investigación titulado: **"EVALUACIÓN DEL PROTOCOLO 802.1Q EN LA IMPLEMENTACIÓN DE VLANS EN ENTORNOS WIRELESS MEDIANTE LA APLICACIÓN DE SOFTWARE LIBRE"**, de responsabilidad del ingeniero Juan Carlos Yungán Cazar ha sido prolijamente revisado y se autoriza su presentación.

Tribunal

Ing. Verónica Mora, Ms.C.	_____
PRESIDENTA DEL TRIBUNAL	**FIRMA**
Ing. José Javier Haro Mendoza, Ms.C.	_____
DIRECTOR	**FIRMA**
Ing. Edwin Altamirano Santillán, Ms.C.	_____
MIEMBRO	**FIRMA**
Ing. Wladimir Castro Salazar, Ms.C.	_____
MIEMBRO	**FIRMA**
DOCUMENTALISTA SISBIB-ESPOCH	_____
	FIRMA

Riobamba, 2016.

Yo, Juan Carlos Yungán Cazar, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el presente Proyecto de Investigación y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo

_____

JUAN CARLOS YUNGÁN CAZAR

DECLARACIÓN DE AUTENTICIDAD

Yo, Juan Carlos Yungán Cazar, declaro que el presente Proyecto de Investigación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

Riobamba, abril de 2016

_____

JUAN CARLOS YUNGÁN CAZAR

0602922361

DEDICATORIA

Con todo amor, dedico este trabajo a:

Gonzalo y Anita, mis padres, mis mejores amigos, mi razón de ser.

María de Lourdes por haber compartido juntos los más duros momentos.

Mi querido Nicolás (+), que con su ternura y fidelidad lleno de felicidad mis días lejos de casa.

AGRADECIMIENTO

A Dios y a mis padres lo más importante en mi vida…

A la Escuela Superior Politécnica de Chimborazo. Al Instituto de Posgrado y Educación Continua. Al Ing. Javier Haro, al Ing. Edwin Altamirano, al Ing. Wladimir Castro, miembros tutores del presente Trabajo de Investigación. Al Ing. Javier Silva Castañeda y su familia. A la Ing. María de Lourdes López Jaramillo. A todos quienes contribuyeron para la realización de este trabajo.

ÍNDICE DE ABREVIATURAS

AJAX	Asynchronous JavaScript And XML
AP	Access Point o punto de acceso inalámbrico
AVB	Audio Video Bridging
AVLAN	Authenticate Virtual Local Area Networks
BATMAN	Better Approach to Mobile Adhoc Networking
BPDU	Bridge Protocol Data Units
CFI	Canonical Format Identifier - Identificador de formato Canónico
CPU	Central Process Unit - Unidad central de procesamiento
DCB	Data Center Bridging
DDNS	Dinamic Domain Name System
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DSL	Digital Subscriber Line o línea de abonado digital.
EAP	Extensible Authentication Protocol
ESP	Ethernet Switched Path
FCS	Frame Check Sequence
FDB	Filtering Database
GNU	GNU's Not Unix
GPL	General Public License
HSP	Host Signal Processing
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
ISL	Inter-Switch Link Protocol
ISS	Internal Sublayer Service (IEEE 802.1AC)
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPX	Internetwork Packet Exchange
JFFS	Journalling Flash File System
JFFS2	Journalling Flash File System version 2
LAN	Local Area Network
LLC	Link Local Control (ISO/IEC IEEE 802.2)
MAC	Media Access Control (IEEE 802.3)
MAN	Metropolitan Area Network
MB	Megabyte

MHZ	Megaherz
MIB	Management Information Base
MIPS	Microprocessor without Interlocked Pipeline Stages
MMC	Multi Media Card
MPR	Multiple Registration Protocol
MS	MAC Service
MST	Multiple Spanning Tree
NAT	Network Address Translation
NTP	Network Time Protocol
NVRAM	No Volatil Random Access Memory
OID	Object Identifier
OSI	Open System Interconection
PPoE	Point to Point on Ethernet
PVID	Port VLAN (Virtual Local Area Network) Identifier
QoS	Quality of Service
RAM	Random Access Memory
RIF	Routing Information Field
RISC	Reduced Instruction Set Computing
RST	Rapid Spanning Tree
RST BPDU	Rapid Spanning Tree Bridge Protocol Data Unit
RSTP	Rapid Spanning Tree Algorithm and Protocol
SD	Secure Digital
SDN	Software Definied to Network
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SPB	Shortest Path Bridging
SPBM	Shortest Path Bridging MAC
STP	Spanning Tree Algorithm and Protocol
SSID	Service Set Identifier
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
MTU	Maximum Transmission Unit
VID	Virtual Identifier identificador virtual
VLAN	Virtual Local Area Network

VPN	Virtual Private Network
WIFI	Wireless
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WRAN	Wireless Regional Area Network

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

RESUMEN

Se aplicó el protocolo IEEE 802.1Q en la implementación de redes de área local virtuales (VLAN) en entornos inalámbricos, utilizando hardware especializado y configurado con Software Libre. A través de la evaluación del protocolo se identificó el procedimiento que aplica la Arquitectura de Puenteo a las tramas que llegan al puerto de un dispositivo que opera en capa de Enlace de Datos (Capa 2). El procedimiento aplicó dos funciones: reenviar las tramas entrantes a la misma LAN virtual o a una diferente; o descartar tramas que no cumplan con los parámetros de configuración. Un router inalámbrico al ser provisto de un Firmware de distribución libre, se convierte en un dispositivo con mayor flexibilidad y adaptabilidad en su configuración y operación. El uso de dispositivos completamente configurables en redes de datos y comunicación permitieron elevar los niveles de rendimiento y seguridad. Para comprobar la aplicación del protocolo IEEE 802.1Q, se implementó un prototipo de red inalámbrica con varias LAN Virtuales. Las pruebas de conectividad ejecutadas, permitieron probar y validar la aplicación del protocolo en entornos inalámbricos. Finalmente se presentó la propuesta como una alternativa de solución al problema de segmentación de red física en redes lógicas en entornos inalámbricos. Se recomienda aplicar el protocolo IEEE 802.1Q en la segmentación de redes físicas en entornos inalámbricos para mejorar el nivel de eficiencia de tráfico en las redes de datos.

Palabras claves:

<REDES INALAMBRICAS [WIRELESS]>, <MULTIPLES IDENTIFICADORES [SSIDS Y VLANS]>, <PROTOCOLO 802.1Q EN WIRELESS>, <SISTEMA OPERATIVO [FIRMAWARE DD-WRT]>, <SEGMENTACIÓN EN WIRELESS>, <INTERCONECTIVIDAD DE REDES>.

SUMMARY

IEEE 802.1Q protocol was applied in the implementation of virtual local area networks – VLAN in wireless environments by using specialized hardware configured with free software. The evaluation of the protocol was a useful tool to identify the procedure applied by bridging architecture towards the frames arriving to a device that operates on Data Link layer – Layer 2. The procedure performed two roles: first, to redirect the coming frames to the same LAN that can be virtual or different. Second, it rejects frames that do not adjust to the configuration parameters. Once a wireless router is provided with a freely distributable firmware, it becomes a device with greater flexibility and adaptability in its configuration and operation. The use of fully configurable devices in data networks and communication enabled to raise levels of performance and safety. In order to verify the application of the protocol IEEE 802.1Q, a prototype wireless network with multiple virtual LAN was implemented. Connectivity test conducted, made possible to check and validate the implementation of the protocol in wireless environments. Finally, the proposal was presented as an alternative solution to the problem of segmentation of physical network into logical networks in wireless environments. It is recommended to apply the IEEE 802.1Q protocol in the segmentation of physical networks in wireless environments for improving the level of traffic efficiency on data networks.

Key words:

<WIRELESS NETWORKS>, <MULTIPLES IDENTIFIERS [SSIDS AND VLANS]>, <802.1Q PROTOCOL IN WIRELESS>, < [FIRMWARE DD-WRT] OPERATIVE SYSTEM>, <SEGMENTATION IN WIRELESS>, <NETWORK INTERCONECTIVITY>

.

CAPITULO I

1. INTRODUCCIÓN

1.1 Planteamiento del problema – Antecedentes

La denominación de red inalámbrica se utiliza para definir la conexión de equipos que utilizan como medio de comunicación el espectro de ondas electromagnéticas, sin necesidad de una red de cables. Una de las principales ventajas es el costo, ya que elimina el cableado y las conexiones físicas entre equipos, sin embargo tiene una desventaja considerable ya que para este tipo de red se debe considerar una seguridades de alta prestación y robusta para evitar a los intrusos.

El estándar IEEE 802.1Q, se ha establecido como un mecanismo para brindar seguridad y rendimiento en redes de área local mediante el establecimiento de LANs virtuales que permite separar de manera lógica la conexión de las estaciones y dispositivos activos, sin embargo para su funcionamiento se requieren de switchs costosos y casi exclusivamente en entornos de red Ethernet cableada.

Existen varios entornos en los que se hace uso de redes inalámbricas de manera exclusiva, en los cuales se requieren mecanismos de separación para evitar sobrecarga de broadcasting y privacidad de uso. Siendo la especificación del protocolo 802.1Q flexible es posible utilizar su especificación en redes WLAN, de manera nativa mediante la implantación del mismo.

El uso de alternativas de código libre permite su ejecución en entornos hardware de bajo costo, con seguridad y robustez, sin requerir hardware de altas características para operar sistemas con la funcionalidad apropiada.

El presente trabajo de investigación se enfoca en la implementación del protocolo 802.1Q en entornos Wireless con el uso de herramientas de software libre y hardware de bajo costo.

1.2 Justificación

1.2.1 Justificación teórica

El desarrollo de modelos teóricos y prácticos producen el progreso de la ciencia, entonces surge la necesidad de construir procesos técnicos que permitan la creación de nuevos estándares.

El software libre permite realizar la instauración de avanzadas funcionalidades, en este caso de protocolos a nivel de gestión de redes. GNU/Linux es un sistema operativo muy versátil y dentro de sus variadas distribuciones, existen aquellos que son especializados en ejecutarse en entornos de hardware modestos de manera eficiente. Constituyéndose en Firmware dentro de ellos, existen mecanismos de instalación y configuración de dichas distribuciones en dispositivos de red inalámbricas (como Access Point y Routers).

Tradicionalmente soluciones propietarias para la construcción de infraestructura de red, sin embargo los estándares que los rigen son abiertos y con el soporte de todas estas herramientas es posible estudiar y luego implementar soluciones completas basadas exclusivamente en normas disminuyendo el costo de las mismas.

La integración de sistemas permite el crecimiento de los mecanismos de establecimiento de nuevas soluciones y modelamiento de estándares. El presente trabajo permite desarrollar un conocimiento más amplio en la especificación y funcionamiento del protocolo 802.1Q para su implementación en entornos Wireless.

A través del estudio en el que se aborda la utilización de la norma 802.1Q, la instalación y configuración de distribuciones de Linux en entornos embebidos y la operación del protocolo en Wireless en la práctica es posible implementar una solución que permita la aplicación del Protocolo 802.1Q (VLAN) en entornos Wireless.

1.2.2 Justificación práctica

Los entornos en los que se utilizan Redes Inalámbricas, normalmente son dependientes de equipos cableados para el complemento de sus configuraciones, en el caso de la implementación de VLAN, normalmente se requiere de un switch inteligente, y adicionalmente la conexión directa de los concentradores inalámbricos a los mismos.

Los problemas asociados a tener una gran cantidad de equipos conectados en el mismo medio físico y compartiendo el mismo segmento de red, son conocidos por pérdida de velocidad y el incremento de colisiones y tráfico de broadcast. El establecimiento de VLANS es un mecanismo que permite resolver estos inconvenientes de manera eficiente. Las redes Inalámbricas también presentan los mismos inconvenientes al compartir los modelos de los estándares de Ethernet dentro de su implementación.

En la actualidad muchos entornos dependen exclusivamente del funcionamiento de redes inalámbricas. La implementación de una solución hardware y software para el protocolo 802.1Q en entornos WLAN, mediante el uso de herramientas de software libre y hardware de bajo costo permite desarrollar una solución práctica completa e integrada en los mismos dispositivos inalámbricos que son parte de la infraestructura.

1.3 Objetivos

1.3.1 General

Evaluar la aplicación del Protocolo 802.1Q en la implementación de VLANS en entornos Wireless mediante la aplicación de Software Libre.

1.3.2 Específicos

- Fundamentar la operación del protocolo 802.1Q para la implementación de VLANS.
- Establecer alternativas de implementación del protocolo 802.1Q en VLANS en entornos Wireless mediante la aplicación de Software Libre.
- Implementar un prototipo para aplicación del protocolo 802.1Q en VLANS en entornos Wireless.

1.4 Hipótesis

La evaluación del protocolo 802.1Q permite la implementación de VLANS en entornos Wireless mediante la aplicación de Software Libre.

CAPITULO II

2. REVISIÓN DE LITERATURA

2.1 LAN Virtuales – VLAN

Una red de área local (LAN Local Area Network) es una red de estaciones de trabajo localizada en un área geográficamente limitada, como se muestra en la figura 1 – 2. Es común encontrarlas implementadas en edificios de empresas o corporaciones, campus, ambientes domésticos, etc. Todas las estaciones están conectadas a un dispositivo que se encarga de concentrarlas formando un solo dominio de colisión. Este hecho en adelante ha sido el relevante para poder segmentar la red física en varias redes lógicas a través de software.

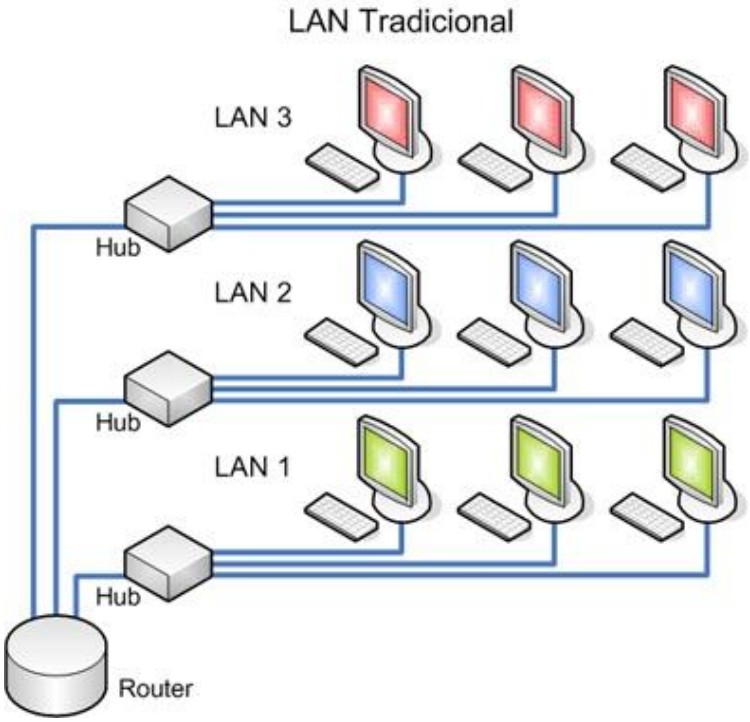


Figura 1 – 2 Red de Área Local LAN
Fuente: http://www.anexom.es/tecnologia

2.2 Importancia de segmentar las redes físicas en redes lógicas

Existen diversas razones para la segmentación de redes:
Un primer aspecto está enfocado en los niveles de organización, los administradores de red agrupan a los usuarios en redes LAN para reflejar la estructura organizacional. Una LAN podría contener a los servidores web y otras computadoras destinadas para uso público. Por ejemplo Internet, mientras que otra LAN podría contener a las computadoras que manejen información de diferentes niveles de organización (Gerencia, Dirección, Gestión, Calidad, etc.) que no deben salir del ámbito al que pertenecen.

Un segundo aspecto a considerar es el tipo de información que manejan (carga útil) ya sea esta datos, voz, video, etc. Algunas redes LAN utilizan más carga útil que otras, y en ocasiones podría ser conveniente separarlas. Por ejemplo, si los usuarios del nivel organizacional Calidad realizan toda clase de experimentos generan excesivo tráfico en la red llevándola a la saturación, tal vez a los usuarios de los demás niveles departamentales experimenten bajo rendimiento en el uso de servicios de red.

Un tercer aspecto es el tráfico de difusión (Broadcast). La difusión de tráfico cuando no conocen la ubicación de destino. Por ejemplo, cuando un usuario desea enviar un paquete a una dirección IP, cómo no sabe qué dirección MAC poner en la trama lo que hace es difundir una trama preguntando a quién le pertenece la dirección IP y esperar la respuesta. Se debe considerar que a medida que aumenta el número de computadoras en una LAN, este fenómeno también aumenta.

Cuando una interfaz de red se avería o desconfigura genera flujos interminables de tramas de difusión. Si la red no responde a un diseño bien definido, algunas de estas tramas provocarán respuestas que a su vez generarán más tráfico. El resultado de esta tormenta de difusión es que el tráfico de tramas de difusión ocupa toda la capacidad de la LAN, y las computadoras de todas las redes LAN interconectadas utilizan todos sus recursos al procesar y desechar todas las tramas difundidas.

En respuesta a la petición de los usuarios en segmentar la red física en redes lógicas con el propósito de obtener mayor flexibilidad en el tráfico de red, surge el concepto de LAN virtual o VLAN. Las redes VLAN se basan en switches especialmente diseñados para este propósito. Su funcionalidad se basa en la utilización de tablas que indican cuáles VLAN se pueden acceder a través de qué puertos. El comité IEEE 802 lo estandarizó y ahora utilizado ampliamente en muchas infraestructuras de red.

La característica de una LAN es que los dispositivos que integran la red comparten el ancho de banda del medio físico que los une. Esto es evidenciable en redes cuyo dispositivo concentrador es el hub. Cuando utilizamos un concentrador o hub en una red, se puede ver que las estaciones de trabajo conectadas a la misma toman cierta cantidad de ancho de banda, y mientras más máquinas existan en esa LAN, menor será la cantidad de ancho de banda que podrán utilizar. A este segmento de red se lo denomina "dominio de colisión". El empleo de un switch mejora el rendimiento de la red debido a que este dispositivo divide los dominios de colisión a uno por cada puerto, como se muestra en la figura 2 – 2.

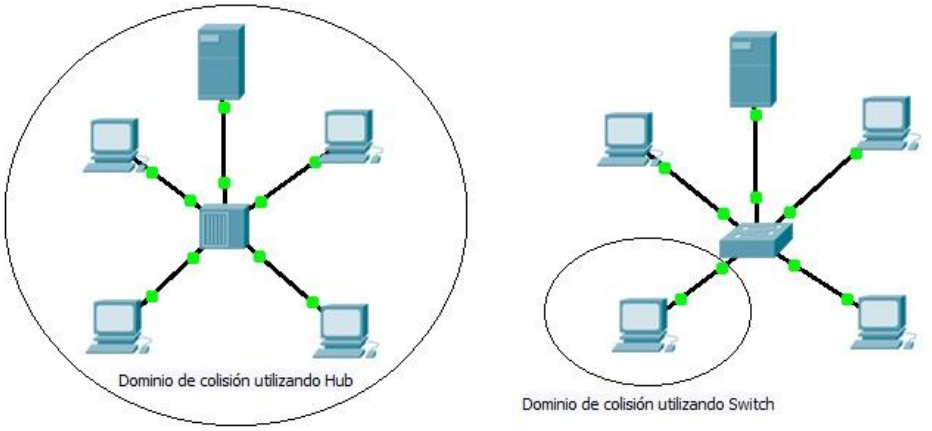


Figura 2 – 2 Dominio de Colisión
Realizado por: Yungán, J. 2016

Algo que no puede mejorar ni el switch, ni el hub o concentrador, es el envío de mensajes de difusión denominados broadcast. Estos mensajes son enviados a través de todos los puertos de un hub o de un switch cuando una estación de trabajo quiere comunicarse con otra y no sabe en dónde se encuentra, entonces envía mensajes de difusión a las demás estaciones que integran la LAN denominado "dominio de broadcast", todas las estaciones de trabajo escucharán el mensaje pero solo contestará la que se está buscando, como se muestra en la figura 3 – 2.

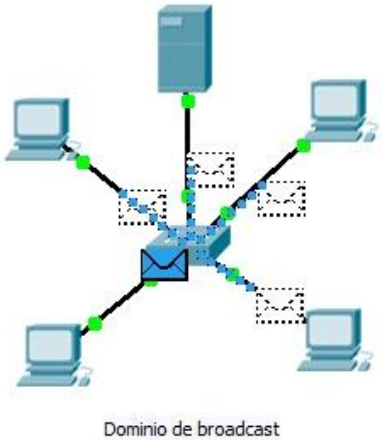


Figura 3 – 2 Dominio de Broadcast
Realizado por: Yungán , J. 2016

Los mensajes de broadcast en muchas ocasiones, son originados por: un mal diseño de red, dispositivos con configuraciones incorrectas, peticiones innecesarias realizadas a través de software o cuando tratamos de encontrar una estación en específica en la red, afectando el rendimiento.

Esta fue una de las razones más importantes por la que se dio origen a las LAN virtuales (VLANS), Las LAN Virtuales, son configuradas en los switches con el fin de dividir las LAN físicas en diferentes "dominios de broadcast", creando dominios más pequeños y aislar los efectos que causan los mensajes de broadcast afectando a la menor cantidad de estaciones de trabajo posibles.

2.3 Red de Área Local Virtual VLAN

Una LAN Virtual es un grupo de estaciones de trabajo concentradas por un Bridge o un Switch con características comunes sin importar su ubicación. Físicamente pertenecen al mismo segmento de red pero lógicamente se encuentran divididas para ser consideradas cada una de ellas como un dominio de difusión lógica, como se muestra en la figura 4 – 2.

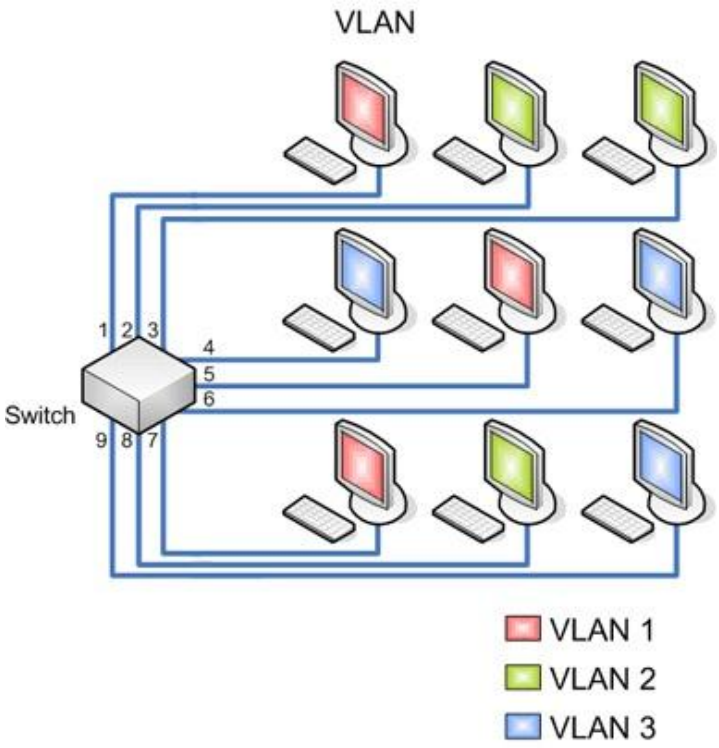


Figura 4 – 2 Segmentación de redes - LAN Virtuales
Fuente: http://redesconfiguracion.blogspot.com/

Con los switchs, el rendimiento de la red mejora en los siguientes aspectos:

- Aislar los “dominios de colisión” por cada uno de los puertos.
- Asignar ancho de banda a cada uno de los puertos.
- Aísla los “dominios de broadcast”, en lugar de uno solo, se puede configurar el VLANs para que existan más “dominios”.
- Proporciona seguridad, ya que si se quiere conectar a otro puerto del switch que no pertenece a la VLAN.
- Controla más la administración de direcciones IP. Por cada VLAN se recomienda asignar un bloque de direcciones IP, independiente
- No importa en donde se encuentre la conexión dentro del edificio de oficinas, si estamos configurados en una VLAN.

2.3.1 Tipos de LAN Virtuales

Existen dos clases de VLAN: implícitas y explícitas:

1. Las VLAN implícitas que no necesitan cambios en la trama, pues de la misma forma que reciben información la procesan, ejemplo de ello son las VLAN basadas en puertos. En esta clase de VLAN el usuario no modifica ni manipula la trama, ya que solo posee una marca y por lo tanto el sistema se vuelve propietario.
2. Las VLAN explícitas que si requieren modificaciones, adiciones y cambios a la trama, por lo que se creó el estándar IEEE 802.1Q, en donde se colocan etiquetas en la trama para manipularla.

2.3.2 Generaciones de LAN Virtuales

1. Basadas en puertos y direcciones MAC
2. Internet Working; se apoya en protocolo y dirección capa tres.
3. De aplicación y servicios: aquí se encuentran los grupos multicast y las VLAN definidas por el usuario.
4. Servicios avanzados: ya se cumple con los tres criterios antes de realizar alguna asignación a la VLAN; se puede efectuar por medio de DHCP (Dynamic Host Configuration Protocol;

Protocolo de configuración dinámica) o por AVLAN (Authenticate Virtual Local Area Networks; Redes virtuales autenticadas de área local).

- VLAN por Puerto. Este tipo es el más sencillo ya que un grupo de puertos forma una VLAN un puerto solo puede pertenecer a una VLAN.
- VLAN por MAC. Se basa en las direcciones MAC, por lo que se realiza un mapeo para que el usuario pertenezca a una determinada VLAN. Este tipo de VLAN ofrece mayores ventajas, pero es complejo porque hay que manejar las direcciones MAC.
- VLAN por Protocolo. Lo que pertenezca a IP sé enrutará a la VLAN de IP e IPX se dirigirá a la VLAN de IPX, es decir, se tendrá una VLAN por protocolo.
- VLAN por subredes de IP o IPX. Aparte de la división que ejecuta la VLAN por protocolo, existe otra subdivisión dentro de este para que el usuario aunque esté conectado a la VLAN del protocolo IP sea asignado en otra VLAN.
- VLAN definidas por el usuario. En esta política de VLAN se puede generar un patrón de bits, para cuando llegue la trama. Si los primeros cuatro bits son 1010 se irán a la VLAN de Gerencia, sin importar las características de puerto, protocolo o dirección MAC.
- VLAN Binding. Se conjugan tres parámetros o criterios para la asignación de VLAN: el puerto, el protocolo y dirección MAC, si algún parámetro no coincide, entonces se rechaza la entrada o se manda a otra VLAN.
- VLAN por DHCP. Aquí ya no es necesario proporcionar una dirección IP, sino que cuando el usuario enciende la computadora automáticamente el DHCP pregunta al servidor para que tome la dirección IP y con base en esta acción asignar al usuario a la VLAN correspondiente.

2.4 Estándares IEEE 802

IEEE 802, es un estudio de estándares elaborado por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) que actúa sobre Redes de Computadoras. Fue creado en febrero de 1980 con el fin de definir estándares para que diferentes tipos de tecnologías pudieran integrarse y trabajar juntas. En el proyecto 802 se definieron aspectos relacionados con el cableado físico y la transmisión de datos. El estándar es total y ampliamente ajustable a redes de computadoras de área local LAN y hoy en día se extiende su aplicación a redes de área metropolitana MAN. (IEEE STANDARDS ASSOCIATION, 2014), en la figura 5 – 2, se muestra la clasificación de estándares IEEE 802.

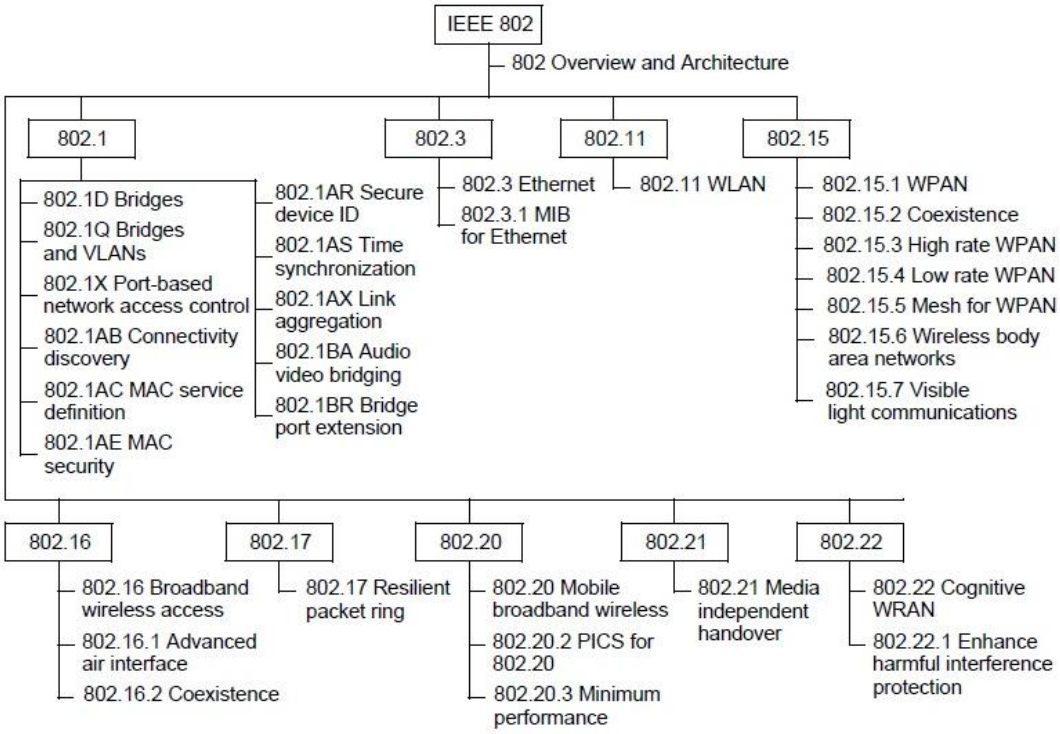


Figura 5 – 2 Estándares IEEE 802
Fuente: (IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture,2014)

El grupo de estándares IEEE 802 se encarga de:

- Describir la familia de estándares 802.
- Determinar la arquitectura LAN.
- Definir el formato de direcciones para redes LAN,
- Describir el funcionamiento del Protocolo para el Acceso a la Subred (SNAP Subnet Access Protocol)
- Regular el uso y coexistencia de los diferentes tipos de Ethernet
- Regular la gestión de entidades en una red de comunicación, a través de identificadores de objetos (OID Object Identifier) utilizado en protocolos SNMP

2.5 Estándares IEEE 802.1

Se encarga de estandarizar la gestión de red y la interconexión de redes, describe funciones para aplicar puenteo y seguridad entre redes LAN. (Tony Jeffree, 2011). Se clasifica en dos grupos de trabajo importante:

1. Estándares de puenteo (The Bridging Standards) ,

- Puenteo tradicional (Tradicional" Bridging)
- Puenteo de audio y video (AVB Audio Video Bridging)
- Puenteo de Centro de Datos (DCB Data Center Bridging)

2. Estándares de Seguridad

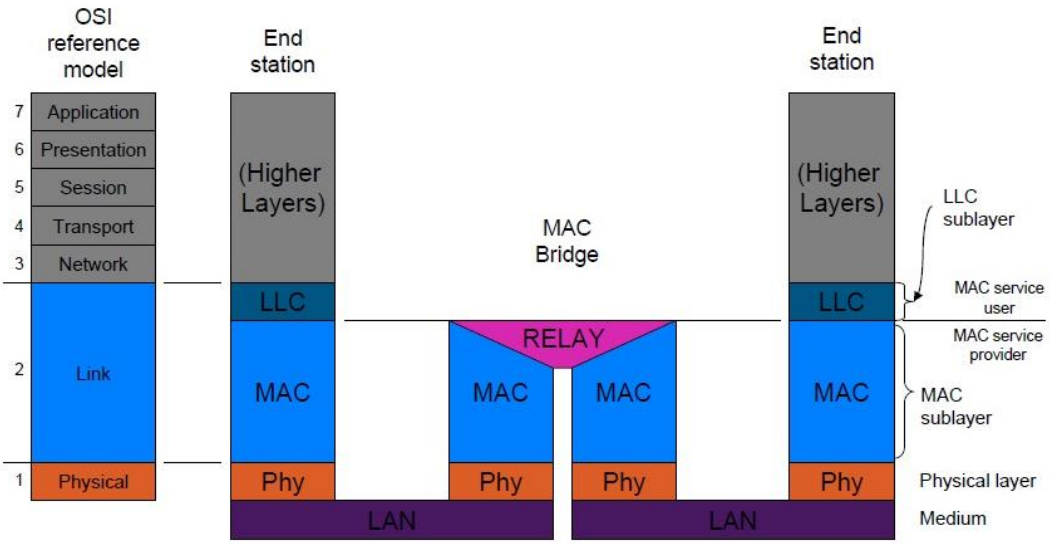


Figura 6 – 2 Ubicación dentro del Modelo OSI
Fuente: (The IEEE 802.1 Standards,2011)

En la figura 6 – 2, se describen los tecnicismos relacionados con la arquitectura y la gestión de redes. El grupo de estándares IEEE 802.1 detalla la interrelación con el Modelo de referencia OSI.

2.6 Estándares de Puenteo

2.6.1 IEEE 802.1D – Spanning Tree Protocol (STP)

Creado en el 2004, 802.1D es el estándar de IEEE para bridges MAC (puentes MAC), en el que define la técnica de reenvío de paquetes que usan los switches. Determina la aplicabilidad del protocolo Spanning Tree para impedir la formación de bucles que se forman cuando los puentes o conmutadores están interconectados a través de varias rutas. Mediante el intercambio de mensajes entre los switches interconectados, el Protocolo de Puente de Unidades de Datos (BPDU Bridge Protocol Data Units) detecta bucles y a continuación los elimina bloqueando la interfaz de

puente seleccionado, garantizando de esta manera que haya una sola ruta activa entre los dispositivos de red.

2.6.2 IEEE 802.1Q – Virtual Local Area Networks (VLAN)

Creado en el año 2005, 802.1Q es, conocido también como dot1Q, fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita segmentar una red física en varias redes lógicas, sin problemas de interferencia entre ellas. 802.1Q en realidad no encapsula la trama original sino que añade 4 bytes al encabezado Ethernet original. Todos los dispositivos de red que soportan VLAN siguen el estándar IEEE 802.1Q que especifica el funcionamiento y administración de LAN virtuales. En revisiones posteriores del estándar se decidió incluir IEEE 802.1D en IEEE 802.1Q.

Se distinguen las siguientes características de orden general:

- Admite el concepto de LAN virtual (hasta 4094 VLAN en un solo árbol de expansión (SST Single Spanning Tree) y sobre múltiples arboles de expansión hasta 64 VLAN (MST Multiple Spanning Tree);
- A través de la segmentación de redes en VLANs se implementan opciones para el equilibrio de carga;
- El apoyo a las reconfiguraciones de LAN que utilizan (RST Rapid Spanning Tree);
- Permite determinar la forma de aplicación STP a una VLAN.

2.6.3 IEEE 802.1AQ – Shortest Path Bridging (SPB)

Proyecto actualmente en desarrollo. 802.1aq, conocido como a ruta más corta de puente o SPB en las redes de computadoras es una tecnología que simplifica enormemente la creación y configuración de nubes de redes de nubes permitiendo que todos los caminos activos tengan igual costo, ofreciendo tiempos de convergencia más rápidos, mejorando la el uso de redes mesh a través del diseño y uso eficiente de ancho de banda.

2.7 Estándar IEEE 802.1Q

Para implementar el esquema de segmentación de red física en más de una red lógica, los puentes necesitan saber a qué VLAN pertenece una trama entrante y decidir su descarte o reenvío. El comité IEEE 802 se enfrentó a este problema en 1995, y después de discusiones y consensos, se decidió incorporar en la trama Ethernet nuevos campos VLAN que lograran este cometido, dando lugar al nuevo formato de trama que se publicó en el estándar IEEE 802.1Q, emitido en 1998. (IEEE STANDARDS ASSOCIATION, 2014).

La solución consistió en comprender que los nuevos campos incorporados a la trama Ethernet sólo los utilizan los puentes y los conmutadores, no las computadoras de los usuarios. Además, para utilizar VLAN, los puentes y conmutadores deben tener soporte para VLAN. Puesto que puede haber dispositivos que no tengan soporte para VLAN, el primer puente con soporte para VLAN en recibir una trama agrega campos VLAN y el último en el camino los elimina. Este hecho ayuda a que el diseño sea viable.

2.7.1 Arquitectura de puenteo

Las redes definidas por software, en inglés Software Defined Networking (SDN), son un conjunto de técnicas relacionadas con el área de redes computacionales, cuyo objetivo es facilitar la implementación e implantación de servicios de red de una manera dinámica y escalable, evitando al administrador de red gestionar dichos servicios a bajo nivel. Todo esto se consigue mediante la separación del plano de control (software) del plano de datos (hardware).

2.7.2 Plano de control

El Plano de control se encarga de la elaboración de la topología de la red lógica, en base a la información registrada en la tabla de reenvío (Conmutación de tramas – Switching) o de enrutamiento (Enrutamiento de paquetes – Routing). El plano de control decide qué hacer con las tramas o paquetes entrantes. La lógica del plano de control determina que mensajes pasan, cuáles se descartan, así como también se define el tratamiento preferencial de ciertos mensajes con la finalidad de elevar la calidad de servicio por medio de la diferenciación de servicios.

2.7.3 Plano de datos

El plano de datos**,** también llamado plano de reenvío, es la parte de la arquitectura de puenteo encargada de decidir qué hacer con los mensajes que llegan en una interfaz de entrada. El dispositivo ya sea este router o switch, busca la dirección de destino del mensaje entrante y recupera la información necesaria para determinar el camino a seguir para llegar a la interfaz de salida adecuada correspondiente al elemento receptor.

2.7.4 Descripción de la arquitectura de puenteo

El estándar IEEE 802.1, está basado en la separación del plano de datos y el plano de control, como se muestra en la figura 7 – 2. La arquitectura de puente MAC está especificada por el estándar IEEE 802.1Q, el mismo que permite segmentar la red física en diferentes redes lógicas a través de identificadores. Los protocolos de control distribuido como puenteo de camino más corto (SPB Shortest Path Bridging) están implementados en las entidades de capa superior, que luego intervienen en el control del plano de datos. Además, la norma permite la también el control por un agente externo

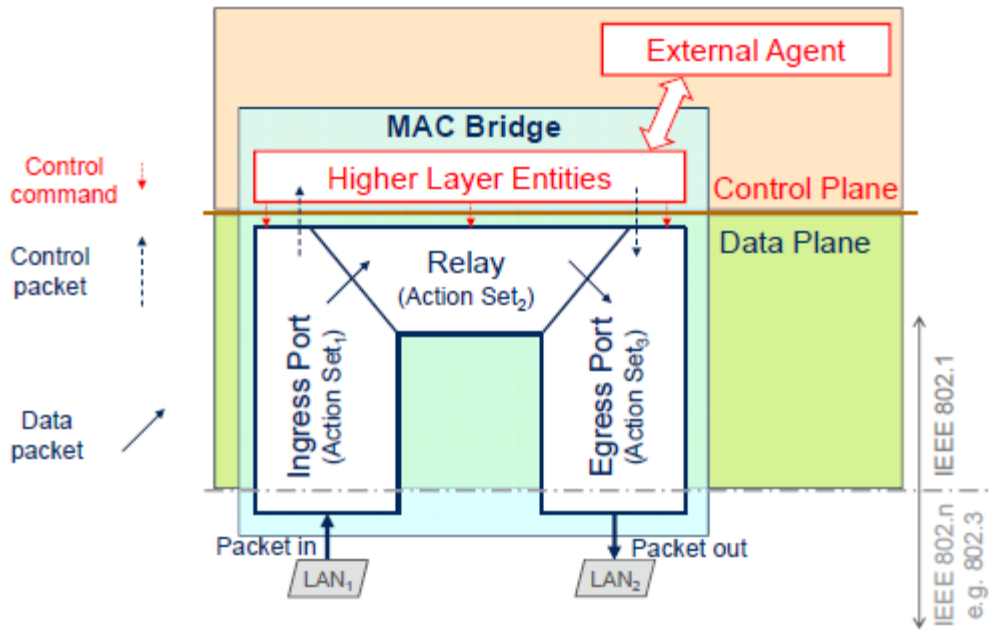


Figura 7 – 2 Arquitectura de Puente
Fuente: (IEEE 802.1Q Media Access Control Bridges and Virtual Bridged Local Area Networks, 2013)

El plano de datos de un puente en la figura muestra dos puertos y un relé entre ellos. Los mensajes son recibidos por el puerto de ingreso (Ingress Port) el mismo que puede realizar una o más acciones dependiendo en la forma que fue programado. Los mensajes son enviados a la central de procesos, es decir al relé (Relay), para finalmente conducir el mensaje al puerto de salida (Egress Port), en el que también se realizan algunas acciones programadas. Los mensajes de control que permiten la administración de la red son enviados a entidades de capa superior para su tratamiento. El agente externo o el protocolo control distribución determinan lo que ocurre exactamente a un mensaje de datos (descarte o reenvío). Las acciones se agrupan en tres conjuntos: para el puerto de ingreso, el relé y el puerto de salida. Cada conjunto de acciones proporcionan una amplia gama de funciones programables, que se discuten a continuación.

2.7.5 Puerto de Ingreso –Ingress Port

Dentro de las acciones programadas para el puerto de entrada se citan las siguientes:

- Descartar – Filtrar
- Etiquetar – Desetiquetar
- Traducción del identificador virtual VID de la red virtual LAN
- Encapsulamiento – Desencapsulamiento
- Medida

El mensaje ingresa por el puerto y se descarta si está activada la función de filtrado o si el puerto de entrada no es un miembro de la VLAN al que pertenece el mensaje. El mensaje también se puede descartar con propósitos de mitigación de bucles de encaminamiento. El puerto de entrada puede añadir una nueva etiqueta o una nueva cabecera Ethernet al mensaje o puede eliminar la etiqueta más externa o encabezado. Además, la traducción del VID también se puede realizar utilizando la tabla de traducción de VID, es decir, el VID más externo puede ser sustituido por otro VID. La acción de medición puede dar lugar a marcar o descartar los mensajes que exceden los límites de ancho de banda.

2.7.6 Reenvío – Relay

Es el responsable de reenviar el mensaje a los puertos de salida en función del identificador de VLAN y la dirección de destino transportada en el mensaje. El funcionamiento del relé se basa en tablas de reenvío, que pueden contener entradas de varios tipos. El relé también puede descartar mensajes.

2.7.7 Puerto de Salida – Egress Port

Dentro de las acciones programadas para el puerto de salida se citan las siguientes:

- Descartar (filtrar);
- Etiquetar, desetiquetar;
- Traducción VID;
- La encapsulación, desencapsulación;
- Encolamiento;
- Selección de Transmisión.

El puerto de salida también puede descartar el mensaje si está activada la función de filtrado o si el puerto no es miembro de la VLAN al que pertenece el mensaje. El puerto de salida puede quitar o añadir una etiqueta o cabecera. Traducción del VID puede ser también realiza en base a la tabla de traducción VID. El encolamiento y selección transmisión determinan cómo se enviará el mensaje.

2.7.8 Formato de trama 802.1Q

En cuanto al problema del tamaño de las tramas recordemos que una trama Ethernet tiene un tamaño de 1518 bytes, distribuidos de la siguiente forma:

1. Dirección de destino 6 bytes
2. Dirección de origen 6 bytes
3. Longitud / Tipo 2 bytes
4. Datos – relleno 46 – 1500 bytes
5. Suma de verificación 4 bytes

Al añadir dos campos más a la trama, el estándar IEEE 802.1Q tan sólo incrementó el límite a 1522 bytes distribuidos de la siguiente manera:

1. Dirección de destino 6 bytes
2. Dirección de origen 6 bytes
3. Protocolo de VLAN 2 bytes
4. Etiqueta 2 bytes
5. Longitud / Tipo 2 bytes
6. Datos – relleno 46 – 1500 bytes
7. Suma de verificación 4 bytes

Sólo los puentes y conmutadores con soporte para VLAN admiten tramas de este tamaño.

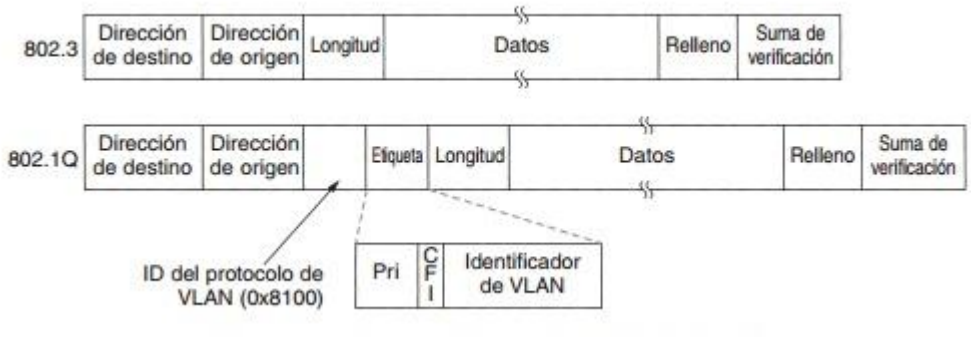


Figura 8 – 2 Formato de trama Ethernet y 802.1Q
Fuente: TANENBAUM, A.S. (2012), Redes de Computadoras, 5ta edición

El formato de trama del 802.1Q que se muestra en la figura 8 – 2, se representa la adición de dos nuevos campos de dos bytes cada uno.

El primer campo corresponde al identificador del protocolo de VLAN, que siempre tiene registrado valor 0x8100. Como este número es mayor de 1500, todas las tarjetas Ethernet lo interpretan como un tipo y no como una longitud.

El segundo campo de dos bytes contiene tres subcampos 1. Prioridad, 2. CFI- Identificador de formato canónico y 3. Identificados de VLAN.

Identificador de VLAN, es el campo principal. Ocupa los 12 bits y es el punto central puesto que representa al identificador de VLAN a la que pertenece la trama, es decir que, el identificador

asumiría valores entre uno que resulta de elevar la base dos al exponente cero (2 ^ 0) y 4096 que resulta de elevar la base dos al exponente doce (2 ^ 12), cabe mencionar que se debe excluir el identificador de VLAN 1 debido a que este corresponde la VLAN nativa.

Prioridad, este campo de 3 bits no tiene nada que ver con las VLAN. Este campo permite distinguir el tráfico en tiempo real estricto del tráfico en tiempo real flexible y del tráfico insensible al tiempo. Es decir, a través de este campo puedo definir prioridad de tráfico con motivos de ampliar la calidad de servicio.

Identificador de Formato Canónico (CFI Canonical Format Identifier). Su propósito original era indicar el orden de los bits en las direcciones MAC (Little endian en comparación con big endian). Usado para indicar la presencia de Información de Ruteo (RIF Routing Information Field). Este campo se utiliza en redes Token Ring, y contiene información de enrutamiento que se utilizada por puentes de enrutamiento para determinar a qué ruta reenviar los datos de una red Token Ring a otra.

En resumen, la Arquitectura de Puente ofrece una amplia gama de funciones para la programabilidad de la red. Cuando una trama etiquetada llega a un switch con soporte para VLAN, éste utiliza el identificador de la VLAN como índice en una tabla para averiguar a cuáles puertos enviar la trama, o a su vez descartarla puesto que no cumple con los parámetros de configuración.

2.8 Evaluación comparativa entre IEEE 802.1Q e ISL

ISL – Inter-Switch Link Protocol o Protocolo de Enlace entre Switch. Es un protocolo propietario de Cisco. Opera en Capa de Enlace de Datos y encapsula la trama Ethernet con una nueva cabecera de 26 bytes, que contiene al identificador VLAN (VLAN ID), y además añade un campo de secuencia de chequeo de trama (FCS o CRC) de 4 bytes al final de la trama, como se muestra en la figura 9 – 2.

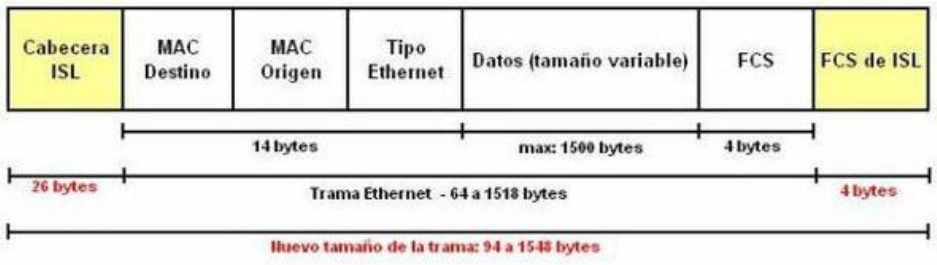


Figura 9 – 2 Formato de trama ISL
Fuente: https://es.wikibooks.org/wiki/Planificación_y_Administración_de_Redes

Tabla 1 – 2 Evaluación comparativa IEEE 802.1Q – CISCO ISL

Características	802.1Q	ISL
Propiedad	Estándar abierto IEEE	CISCO
Trama Ethernet	Inserta campo TAG (4 bytes)	Encapsula cabecera ISL (26 bytes) y FCS (4bytes)
Tamaño	68 bytes mínimo – 1522 bytes máximo	94 bytes mínimo – 1548 bytes máximo
Estado	En vigencia	Solo dispositivos CISCO
Evaluación	100 % utilizado	En desuso

Realizado por: Yungán, J. 2016

La encapsulación de tramas ISL es de 30 bytes, como se muestra en la figura 9 – 2. Si se encapsulan los paquetes de Ethernet solamente, la gama de tamaños de trama ISL es de 94 a 1548 bytes. No se requiere la fragmentación. Por lo tanto, el tamaño de trama ISL es 1548 bytes de longitud para Ethernet. La trama ISL contienen dos FCS. EL primero se calcula para los datos originales. El segundo FCS se calcula después de que el paquete ha sido encapsulado en ISL. Razón por la cual 802.1Q es el más utilizado.

2.9 Evaluación Operativa del Protocolo IEEE 802.1Q

2.9.1 Operación de puente

Cada trama está sujeta a funciones de reenvío, registro y filtrado. La trama entrante será analizada iniciando este proceso en el puerto de recepción y de ser el caso será enviada a un determinado puerto o grupo de puertos de transmisión o a su vez puede ser filtrada y descartada sin opción a ser reenviada a ningún puerto, como se muestra en la figura 10 – 2.

Los elementos principales de la operación de puente son:

a. Reenvío y filtrado de tramas
b. El mantenimiento de la información necesaria para realizar el filtrado de tramas y las decisiones de retransmisión
c. Gestión de reenvío de tramas y mantenimiento de la información de filtrado

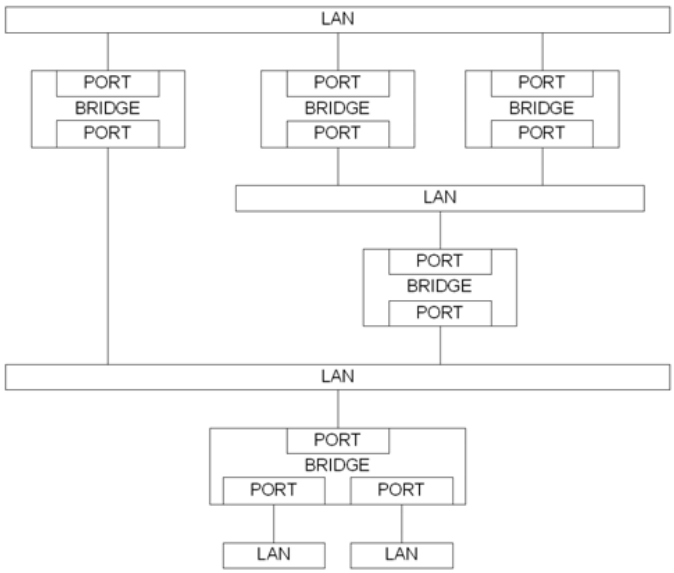


Figura 10 – 2 Topología de una red puenteada
Fuente: IEEE STANDARDS ASSOCIATION. (2014, Noviembre 03)

El modelo de operación es simple y describe la funcionalidad del puente. Los procesos y entidades que modelan el funcionamiento de un puerto de puente, como se muestra en la figura 11 – 2, incluyen los siguientes componentes:

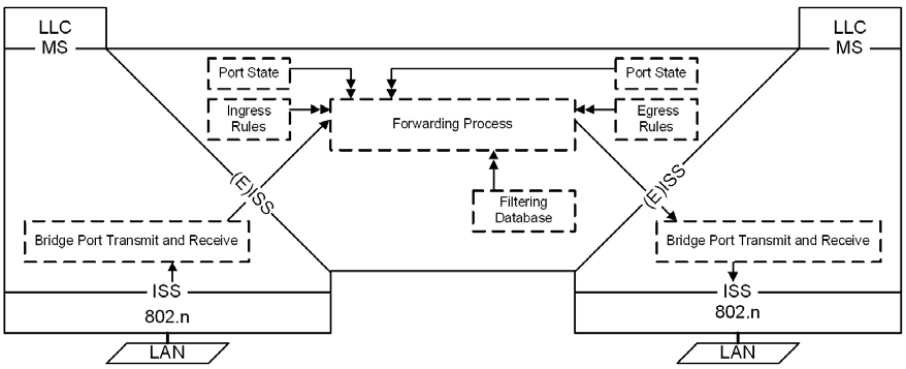


Figura 11 – 2 Componentes – Operación de Puente
Fuente: IEEE STANDARDS ASSOCIATION. (2014, Noviembre 03)

Componentes

Un puerto puente de transmisión y recepción que:

1. Recibe y transmite tramas desde y hacia la LAN conectada;
2. Filtra tramas recibidas con etiqueta de VLAN, sin etiqueta de VLAN o un VID nulo;
3. Clasifica tramas recibidas en las VLAN, asignando a cada una un VID;
4. Determina el formato de tramas etiquetadas, desetiquetadas;
5. Entrega y acepta tramas hacia y desde las entidades reenvío MAC.

La entidad LLC y entidades de Capa Superior como:

1. Spanning Tree Protocol;
2. Multiple Registration Protocol (MRP);
3. Administración de Puente.

El proceso de reenvío:

1. Interpretar topologías activas libres de bucles;
2. Filtrar las tramas que utilizan su VID y las direcciones MAC de destino;
3. Opcionalmente, clasificar y medir las tramas recibidas relacionadas con otros puertos puente;
4. Reenviar tramas recibidas que son transmitidas a otros puertos puente.

El proceso de aprendizaje:

1. Observar las direcciones de origen de las tramas recibidas en cada puerto, y
2. Actualiza la FDB;
3. La FDB contiene información de filtrado. El proceso de reenvío se afianza con las consultas que se pueden hacer a la FDB.

2.9.2 El proceso de reenvío

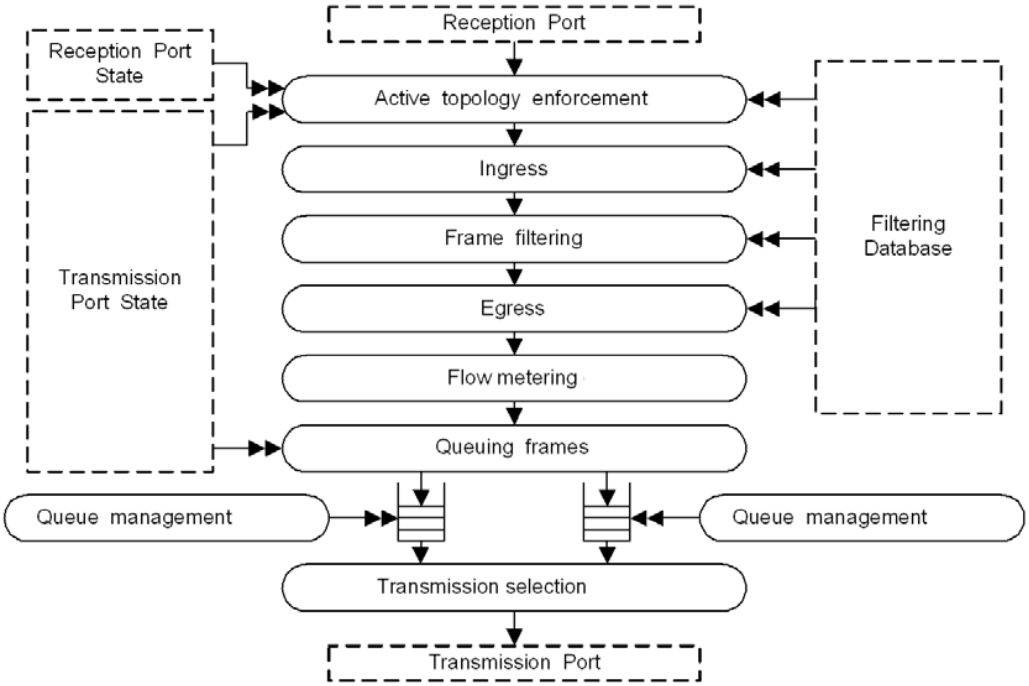


Figura 12 – 2 Proceso de reenvío
Fuente: IEEE STANDARDS ASSOCIATION. (2014, Noviembre 03)

El proceso de reenvío se muestra en la figura 12 – 2, a continuación se detallan cada una de las fases.

Aplicación de la topología activa – Active topology enforcement

Para evitar bucles de datos y el aprendizaje no deseados de direcciones MAC de origen, el proceso de reenvío determina los valores (verdadero o falso) del aprendizaje y los controles de avance correspondientes a cada trama y el puerto de puente recibidas.

Filtrado de entrada – Ingress filtering

Cada puerto puede soportar filtrado de ingreso. Una trama recibida en un puerto que no está en el conjunto de miembros asociado con VID de la trama se descarta.

Filtrado de tramas - Frame filtering

El proceso de reenvío toma decisiones de filtrado, es decir, reduce el conjunto de posibles puertos de transmisión, para cada trama recibida sobre la base de:

a) La dirección MAC de destino;
b) VID;
c) Flujo hash;
d) La información contenida en el FBD para esa dirección MAC y VID;
e) El comportamiento de filtrado de grupo por defecto para la transmisión potencial del puerto.

Filtrado de salida – Egress filtering

Cualquier puerto que no es miembro del conjunto de puertos que reciben tramas con VID asociado es removido del conjunto de puertos de egreso. Esta función no es aplicable a dispositivos que no soportan VLANs.

Clasificación del flujo y medición – Flow classification and metering

El proceso de reenvío puede aplicar la clasificación del flujo y la medición de tramas que se reciben en un puerto puente y que tienen uno o más puertos de transmisión posibles. La clasificación de flujo identifica un subconjunto de tráfico (tramas) que puede estar sujeto al mismo tratamiento en cuanto a la medición y expedición. Las reglas de clasificación de flujo pueden estar basadas en:

a) La dirección MAC de destino;
b) La dirección MAC de origen;
c) VID;
d) Prioridad.

Cola de tramas – Queuing frames

El proceso de reenvío crea una cola en la que cada trama recibida aguarda temporalmente a su turno para su transmisión potencial por un puerto determinado.

Gestión de colas – Queue management

Una trama que se encuentre en la cola para la transmisión debe ser retirada. No se debe hacer otro intento para transmitir la trama en ese puerto. La trama no debe exceder el tiempo en cola de tramas (1.0 s valor recomendado – 4.0 s valor máximo). Las tramas que entran en la cola posterior a la transición fuera del estado Forwarding no se descartan.

Selección de transmisión – Transmission selection

Para cada puerto, las tramas se seleccionan para la transmisión sobre la base de las clases de tráfico que el puerto soporta y el funcionamiento de los algoritmos de selección de transmisión soportados por las colas correspondientes en ese puerto. Las tramas se seleccionan de la cola correspondiente para la transmisión si y sólo si:

a) El funcionamiento del algoritmo de selección de transmisión soportado por esa cola determina que hay una trama disponible para la transmisión; y
b) Para cada cola correspondiente a un valor numéricamente mayor de clase de tráfico soportada por el puerto, el funcionamiento del algoritmo de selección de transmisión soportado por esa cola determina que no hay una trama disponible para la transmisión.

2.9.3 El proceso de aprendizaje

En el proceso de aprendizaje, se reciben las direcciones MAC de origen e identificadores de VLAN VID, sujetas a la aplicación activa topología y la aplicación de filtrado de ingreso. El proceso de aprendizaje no se aplica para las tramas cuyos VID es un ESP-VID o identifica una VLAN con el apoyo de SPBM.

Criterio de filtrado

El valor predeterminado para que un puente VLAN sea miembro del conjunto de puertos es el identificador de VLAN (VID). Si el valor de VID está vacío, quiere decir que no está activo, entonces todas las tramas serán filtradas independientemente de su dirección destino. El criterio de filtrado por defecto siempre se lo hará a través de Puentes MAC.

Criterio mejorado de filtrado

Para un puente VLAN, el criterio mejorado de filtrado no solo se enfoca al VID, incrementa una etapa de filtrado por identificador FID en el que incluyen al puerto o puertos miembro con su estado ya sea de aprendizaje o de reenvío.

Envejecimiento de filtrado de entrada dinámica

Las entradas de filtrado dinámico serán removidas automáticamente después de un tiempo especificado (tiempo de envejecimiento), que es el transcurrido desde que se registra una entrada o desde la última actualización para el proceso de aprendizaje. Se aplica al momento de registrar cambios en la topología.

2.9.4 La base de datos de filtrado (FDB)

La FDB admite consultas para el proceso de reenvío. En este proceso se determina si las tramas recibidas, con valores dados de, dirección MAC de destino, componentes de puente de VLAN, VID, se transmitirán a través de un puerto potencial dado.

Filtrado de entrada estática

Un filtrado de entrada estática especifica:

a) Una dirección MAC especifica;
b) Un VID especifico;
c) Un Mapa del puerto, que contiene un elemento de control para cada puerto saliente, que asocia la trama con una dirección MAC de destino.

Registro de entrada de VLAN estática

Una VLAN estática registra específicamente:

a) El VID al que se aplica la información de filtración estática;
b) A Mapa del puerto, que consta de un elemento de control para cada puerto de salida.

Filtrado de entrada dinámica

El filtrado de entrada dinámico especifica:

a) Una dirección MAC individual;
b) El FID, un identificador asignado por el puente MAC para identificar un conjunto de VID;
c) Un Mapa del puerto de reenvío para especificar la dirección MAC de destino y la FID a un solo puerto.

Registro de entradas de direcciones MAC

Un registro de entrada de direcciones MAC especifica lo siguiente:

a) Una dirección MAC específica;
b) El VID para el que se ha registrado la información de filtrado dinámico;
c) Un Mapa del puerto, que consiste en un elemento de control para cada puerto de salida, que especifica el reenvío (registrado) o filtrado (no registrado) de las tramas destinadas a la dirección MAC y, en el caso de los componentes del puente de VLAN, el VID.

Registro de entradas de VLAN dinámica

Una VLAN dinámica registra específicamente:

a) El VID al que se aplica la información de filtrado dinámico;
b) Un mapa de puerto con un elemento de control para cada puerto de salida que especifica si el VID se ha registrado en ese puerto.

Registro de grupos de direcciones por defecto

El reenvío y filtrado de tramas de grupos de direcciones se lo hace mediante la especificación de los valores predeterminados para cada VID y el puerto de salida.

a) Reenviar todos los grupos. La trama se envía, a menos que una entrada de filtrado estático explícita especifica filtrado independiente de la información de filtrado dinámico.
b) Reenviar Grupos no registrados;
c) Filtrar grupos no registrados.

2.9.5 Parámetros que evalúan la operación del protocolo IEEE 802.1Q

El protocolo IEEE 802.1Q, tiene como objetivo principal "Segmentar la red física en varias redes lógicas a través de la inserción de etiquetas en la trama Ethernet". El principio de funcionamiento del protocolo está fundamentado en tres operaciones 1. Reenvío, 2.Registro y 3. Filtrado de tramas que entran por un puerto llamado puente.

Para el proceso de consulta a la Base de datos de Filtrado FDB se implementan algoritmos que permitan trabajar con: direcciones o grupos de direcciones MAC, identificadores de VLAN etiquetas; dispuestos en entradas estáticas o dinámicas.

A continuación se describen los algoritmos que permiten consultar la Base de Datos de Filtrado:

Combinación de filtrado estático o dinámico para una dirección MAC individual.

Tabla 2 – 2 Filtrado estático o dinámico para una dirección MAC individual

Información de filtrado	Filtrado estático Elementos de control: Dirección MAC, FID, Puerto específico envío.		Filtrado dinámico Elementos de control: Dirección MAC, FID, Puerto de salida específico.		
	"Enviar"	"Filtrar"	"Enviar"	"Filtrar"	Entrada no dinámica
Resultado	Enviar	Filtrar	Enviar	Filtrar	Enviar

Realizado por: Yungán, J. 2016

Descripción del algoritmo

- **Si** cualquiera entrada estática especifica "REENVIAR" **entonces** se REENVÍA
- **Caso contrario, Si** cualquiera entrada estática especifica "FILTRAR" **entonces** se FILTRA
- **Caso contrario, Si** una entrada dinámica especifica "FILTRAR" **entonces** se FILTRA
- **Caso contrario,** se REENVÍA

Diagrama de flujo base:

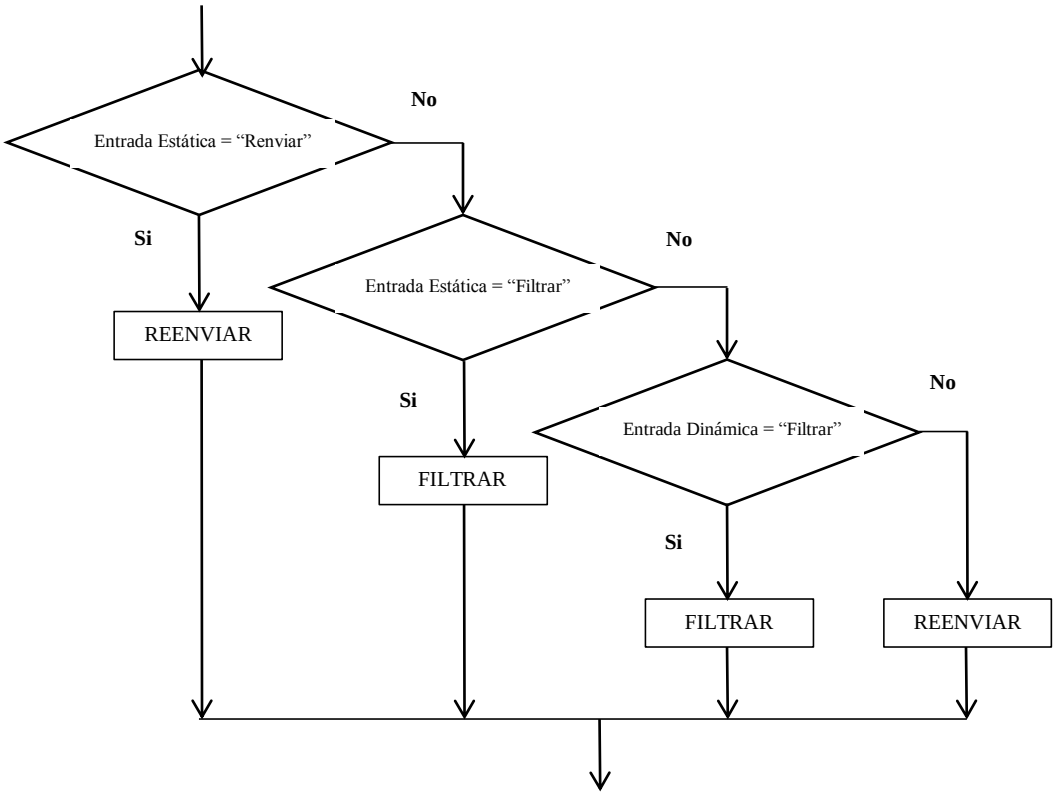


Figura 13 – 2 Filtrado estático o dinámico para una dirección MAC individual
Realizado por: Yungán, J. 2016

Filtrado estático para entrada de una dirección MAC, entrada de un Grupo de direcciones y entrada de Grupo de direcciones no registradas.

Tabla 3 – 2 Filtrado estático o dinámico y registro

Información de filtrado	Registro fijado "Enviar"	Registro prohibido "Filtrar"	Información de registro de direcciones MAC, O no Filtrado estático. Elementos de control: direcciones MAC, Grupo de direcciones, VID, puerto específico de salida.		
			Registro "Enviar"	Registro "Filtrar"	No registro de entradas MAC
Resultado	Registrar	No Registrar	Registrar	No Registrar	No Registrar

Realizado por: Yungán, J. 2016

Descripción del algoritmo:

- **Si** una entrada estática para "Todas las direcciones de grupo" y VID de la trama especifica "REENVIAR" (Registro Fijo), **entonces** "Todas las direcciones de grupo" se REGISTRAN.
- **Caso contrario, Si** una entrada estática para "Todas las direcciones de grupo" y VID de la trama especifica "FILTRAR" (Registro prohibido), **entonces** " Todas las direcciones de grupo" NO se REGISTRAN.
- **Caso contrario, Si** una entrada dinámica para "Todas las direcciones de grupo" de y VID de la trama especifica "REENVIAR" (registrado), **entonces** " Todas las direcciones de grupo" se REGISTRAN
- **Caso contrario,** "Todas las direcciones de grupo" NO ESTÁN REGISTRADAS

Diagrama de flujo base:

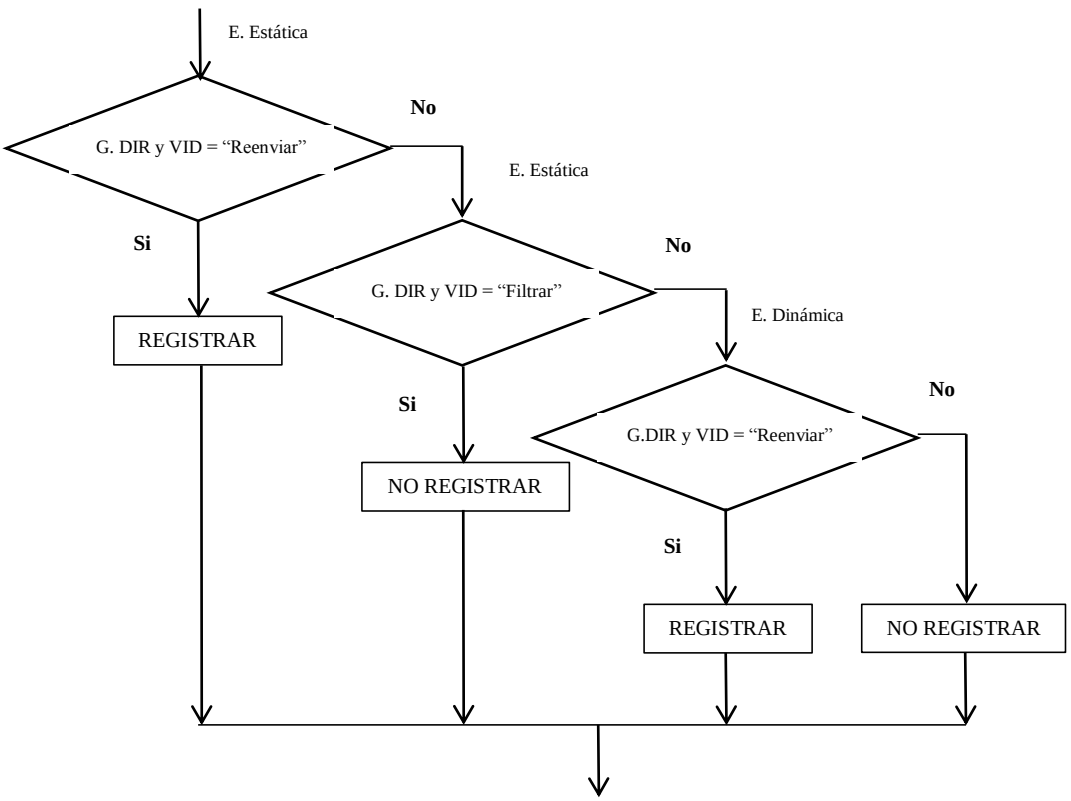


Figura 14 – 2 Filtrado estático o dinámico y registro
Realizado por: Yungán, J. 2016

Reenvío y filtrado de un grupo específico de direcciones MAC

Tabla 4 – 2 Reenvío y filtrado de un grupo específico de direcciones MAC

				Registro fijado enviar	**Registro prohibido filtrar**	**Elementos de control: Direcciones MAC, grupo de direcciones MAC, VID y puerto específico.**		
						Registrado enviar	**No registrado filtrar**	**Entradas de direcciones MAC**
Todos los grupos de direcciones controlados por VID y puerto específico	**No registrado**	**Todos los grupos de direcciones no registrado controlados por VID y puerto**	**No registrado**	Enviar	Filtrar	Enviar	Enviar "Grupo de direcciones no registradas"	Enviar "Grupo de direcciones no registradas"
			Registrado	Enviar	Filtrar	Enviar	Enviar "Grupo de direcciones no registradas"	Enviar "Grupo de direcciones no registradas"
	Registrado			Enviar	Filtrar	Enviar "Grupo de direcciones"	Enviar "Grupo de direcciones"	Enviar "Grupo de direcciones"

Realizado por: Yungán, J. 2016

Descripción del algoritmo:

- **Si** una entrada estática para una dirección de grupo específico y VID de la trama especifica "REENVIAR" **entonces** se REENVÍA.
- **Caso contrario, Si** una entrada estática para una dirección de grupo específico y VID la trama especifica "FILTRAR" **entonces** se FILTRA
- **Caso contrario, Si** una entrada estática para una dirección de grupo específico y VID comodín especifica "REENVIAR" **entonces** se REENVÍA.
- **Caso contrario, Si** una entrada estática para una dirección de grupo específico y VID comodín especifica "FILTRAR" **entonces** se FILTRA.
- **Caso contrario, Si** el resultado del algoritmo anterior para " Todas las direcciones de grupo " se registra **entonces** se REENVÍA.
- **Caso contrario, Si** el resultado del algoritmo anterior para "Todas las direcciones de grupo no registradas" se registra **entonces** se REENVÍA.

- **Caso contrario, Si** una entrada dinámica (MAC Dirección de Registro) para un grupo de direcciones y VID de la trama específica "REENVIAR" **entonces** se REENVÍA.
- **Caso contrario,** se FILTRA.

Diagrama de flujo base:

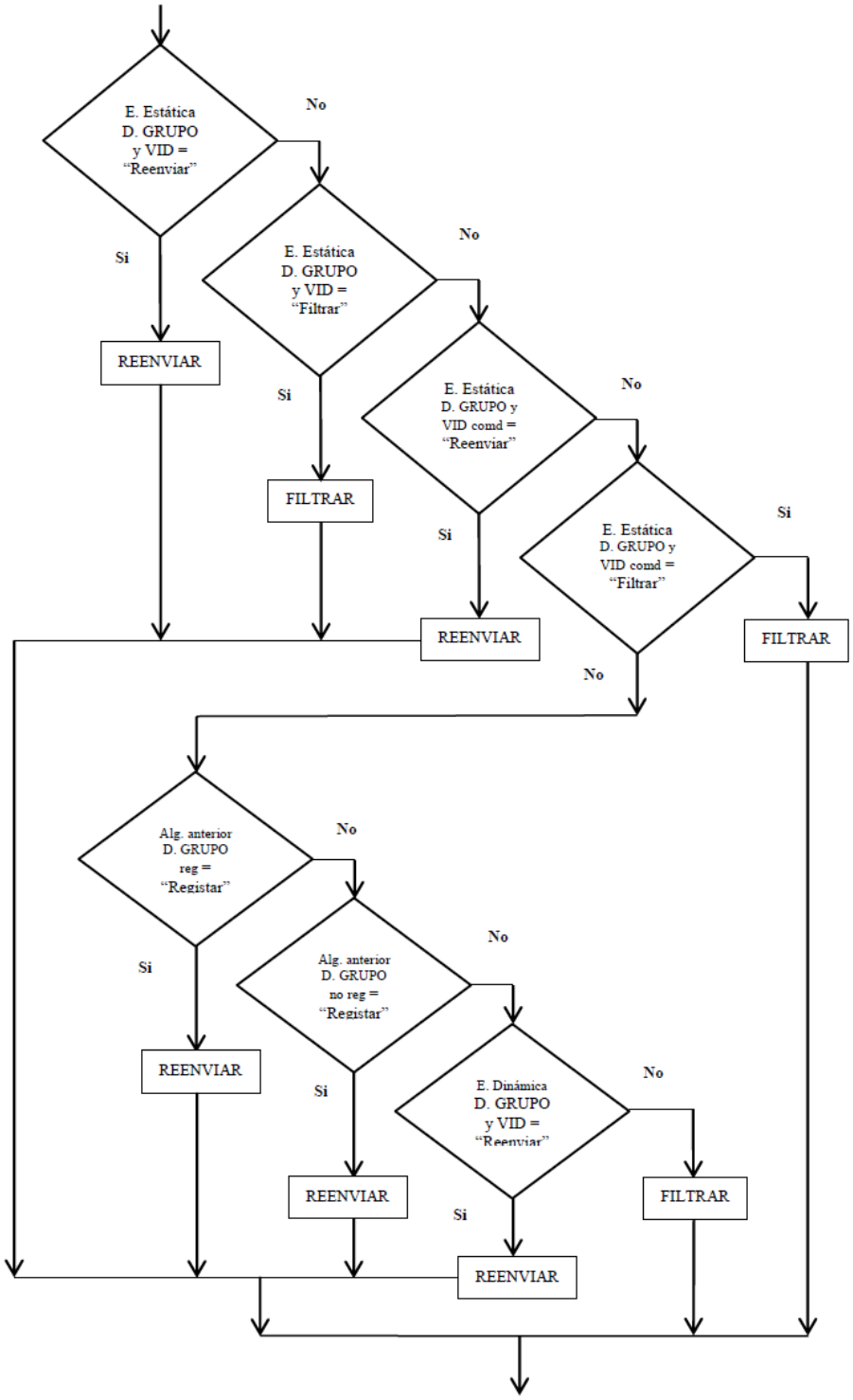


Figura 15 – 2 Reenvío y filtrado de un grupo específico de direcciones MAC
Realizado por: Yungán, J. 2016

2.10 Sistema operativo embebido – Firmware

Con el lanzamiento del código fuente de Linux para dispositivos electrónicos (dispositivos de redes de computadores, equipos de comunicación, equipos de industriales, equipos médicos, equipos de navegación, electrodomésticos, etc.), aparecieron un número de Firmwares que ofrecían extender la funcionalidad de los equipos a través del uso eficiente de sus recursos.

El Firmware no es más que un sistema operativo embebido o empotrado que está integrado en los circuitos de los dispositivos electrónicos. Estos sistemas poseen algunas características de los sistemas de tiempo real los cuales han sido desarrollados con el fin de ejecutar tareas teniendo en cuenta las restricciones de tiempo. Un sistema operativo embebido tiene limitaciones de tamaño, memoria y consumo de energía lo que los hace especiales y no suelen ser visibles.

Entonces, a menudo era difícil encontrar un Firmware con la combinación de la funcionalidad deseada. Todos los Firmwares estaban basados en el código fuente original, y estaban lejos del actual desarrollo de GNU/Linux.

2.11 Firmware OpenWrt

OpenWrt es una distribución GNU/Linux altamente extensible para dispositivos routers inalámbricos que soportan sistemas operativos embebidos. Está construido como una plataforma totalmente funcional, y es fácilmente modificable. Esto significa que se puede añadir las funciones o características que se requieran a medida que la exigencia tecnológica lo requiera. (OpenWrt, 2015)

Libre y de código abierto licenciado bajo los términos GPL. El proyecto pretende siempre estar alojado en un sitio Internet de fácil acceso, con su código fuente completo, y disponible para crear los ejecutables correspondientes. Impulsada por la Comunidad. Basado en el eslogan "Wireless Freedom" traducido como redes inalámbricas libres.

OpenWrt en lugar de iniciarse con el código fuente de Linksys, el desarrollo lo hizo desde cero. Lo que hace a OpenWrt único es empleo de un sistema de archivos con posibilidad de escritura, por lo que el Firmware ya no es sólo una compilación estática de software, sino que es posible instalar dinámicamente ajustándose a las necesidades.

Open WRT utiliza el kernel de Linux por tanto es GNU/Linux. Proporciona la capacidad de hacer lo que se necesita con un hardware barato y evitando usar software propietario e inflexible. OpenWrt es el Firmware más rápido basado en Linux para una gran cantidad de routers con Ethernet y Wireless. En este momento, la distribución contiene más de 100 paquetes de software.

2.11.1 Características

- Es un Firmware flexible de alto rendimiento ya que se pueden instalar módulos que se necesita para: administrar, configurar, calidad de servicio, seguridad, etc.
- Creación de múltiples redes inalámbricas, múltiples SSIDs y mapeo entre VLANs.
- Creación de múltiples redes lógicas utilizando el módulo 802.1Q.
- Utiliza tablas IP estándar para aplicar reglas de acceso y firewalls.
- Calidad de servicio. A través de la configuración avanzada de marcación de paquetes y reglas de etiquetado.
- Añadir módulos software para convertir al router inalámbrico en un potente servidor Web, un cliente de bitorrent o streamer.
- Cliente PPoE/Cliente DSL. resuelve las limitaciones y restricciones de los módems DSL.
- Un servidor de archivos.
- Crear o formar parte de una red Open Mesh o redes inalámbricas malladas, también conocidas como BATMAN.
- Servidores web como uhttp y nginx.
- Servidor de impresión, servidor de horario (NTP), etc.
- Al ser una distribución GNU/Linux vamos a tener acceso completo a los logs del sistema, logs del kernel, demonios que queremos que se ejecuten al inicio, etc.
- Provee un sistema de archivos completamente escribible con un gestor de paquetes opcional
- OpenWrt es una evolución de DD-WRT, que funciona en el WRT54G de Linksys.

2.11.2 Versiones de Firmware OpenWrt

El proyecto comenzó en Enero de 2004. La primera versión de estaba basada en el código fuente GPL de Linksys para WRT54G y el buildroot (Es una herramienta que simplifica y automatiza el proceso de construcción de un sistema Linux completo para un sistema integrado, utilizando compilación cruzada.) desarrollado por el proyecto uClibc (es una biblioteca C para el desarrollo de sistemas embebidos Linux. Es mucho más pequeña que la biblioteca C de GNU, pero casi

todas las aplicaciones compatibles con glibc también funcionan perfectamente con uClibc. Esta versión era conocida como una versión de OpenWrt estable y tuvo un extenso uso.

En los comienzos de 2005 se publica la primera versión experimental de OpenWrt. Las versiones experimentales usan un sistema de construcción robusto y personalizado basado en buildroot2 del proyecto uclibc. En septiembre de 2007, se empezó a utilizar el nombre de kamikaze, lo más reseñable de esta versión es el abandono de la NVRAM para poder extender el uso a la mayor parte de dispositivos, Existen dos versiones de kamikaze: la versión 7.09 de Septiembre 2007 y la versión 8.09 de Septiembre de 2008). Existe también dos versiones de backfire: la versión 10.3 de Abril 2010 y la versión 10.3.1 (Diciembre 2012). Actualmente, la última línea de desarrollo se denomina con el nombre en código de Barrier Breaker y la versión de este es 14.07 de Octubre 2014, como se registra en la tabla 5 – 2.

Tabla 5 – 2 Versiones Firmware OpenWrt

Versión	Fecha liberación
Chaos Clamer 15.05	2015, Septiembre
Barrier Breaker 14.07	2014, Octubre
Attitude Adjustment 12.09	2013, Abril
Backfire 10.03.1	2011, Diciembre
Backfire 10.03	2010, Abril
Attitude Adjustment 12.09	2013, Abril
Backfire 10.03.1	2011, Diciembre
Backfire 10.03	2010, Abril
Kamikaze 8.09.2	2010, Enero
Kamikaze 8.09.1	2009, Junio

Fuente: https://wiki.openwrt.org/es/about/history

2.11.3 Hardware necesario para implantar el Firmware OpenWrt

- Una computadora (escritorio o portátil con Sistema Operativo Windows, Linux, Mac; con navegador Web para acceder a la interfaz de administración)
- Una conexión de banda ancha a Internet (DSL, Cable, o similar)
- Un router Linksys WRT54G/GL/GS o una placa Broadcom BCM5452 compatible
- La imagen de Firmware de OpenWrt (kmod-b43)
- Documentación de soporte (wiki OpenWrt)

2.12 Firmware DD-WRT

DD-WRT es un Firmware alternativo basado OpenSource Linux adecuada para una gran variedad de routers WLAN y sistemas embebidos. El énfasis principal radica en proporcionar la más fácil el manejo sea posible mientras que al mismo tiempo el apoyo a un gran número de funcionalidades en el marco de la plataforma de hardware respectivo utilizado.

DD-WRT es un Firmware libre bajo los términos de la licencia GPL para la mayoría de router 802.11g basados en un chip Broadcom. El creador de Firmware es BrainSlayer y está alojado en sitio web.

Las primeras versiones estaban basadas en el Firmware Alchemy de Sveasoft Inc., que es una empresa desarrolladora de distribuciones de Firmware basado en kernel Linux para routers WiFi ASUS, Belkin, Buffalo Technology, Linksys y Netgear. Existen tres versiones de Firmware: Satori, Alchemia y Talisman. Aunque muchos de los paquetes de software en el Firmware están bajo la licencia GNU General Public License (GPL), incluyendo el kernel de Linux, el firmaware se ofrece bajo una suscripción anual, motivo por el cual es rechazado por la comunidad de libre.

La nueva versión de DD-WRT (v23) ofrece numerosas características que no ofrecen por defecto los dispositivos con su Firmware de fábrica e incluso más que el Firmware comercial de Sveasoft, como se registra en la tabla 6 – 2

2.12.1 Características

- 802.1x (EAP Extensible Aunthentication Protocol). Protocolo de autenticación extensible, EAP se utiliza para seleccionar un mecanismo de autenticación específico, típicamente después de que el autenticador solicita más información a fin de determinar el método.
- Restricciones de Acceso. Este modo le permite restringir el acceso sobre la base de tiempo, protocolo o destino.
- Adhoc. Permite conectarse a otros dispositivos inalámbricos que también están disponibles para las conexiones ad hoc.
- Afterburner. También conocido como SpeedBooster, SuperSpeed, TurboG, 125Mbps, HSP125, y G+ es una característica integrada en algunos routers que, teóricamente, aumentan el rendimiento mediante el uso de software o firmware.
- Modo de Aislamiento de Cliente. Limita a los clientes para comunicarse sólo con la AP y no con otros clientes inalámbricos (por lo general establecidos en puntos de acceso).

- Modo Cliente. También denominada AP modo cliente AP, permite que el router se conecte a otros puntos de acceso como cliente.
- DHCP Forwarder (udhcp). Es un agente que retransmite mensajes DHCP entre diferentes subredes Ethernet.
- Servidor DHCP (udhcp o Dnsmasq). Permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente.
- DNS Forwarder (Dnsmasq). Envía un requerimiento DNS a cualquier servidor DNS, usado por cuestiones de configuración y velocidad. Conocido como servidor recursivo DNS
- Dynamic DNS. DNS dinámico es un término genérico para un servicio que está alojado fuera de la red para proporcionar respuestas DNS válidas
- DMZ. Soporta diseño conceptual de red donde los servidores de acceso público se colocan en un segmento separando los servidores del acceso público
- Hotspot Portal. Soporte para acceso a Internet a través de una red inalámbrica y un enrutador conectado a un proveedor de servicios de Internet con servicios de autenticación
- IPv6. Soporte para direccionamiento IP versión 6.
- JFFS2. El sistema de archivos transaccional Flash (JFFS) le permite tener un sistema de permisos de escritura de archivos de Linux en un router habilitado DD-WRT. Se utiliza para almacenar programas de usuario y datos en la memoria flash.
- MMC/SD Card Support. Soporte para añadir MultiMediaCard (MMC) tarjeta de memoria flash estándar y Secure Digital (SD) que es una tarjeta de memoria flash no volátil.
- NTP. Network Time Protocol. Protocolo de Sincronización de Red ES un protocolo que permite sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable.
- Ntop Remote Statistic. Es un analizador de tráfico de red, de forma similar a lo que hace el comando top en Unix. Ntop se basa en libpcap y se ha escrito en una manera portátil para ejecutar prácticamente en todas las plataformas Unix y Win32.
- VPN Server. Soporta la creación de varias redes virtuales privadas. Una VPN es una red privada a la que nos conectamos desde cualquier ubicación. El medio utilizado para conexión entre la red VPN y el equipo es internetOpenVPN (Cliente y Servidor).
- OpenVPN usa SSL / TLS para manejar y cifrar flujo de datos. Esto hace que la solución sea muy propicia para entornos de red modernos, con conexiones NAT.
- Port Triggering. Permite dirigir el tráfico dirigido de un puerto del router a un puerto de un equipo de la red privada, esto es necesario porque los servidores esperan conexiones ‘entrantes’ y típicamente los routers sólo permiten las salientes.

- Port Fowarding. Permite la asignación o reenvío de puertos para transmitir información a través de una red. Esta técnica utiliza el protocolo TCP/IP, y se encarga de transmitir paquetes de información entre servidores externos y los servidores internos de una red particular.

2.12.2 Versiones de Firmware DD-WRT

Tabla 6 – 2 Versiones Firmware DD-WRT

Nombre de archivo	Descripción
dd-wrt.v24_<type>_asus.trx	Versión de interfaz Web para flashear.
dd-wrt.v24_<type>_generic.bin	Versión genérica para flashear a través de interfaz web en todos los dispositivos compatibles (incluyendo Linksys WRT54G / GL / GS) y para flashear Siemens SE505 con tftp arranque en 192.168.2.1.
dd-wrt.v24_<type>_wrt54g.bin	Versión tftp para WRT54G. Utiliza interfaz web. Esta versión fue específicamente hecha para los routers. (v5 / v6 note: Desde el WRT54G/GS v5-v6 usan una modificación WAP54Gv3).
dd-wrt.v24_<type>_wrt54gs.bin	Versión tftp para WRT54GS. Utiliza interfaz web. Esta versión fue específicamente hecha para los routers.
dd-wrt.v24_<type>_wrt54gsv4.bin	Versión tftp para WRT54GSv4. Utiliza interfaz web. Esta versión fue específicamente hecha para los routers.
dd-wrt.v24_<type>_wrtsl54gs.bin	Versión tftp para WRTSL54GS. Utiliza interfaz web. Esta versión fue específicamente hecha para los routers.
dd-wrt.v24_<type>_moto.trx	Solo para Motorola WR850G (construido solamente para Micro y Mini

Fuente: https://www.dd-wrt.com/wiki/index.php/What_is_DD-WRT%3F

2.12.3 Hardware necesario para implantar el Firmware DD-WRT

- Una computadora (escritorio o portátil con Sistema Operativo Windows, Linux, Mac; con navegador Web para acceder a la interfaz de administración);
- Una conexión de banda ancha a Internet (DSL, Cable, o similar);
- Un router Linksys WRT54G/GL/GS, placa Broadcom compatible;
- La imagen de Firmware de DD-WRT (dd-wrt.v24_<mini>_generic.bin);
- Documentación de soporte (wiki DD-WRT).

2.13 Otros Firmware (Velásquez, 2014)

HyperWRT. Se basa en el Firmware de Linksys y está dirigido principalmente a ofrecer una gama más amplia de funcionalidades mientras se mantiene similitudes con el Firmware original.

FreeWRT. Se trata de un tenedor de OpenWrt que surge debido a los problemas de comunicación entre la comunidad OpenWrt. Su propósito es ofrecer un Firmware que cumple con la mayoría de los requisitos de un entorno comercial. El software adicional puede ser instalado a través de ipkg.

Tomate. Es un derivado de HyperWRT con un kernel de Linux. Incluye una interfaz gráfica de usuario basada en AJAX y características tales como QoS, firewall personalizable, DDNS, etc.

ZeroShell. Es una distribución libre para servidores y dispositivos embebidos o integrados, cuyo objetivo es ofrecer los principales servicios que una LAN requiere

2.14 System on Chip Broadcom BCM5352

El chip es Broadcom BCM5352, utiliza plataforma de procesamiento RISC y permiten la instalación de diferentes distribuciones Firmwares especialmente aquellos derivados del kernel de Linux constituyéndose en equipos flexibles a la implantación de distintas soluciones.

2.14.1 Descripción física

La familia BCM 5352, como se muestra en la figura 16 – 2, integran un procesador MIPS32 de alto rendimiento, proporciona conectividad LAN inalámbrica con velocidades de datos de hasta 125 Mbps, y es compatible con el estándar IEEE 802.11 b / g. Dispone de una conexión WAN a través de su interface configurable de comunicación. Tiene una arquitectura de colas de prioridad por puerto de cuatro niveles que permiten gestionar la calidad de servicio (QoS IEEE 802.1p). Para el balanceo de carga y el uso eficiente del de ancho de banda permite aplicar, DiffServ / TOS y L2 / L3 IGMP. Adicionalmente soportan el protocolo IEEE 802.1Q VLAN el cual permite una configuración de VLAN flexible y segregación del puerto WAN. Las características se registran en la tabla 7 – 2

Figura 16 – 2 Placa BCM 5352
Fuente: https://wiki.openwrt.org/toh/Linksys/wrt54g

Tabla 7 – 2 Características placa Broadcom BCM-5352

Componente	Capacidad
Plataforma	Broadcom BCM5352
Subconjunto de instrucciones	MIPS 24Kc
CPU	200 MHz
FLASH	4 MB
RAM	16 MB
LAN	4 puertos Fastethernet
WLAN	1 puerto IEEE 802.11 b/g

Fuente: https://wiki.openwrt.org/toh/Linksys/wrt54g

2.14.2 Conexión de puertos

La placa Broadcom 5352, se compone de un Switch con seis (6) puertos en total, de los cuales cinco (5) son visibles, los cuatro (4) puertos corresponden a la LAN, un (1) puerto a la WAN, y un puerto interno para la conexión a la CPU. El CPU contiene dos (2) puertos internos, eth0 (Ethernet 0) que se conecta al puerto 5 del Switch y eth1 (Ethernet 1) que se conecta al puerto WiFi. Los puertos eth0 (CPU) y puerto 5 (Switch) son del tipo tagging (trunk), para la interconexión de las VLAN del Switch y la CPU.

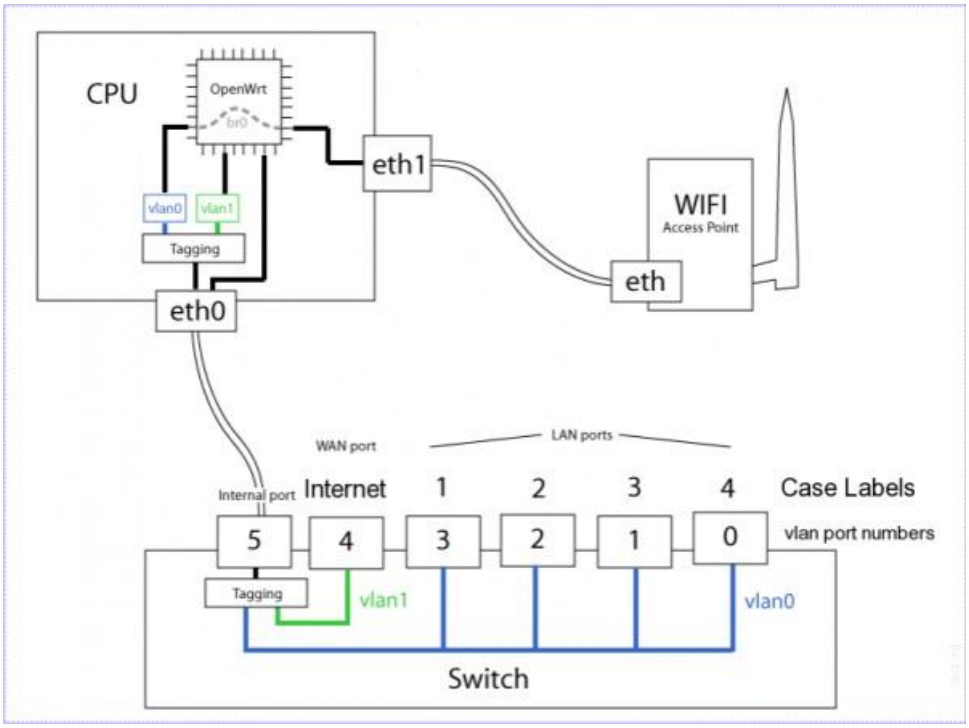


Figura 17 – 2 Conexión de puertos placa BCM-5352
Fuente: https://wiki.openwrt.org/toh/Linksys/wrt54g

2.14.3 Descripción de puertos

Inicialmente el dispositivo está configurado como Punto de Acceso (AP Access Point), como se lo muestra en la figura 17 – 2. La descripción de puertos se registra en las tablas 8 – 2 y 9 – 2.

Tabla 8 – 2 Descripción de puertos

Puerto Físico Puerto Router (CPU)	vlanXports (nvram variable)	Puerto CPU	VLAN / Puerto-Bridge	Puerto Router (CPU)
Internet (0)	4		vlan1 / no	vlan1
1 (LAN)	3		vlan0 / br0-1	
2 (LAN)	2		vlan0 / br0-1	
3 (LAN)	1		vlan0 / br0-1	
4 (LAN)	0		vlan0 / br0-1	
WIFI		eth1	vlan0 / br0-2	br0
	5	eth0	tagging (vlan0 vlan1)	

Fuente: Linksys WRT54G y DD-WRT – Guía práctica 2012

Tabla 9 – 2 Descripción de puertos

Variable	Valor	Descripción
portXVLANs (X = 0-5)	VLAN asignada a un puerto. El número de la variable corresponde al número físico (Ej. puerto 3 LAN = port3VLANs)	
	0-15	Número de VLAN (pueden ser varios a la vez)
	16	Tagging (802.1Q)
	17	auto-negociación desactivado
	18	10/100 Mbps (si auto-negociación desactivado = 10 Mbps)
	19	Full/Half Duplex (si auto-negociación desactivado = Half Duplex)
vlanXports (X = número de VLAN)	Puertos (número y tipo) asignados al número de la VLAN No corresponde a los puertos físicos, sino a la numeración interna del Switch (la relación entre puerto físico y puerto interno se muestra más adelante)	
	0-5	Número de puerto interno de Switch
	*	Identificador del primer VLAN, PVID por sus siglas en inglés
	T	Tagging (para puerto 5 opcional)
VLANs	0	VLAN adicional (por defecto VLAN 0 y 1)
	1	VLAN adicional
vlanXhwname (X = núm. de VLAN)	eth0	Puerto del CPU que conecta al puerto 5 del Switch. La CPU solamente se conecta a las VLAN del Switch a través del puerto eth0 y por tanto debe ser el mismo valor para todos las VLAN

Fuente: Linksys WRT54G y DD-WRT – Guía práctica 2012

2.14.4 Archivos de configuración NVRAM

Memoria de Acceso Aleatorio no Volátil (NVRAM Non Volatile Random Access Memory). En la NVRAM se guarda todos los valores de las variables que se usa para iniciar el router. Esto implica que un daño en el NVRAM provocaría que el dispositivo no inicie correctamente. Para la administración de la NVRAM, el Firmware DD_WRT implementa tres (3) variables configurables rc_startup, rc_firewall, y rc_shutdown. La variable rc_startup, permite ejecutar comandos de forma sucesiva durante el arranque del router. La variable rc_firewall, es donde se

implementan las reglas de seguridad. Y la variable rc_shutdown que ejecuta funciones para apagar el equipo.

El sistema de archivo del firmaware DD-WRT (JFFS Journaled Flash File System), en sus primeras versiones no permitía que los cambios de configuración sobre estas variables permanecieran luego de reiniciar el equipo. Para solucionar este problema el sistema de archivos tuvo una evolución importante a JFFS2 y desde la versión dd-wrt.v23_generic.bin, entonces, a más de guardar las configuraciones sobre las variables, permite el almacenamiento de archivos y programas personales.

El Linksys WRT54G es un router inalámbrico muy popular, permite interconectar varias computadoras mediante enlaces Ethernet 802.3 y 802.11g inalámbricas. Este router es considerado como doméstico, debido a que los desarrolladores de Linksys tuvieron que liberar el código fuente del firmware del router para cumplir con las obligaciones de la GNU GPL. Este hecho ha permitido a los desarrolladores de software modificar el firmware para añadir funcionalidades al dispositivo.

Figura 18 – 2 Router Lynksys WRT54G
Fuente: http://www.linksys.com/es/routers-inalambricos/c/routers-inalambricos-wrt/

El WRT54G original está equipado con una CPU MIPS a 125 MHz con 16 MB de memoria RAM y 4 MB de memoria flash para almacenar el firmware. Disponen de 5 puertos y con un chipset inalámbrico Broadcom. Está provisto de dos antenas externas conectadas a través de conectores de polaridad inversa TNC (Threaded Neill – Concelman).

CAPITULO III

3. MATERIALES Y MÉTODOS

3.1 Diseño de la investigación

El trabajo de tesis está descrito como una investigación cuasi-experimental. La información que se utilizó para comprobar la conectividad entre estaciones de trabajo no fue tomada al azar. Se consideró una Topología de Red Inalámbrica como ambiente de pruebas. Esta topología permitió evidenciar la segmentación de red física en varias LAN Virtuales y aporto con información para su posterior análisis.

3.2 Tipo de investigación.

El presente trabajo está definido como una Investigación Aplicada, puesto que parte de un problema que requiere ser intervenido y resuelto. La Aplicación del Protocolo 802.1Q en la implementación de LAN Virtuales en entornos Wireless mediante la Aplicación de Software Libre, consistió fundamentalmente en: La evaluación del Protocolo 802.1Q. El análisis de alternativas para implantar firmware libre con soporte de Protocolo 802.1Q en dispositivos inalámbricos que operan en Capa 2 del modelos OSI. Para comprobar la aplicación de Firmware Libre con soporte de Protocolo se implementa un prototipo de red inalámbrica con cuatro (4) LAN Virtuales. Finalmente se realiza un análisis de resultados de las pruebas de conectividad ensayadas sobre el prototipo.

3.3 Métodos

Se utilizó para este trabajo de tesis los siguientes métodos de investigación:

3.3.1 Método Científico

Se utilizó el método científico ya que fue necesario partir de conceptualizaciones y teorías probadas y verificables. A demás que este método permitió recopilar la información pertinente para definir la metodología apropiada a seguir para la implantación de LAN Virtuales.

3.3.2 Método Deductivo

A través de la deducción, fue posible responder a la problemática de implantar LAN Virtuales en entornos inalámbricos. Para esto se evaluó la Arquitectura de Puenteo planteada en el estándar IEEE 802.1Q y su aplicabilidad a las redes sin cables.

3.4 Técnicas y Fuentes de recolección de datos

3.4.1 Técnicas

Las técnicas empleadas en el presente trabajo de investigación se describen a continuación:

1. Revisión de documentación referente a:
- El problema de tener dominios de colisión extensos y sus necesidades de segmentar la red física en diferentes redes lógicas.
- La posibilidad de segmentar la red física en redes lógicas haciendo uso del concepto de LAN Virtuales.
- Fundamentar el funcionamiento de la arquitectura de puenteo. Estándar IEEE 802.1Q.
- Sistema operativo empotrado conocido como Firmware, basado en GNU/Linux que pueda ser implantado en un router inalámbrico y que integren el soporte del protocolo estudiado.
2. Implantación de Firmware. Fue necesario revisar documentación de soporte de hardware y las oportunidades de brindar compatibilidad con Firmware basados en GNU/Linux.
3. Configuración de Firmware. Haciendo uso de la documentación oficial del Firmware se definió el procedimiento a seguir para configura el Firmware con soporte del estándar IEEE 802.1Q.
4. Razonamiento. A través del razonamiento y el sentido común, se determinó con precisión el funcionamiento de las LAN Virtuales.

5. Observación. La observación de los procesos de instalación del Firmware, la configuración de LAN virtuales y funcionamiento del prototipo permitió comprobar el funcionamiento de la Arquitectura de Puenteo planteada en el estándar.
6. Pruebas. Se aplicaron pruebas para determinar el funcionamiento del prototipo. Se comprobó la conectividad entre equipos de la misma LAN Virtual y equipos de diferentes LAN Virtuales.

3.4.2 Fuentes

Las fuentes de que se utilizaron el trabajo de tesis fueron:

Fuentes Primarias:

- Investigaciones;
- Material Bibliográfico;
- Publicaciones;
- Papers;
- Revistas especializadas;
- Estándares de calidad;
- Documentos RFC.

Fuentes Secundarias:

- Textos;
- Revistas;
- Observaciones.

3.4.3 Instrumentos

Por la naturaleza del trabajo de tesis en el que se desea comprobar la implementación de LAN Virtuales, Se utilizó instrumentos de control, captura, análisis y monitorización de conexión de red, para realizar un seguimiento al tráfico. Para comprobar la conectividad se usó el comando Ping que permite enviar paquetes tanto de ida como de regreso. La información obtenida a través de la ejecución de este comando fue registrada para su posterior análisis estadístico. Los

resultados obtenidos luego del análisis permitieron validar la implementación de LAN Virtuales en entornos inalámbricos.

3.4.4 Validación de los instrumentos

La validez de los instrumentos es dependiente del nivel de medida del dominio específico de las variables que intervienen en la investigación. Es decir que para determinar la validez de los instrumentos se tomó como referencia las características de las distribuciones de Firmware para su implantación en routers inalámbricos.

Para la validación de la configuración del ambiente de pruebas planteado en el presente trabajo de investigación, se emplea un sniffer como Wireshark para así visualizar las capturas de tramas etiquetadas por el protocolo 802.1Q.

3.5 Planteamiento de la Hipótesis

3.5.1 Hipótesis

La Aplicación del Protocolo 802.1Q con el uso de Software Libre permite la implementación de VLANs en entornos Wireless.

3.5.2 Determinación de las variables

De acuerdo a la hipótesis se han identificado las siguientes variables:

Variable Independiente VI
La evaluación del protocolo 802.1Q

Variable Dependiente VD
VLANS en entornos Wireless

3.5.3 Operacionalización conceptual

La operacionalización conceptual permite definir a cada una de las variables, a continuación la tabla 1 – 3, se registra la operacionalización conceptual de las variables.

Tabla 1 – 3 Operacionalización Conceptual

Codificación	Variable	Tipo	Definición
VI1	La evaluación del protocolo 802.1Q	Independiente	El protocolo 802.1Q es una especificación y normativa que permite separar de manera lógica la conexión de las estaciones y dispositivos activos.
VD1	VLANS en entornos Wireless	Dependiente	Las Redes Virtuales de Área Local son mecanismos de construcción de separación de elementos, en este caso en entornos Inalámbricos (wireless).

Realizado por: Yungán, J. 2016

3.5.4 Operacionalización Metodológica

La operación metodológica permite identificar los indicadores así como también las técnicas de validación y los instrumentos de verificación, a continuación la tabla 2 – 3, se registra la operacionalización metodológica de las variables.

Tabla 2 – 3 Operacionalización Metodológica

Código	Variable	Categoría	Indicadores	Técnicas	Verificación / Instrumentos
VI1	Protocolo 802.1Q	Independiente	Instalación; Configuración; Implementación.	Observación Directa; Test de Funcionamiento.	Criterio de Experto; Resultado de los Test.
VD1	VLANs en entornos Wireless	Dependiente	Conectividad	Observación Directa; Test de Operación; Medición.	Criterios Técnicos; Resultado del Test Sniffers.

Realizado por: Yungán, J. 2016

3.5.5 Operacionalización Metodológica Variable Independiente.

Tabla 3 – 3 Operacionalización Metodológica Variable Independiente

Variable Independiente	Indicador	Índice	Técnica
Protocolo 802.1Q	1. Instalación	Proceso de instalación de Firmware con soporte de protocolo 801.1Q	Revisión de documentación para instalación configuración y administración de Firmware DD.WRT
	2. Configuración	Proceso de configuración de Firmware habilitación de protocolo 802.1Q	
	3. Implementación	Proceso de Implementación del ambiente de pruebas	

Realizado por: Yungán, J. 2016

3.5.6 Operacionalización Metodológica Variable Dependiente.

Tabla 4 – 3 Operacionalización metodológica Variable Dependiente

Variable Dependiente	Indicador	Índice	Técnica
VLANs en entornos Wireless	1.Diseño	Ambiente de pruebas	Intuición Pruebas Observación Razonamiento
	2. Implementación	Funcionamiento	
		Conectividad	

Realizado por: Yungán, J. 2016

3.6 Población y Muestra

3.6.1 Población

Es el conjunto total objetos o medidas que poseen algunas características comunes observables en un lugar y en un momento determinado, dentro de nuestro escenario de pruebas se diseñó un entorno que establece de una empresa pequeña, la cual cuenta con 4 departamentos en las cuales se realizaran las diferentes pruebas.

3.6.2 Muestra

Es un subconjunto, extraído de la población, cuyo estudio sirve para inferir características de toda la población, se seleccionó una muestra no probabilística de unos de los 4 departamentos en los cuales se implementara todas las pruebas para verificar el correcto funcionamiento de las LAN Virtuales.

3.7 Recursos

3.7.1 Recursos humanos

Se contó con:

- Ejecutor del trabajo de investigación;
- Tutor y Miembros.

3.7.2 Recursos materiales

Material bibliográfico:

- Libros;
- Estándares IEEE;

- Revistas;
- Tesis;
- Sitios WEB referentes al tema.

Material de escritorio:

- Hojas;
- CDs;
- Lápices – Esferos.

3.7.3 Recursos tecnológicos

Software

- Sistema Operativo:

✓ GNU/Linux – CentOS/Ubuntu;
✓ Windows 7 Ultimate.

- Aplicaciones:

✓ DD-WRT Software Libre para implementación firmware en Routers;
✓ Software de monitoreo Wireshark (Sniffer);
✓ Navegador Web.

- Software Utilitario:

✓ OpenOffice;
✓ Microsoft Office;
✓ Microsoft Project.

Hardware

- Equipos portátil Notebook PC Pavilion g4-2055la:

✓ Intel Core i5 2450M;
✓ RAM 8.00 GB;
✓ Disco duro 250 GB;
✓ Tarjeta de Red Wireless 10/100/1000 Mbps.

- Dispositivos de red:

✓ Router inalámbrico, placa BROADCOM 5352;
✓ Switch;
✓ Access Point.

3.7.4 Presupuesto

El proyecto es en su totalidad autofinanciado. A continuación en la tabla 5 – 3, se registran los gastos que demandará el trabajo de investigación:

Tabla 5 – 3 Presupuesto

Denominación	Indicador	Valor unitario (USD)	Subtotal (USD)
Material Bibliográfico	Libros (2 unid)	75,00	150,00
	Revistas	40,00	40,00
Servicio de Internet	Internet (300 horas) y uso de equipo	1,00	300,00
Materiales y Suministros	Papel Bond (1000 unid)	0,01	10,00
	Caja de DVDs (10 unid)	0.50	5,00
	Tóner (1 unid)	80,00	80,00
	Copias y Anillados (1500)	0,03	45,00
	Empastados (4)	15,00	60,00
Equipos	Uso de equipos informáticos(1)	400,00	400,00
Otros	Imprevistos	200,00	200,00
		Total	1290,00

Realizado por: Yungán, J. 2016

3.8 Procedimientos generales

Con el fin de Estudiar la implementación del protocolo 802.1Q en entornos inalámbricos, se implementó un ambiente de pruebas funcional que permita observar la interoperación y funcionamiento del mismo, para ello se comprobó la conectividad de las estaciones de trabajo según las reglas establecidos

3.8.1 Ambientes de prueba

Se ha diseñado como caso de prueba una empresa pequeña, que incluye cuatro departamentos como se muestra en la figura 1 – 3. En la tabla 6 – 3, se registra el plan de direccionamiento IP.

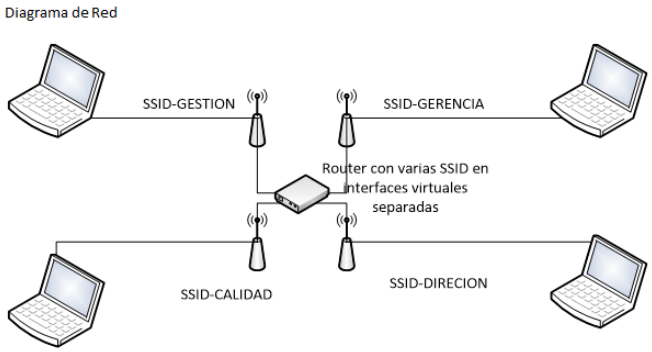


Figura 1 – 3 Ambiente de pruebas
Realizado por: Yungán, J. 2016

3.8.2 Plan de direccionamiento IP

Tabla 6 – 3 Direccionamiento IP

SSID	VLAN	Red	Broadcast	Máscara	Gateway
GESTIÓN	VLAN 11	172.16.10.0	172.16.10.255	255.255.255.0	172.16.10.1
GERENCIA	VLAN 12	172.16.20.0	172.16.20.255	255.255.255.0	172.16.20.1
CALIDAD	VLAN 13	172.16.30.0	172.16.30.255	255.255.255.0	172.16.30.1
DIRECCIÓN	VLAN 14	172.16.40.0	172.16.40.255	255.255.255.0	172.16.40.1

Realizado por: Yungán, J. 2016

3.8.3 Selección de Firmware

Los Firmware OpenWrt y DD-RWT ponen al alcance varias versiones para diferentes fabricantes, modelos y arquitecturas de routers inalámbricos. Para dispositivos con menores recursos hay versiones reducidas que ofrecen funcionalidades restringidas, que están destinados para los routers inalámbricos con menos capacidades. A continuación se detallan las razones para elegir un Firmware en particular:

- Tanto DD_WRT como OpenWrt, disponen de versiones libres bajo licencia GPL y están al alcance en sus sitios oficiales.
- El Firmware DD_WRT y OpenWrt tienen un amplio apoyo de la comunidad por lo que es muy frecuente encontrar soluciones a problemas que experimentan los administradores de red.
- DD-WRT ofrece varias versiones (mini, micro y mega) ya preconfigurado con paquetes preinstalados; mientras que, OpenWrt ofrece una imagen reducida con componentes mínimos, donde que se puede agregar paquetes de acuerdo al ambiente de trabajo.
- DD-WRT es una mejor opción para los usuarios finales, OpenWrt es más técnico puesto que requiere de un dominio de la base teórica tecnológica.
- DD-WRT tiene más soporte para hardware de menor capacidad es decir es funcional en equipos de escala media también conocidos como de mediana y pequeña empresa, mientras que OpenWrt está orientado a ofrecer soluciones a gran escala en hardware con grandes recursos.

Para el presente trabajo se utilizó el Firmware DD-WRT, ya que dispone de un hardware base una placa Broadcom BCM5352 con un procesador de 200 MHz, una memoria RAM de 16MB y una memoria Flash de 4M por lo que se ha decidido instalar el Firmware en su tipo mini, versión V24, nombre del archivo wrt.v24_<type>_generic.bin, el mismo que dispone de una interfaz web para su administración y configuración de servicios.

3.8.4 Procedimiento para instalación de Firmware

Los siguientes pasos permiten instalar DD-WRT v24 en la placa BROADCOM 5352:

1. Descargar el firmware DD-WRT v24.

1.1 Descargar: Versión mini v24 archivo: dd-wrt.v24_sp2_mini.zip

2. Resetear dispositivo vía Interfaz Web

2.1 Conectar la PC a uno de los cuatro (4) puertos LAN

2.2 Abrir el explorador web y en dirección poner la dirección IP 192.168.1.1

3. Ingresar nombre de usuario: en blanco y contraseña: admin

3.1 Hacer click en la pestaña "Administration".

3.2 Hacer click en la sub-pestaña "Factory Defaults".

3.3 Seleccionar "Yes".

3.4 Hacer click en el botón "Save Settings".

3.5 Aparecerá una advertencia, has click en "aceptar".

4. Actualizar Firmware

4.1 Conectar la PC a uno de los cuatro (4) puertos LAN

4.2 Abrir el explorador web y en dirección poner la dirección IP 192.168.1.1

4.3 Ingresar nombre de usuario: en blanco y contraseña: admin

4.3.1 Hacer click en la sub-pestaña "Firmware Upgrade".

4.3.2 Hacer click en el botón "Explorar" (o "Examinar...") y selecciona el archivo "dd-wrt.v24_mini_generic.bin" que descomprimió en el paso 1.

4.3.3 Hacer click en el botón "Upgrade".

4.3.4 No cerrar el navegador, no apagar el router, no apagar la PC

4.3.5 El router tomará unos minutos para subir el archivo, flashear el firmware y resetearse.

4.3.6 Si fue flasheado exitoso se abrirá la interfaz web de DD-WRT y el nombre del router será DD-WRT.

5. Para resetear el dispositivo

5.1 Mantener presionado el botón reset del router por 30 segundos. Esto limpiara la NVRAM, eliminara las configuraciones y reseteará la contraseña a admin.

3.8.5 Implementación de LAN Virtuales

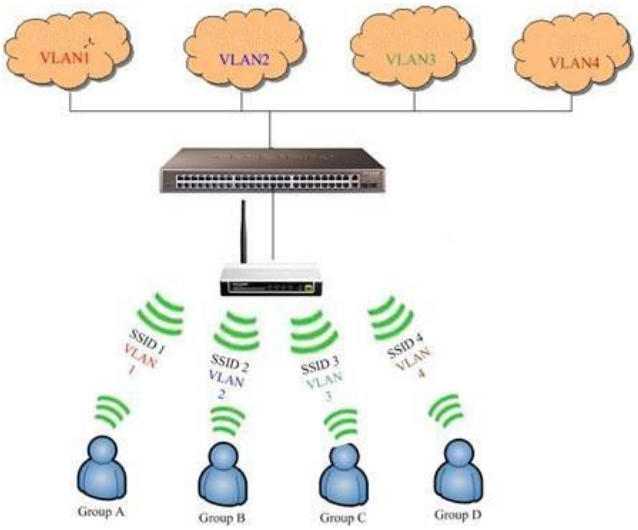


Figura 2 – 3 SSIDs – VLANs
Fuente: http://www.tp-link.com/ar/faq-418.html

Parámetros empleados en la configuración de los SSID

Tabla 7 – 3 Parámetros de configuración SSID

Wireless Physical Interface wl0	
Physical Interface wl0 [ssid-gerencia]	
Wireless Mode:	AP
Wireless Network Mode:	Mixed
Wireless Network Name (SSID):	ssid-gerencia
Wireless Channel:	6 – 2.2437 GHz
Network Configuration:	* Bridged
Virtual Interfaces	
Virtual Interfaces wl0.1 [ssid-direccion]	
Wireless Network Name (SSID):	ssid-direccion
Virtual Interfaces wl0.2 [ssid-calidad]	
Wireless Network Name (SSID):	ssid-calidad
Virtual Interfaces wl0.3 [ssid-gestion]	
Wireless Network Name (SSID):	ssid-gestion

Realizado por: Yungán, J. 2016

Parámetros empleados para crear las VLAN

Tabla 8 – 3 Parámetros para crear VLAN

VLAN	Port					Assigned To Bridge
	W	1	2	3	4	
0						None
1		✓	✓	✓	✓	LAN
11	✓					None
12	✓					None
13	✓					None
14	✓					None
Tagged	✓	✓	✓	✓	✓	
Auto-Negotiate						
Full Speed						
Enabled	✓	✓	✓	✓	✓	
Wireless		LAN				
Link Aggregation on Ports 3 & 4		No				

Realizado por: Yungán, J. 2016

Parámetros empleados para crear puentes y direcciones IP

Tabla 9 – 3 Parámetros para crear Bridges

Bridge 0	br1	STP:	Off	Prio:	32768	MTU:	1500
IP Address	172	16	20	1			
Subnet Mask	255	255	255	0			
Bridge 1	br2	STP:	Off	Prio:	32768	MTU:	1500
IP Address	172	16	30	1			
Subnet Mask	255	255	255	0			
Bridge 2	br3	STP:	Off	Prio:	32768	MTU:	1500
IP Address	172	16	40	1			
Subnet Mask	255	255	255	0			

Realizado por: Yungán, J. 2016

Parámetros de asignación de puentes a Subinterfaces - VLAN

Tabla 10 – 3 Asignación de Bridges a Subinterfaces

Asignación	Puenteo		STP		Interfaces	
Assignment 0	br0	wl0	STP	No	Interface	wl0, VLAN11
Assignment 1	br1	wl0.1	STP	No	Interface	wl0.1, VLAN12
Assignment 2	br2	wl0.2	STP	No	Interface	wl0.2, VLAN13
Assignment 3	br3	wl0.3	STP	No	Interface	wl0.3, VLAN14

Realizado por: Yungán, J. 2016

3.8.6 Pruebas de conectividad

Tabla 11 – 3 Esquema de direccionamiento Ambiente de Pruebas

VLAN	RED	Equipo	IP	Condición
Gestión	172.16.10.0	PC1	172.16.10.2	VLAN SOLA
		PC2	172.16.10.3	
Gerencia	172.16.20.0	PC1	172.16.20.2	VLAN unida con Dirección
		PC2	172.16.20.3	
Calidad	172.16.30.0	PC1	172.16.30.2	VLAN SOLA
		PC2	172.16.30.3	
Dirección	172.16.40.0	PC1	172.16.30.2	VLAN unida con Gerencia
		PC2	172.16.30.3	

Realizado por: Yungán, J. 2016

3.8.7 Resultados de prueba de conectividad

Tabla 12 – 3 Resultado de pruebas de conectividad

		Gestión		Gerencia		Calidad		Dirección	
		PC1	PC2	PC1	PC2	PC1	PC2	PC1	PC2
Gestión	PC1	C	C	F	F	F	F	F	F
	PC2	C	C	F	F	F	F	F	F
Gerencia	PC1	F	F	C	C	F	F	C	C
	PC2	F	F	C	C	F	F	C	C
Calidad	PC1	F	F	F	F	C	C	F	F
	PC2	F	F	F	F	C	C	F	F
Dirección	PC1	F	F	C	C	F	F	C	C
	PC2	F	F	C	C	F	F	C	C

Descripción	Estado		Color
Entre PCs de la misma VLAN y PCs de diferentes VLAN con ruta	C	Exitoso	
Pruebas de conectividad realizadas a si mismo	C	Exitoso	
Entre PCs de diferentes VLAN sin ruta	F	Fallido	

Realizado por: Yungán, J. 2016

CAPITULO IV

4. RESULTADOS Y DISCUSIÓN

4.1 Análisis de Indicadores

Al ser una Investigación Aplicada es necesario comprobar y validar la aplicación del protocolo 802.1Q en redes Wireless, para lo cual el prototipo diseñado es sujeto a la aplicación de pruebas de conectividad en los que se consideraran indicadores como cantidad de paquetes: Transmitidos Tx, Recibidos Rx, y Perdidos y porcentaje de perdidos cantidad de paquetes transmitidos, de paquetes recibidos y los perdidos.

4.2 Indicadores Variable Independiente

La evaluación del protocolo 802.1Q es una especificación y normativa que permite separar de manera lógica la conexión de las estaciones y dispositivos activos. Su arquitectura puntualiza dos funciones:
(1) Permitir el tráfico de mensajes entre equipos pertenecientes a la misma LAN Virtual y
(2) Descartar el tráfico de mensajes que no cumplen con los parámetros de configuración de la LAN Virtual.

4.3 Indicadores Variable Dependiente

4.3.1 Paquetes Transmitidos Tx

Son los mensajes de control de Internet (ICMP Internet Control Message Protocol) enviados desde un equipo a otro en búsqueda de respuesta. En una transmisión de datos local o remota, la cantidad de mensajes transmitidos depende da la infraestructura de tecnológica de red implementada.

4.3.2 Paquetes Recibidos Rx

Son los mensajes ICMP recibidos por su destinatario, estos a su vez son replicados con el propósito de notificar la condición en la que fueron recibidos. La cantidad de paquetes recibidos se sujetara a las condiciones como: los medios de transmisión, el tipo de información que transporten, la infraestructura tecnológica de red, etc.

4.3.3 Paquetes Perdidos

Se refiere a la cantidad de mensajes ICMP que no pudieron llegar a su destino por cualquier alguna circunstancia. Una conexión de red en la que el índice de mensajes perdidos es muy elevada o llegan a ser igual a la cantidad de mensajes enviados, se la considera como una conexión defectuosa o caída de conexión.

4.3.4 Ancho de banda

El ancho de banda es la cantidad de unidades de información que se puede descargar en un determinado tiempo. Un bit es la unidad mínima de información en el mundo binario, y su valor es 0 o 1. Cabe distinguirlo de un byte, que es el conjunto de 8 bits, ya que a veces se juega con la terminología pudiendo confundir.

4.3.5 Latencia

La latencia es un retardo temporal que se produce al transmitir una información por un medio. Puede depender de numerosos factores, pero los principales son: El tamaño de los buffers y el tamaño de los paquetes, la cantidad de “intermediarios” que existan entre el emisor y el receptor, el medio o el material por el cual se transmite y el estado en el que este se encuentra y los protocolos que controlan la transmisión.

4.3.6 Jitter

El camino que puede seguir un paquete entre un mismo transmisor y receptor puede variar en función de ciertos parámetros. A causa de esto y de otros factores, el retardo que puede sufrir un

paquete (latencia) en relación a otro enviado inmediatamente después, puede no ser el mismo. Esto es el jitter, la variación de retardos entre paquetes de la misma comunicación.

4.4 Planteamiento de Hipótesis

La Aplicación del Protocolo 802.1Q con el uso de Software Libre permite la implementación de VLANs en entornos Wireless.

4.4.1 Comprobación de Hipótesis

Para la comprobar de la hipótesis de investigación se procedió a verificar la conectividad. Los resultados se registraron en tablas en las que se sintetizan los resultados obtenidos. Anexo F.

Se aplicaron tres grupos de pruebas:

1. Conectividad entre equipos de la misma LAN Virtual. En la que se aplicó el estudio T STUDENT, que permitió analizar la desviación estándar de los mensajes recibidos y perdidos.
2. Conectividad entre LAN Virtuales con ruta. En la que se aplicó el estudio ADEVA, se analizó la varianza de mensajes enviados y recibidos entre equipos de diferentes LAN Virtuales.
3. Análisis de error paquetes perdidos en la VLAN Calidad. En el que se aplicó Regresión Lineal de Cuarto Orden para medir la variabilidad de mensajes perdidos.
4. Evaluación del parámetro tiempo de ping. En el que se aplicó el estudio ADEVA para contrastar los tiempos promedios de ping entre redes wireless no segmentadas y segmentadas.
5. Evaluación del parámetro paquetes perdidos. En el que se aplicó el estudio ADEVA para contrastar el promedio de paquetes perdidos entre redes wireless no segmentadas y segmentadas.
6. Evaluación del parámetro Jitter. En el que se aplicó el estudio ADEVA para contrastar el promedio de tiempos Jitter entre redes wireless no segmentadas y segmentadas.
7. Evaluación de rendimiento con respecto a la tasa de Descarga. Aplicado entre LAN Virtuales.
8. Evaluación de rendimiento con respecto a la tasa de Carga. Aplicado entre LAN Virtuales.
9. Evaluación de rendimiento con respecto a la Latencia. Aplicado entre LAN Virtuales.

4.5 Resultado e interpretación de pruebas

Condiciones iniciales para la prueba de conectividad. Para verificar la conectividad entre equipos de la misma LAN Virtual y de diferentes LAN Virtuales, se decidió enviar diez mil paquetes desde el origen hacia un destinatario final, durante cinco (5) días.

4.5.1 Evaluación de conectividad entre equipos de la misma LAN Virtual

Tabla 1 – 4 Resultados conectividad entre equipos de la misma LAN Virtual

VLAN	Variables	Estaciones de Trabajo						t student	Prob.	%
		PC 1			PC2					
Calidad	Recibidos	9488,20	+/-	18,14	9497,80	+/-	10,35	-1,03	0,17	17
	Perdidos	511,80	+/-	18,14	502,20	+/-	10,35	1,03	0,17	17
	% Perdidos	5,12	+/-	0,18	5,02	+/-	0,10	1,03	0,17	17
Gestión	Recibidos	9515,80	+/-	26,34	9501,80	+/-	18,53	0,97	0,18	18
	Perdidos	484,20	+/-	26,34	498,20	+/-	18,53	-0,97	0,18	18
	% Perdidos	4,84	+/-	0,26	4,98	+/-	0,19	-0,97	0,18	18
Dirección	Recibidos	9499,00	+/-	17,20	9490,20	+/-	26,05	0,64	0,28	28
	Perdidos	501,00	+/-	17,20	509,80	+/-	26,05	-0,64	0,28	28
	% Perdidos	5,01	+/-	0,17	5,10	+/-	0,26	-0,64	0,28	28
Gerencia	Recibidos	9492,40	+/-	13,96	9501,80	+/-	18,53	-0,74	0,25	25
	Perdidos	507,60	+/-	13,96	498,20	+/-	18,53	0,74	0,25	25
	% Perdidos	5,08	+/-	0,14	4,98	+/-	0,19	0,74	0,25	25

Realizado por: Yungán, J. 2016

Luego de aplicada la prueba T. Student, a los promedios de mensajes recibidos entre las estaciones de trabajo que pertenecen a la misma VLAN tienen una probabilidad mayor al cinco (5) porciento (P > 5 %), lo cual denota que no existe significancia entre paquetes recibidos desde y hacia cada una de las estaciones de trabajo de cada VLAN. Esto demuestra que existe conectividad entre estaciones de trabajo de cada VLAN y se encuentra en igualdad de condiciones. Tabla 1 – 4.

4.5.2 Evaluación de conectividad entre LAN Virtuales con ruta

Conectividad entre estaciones de trabajo de la VLAN Dirección y VLAN Gerencia

Se realizó un Análisis de Varianza (ADEVA), tabla 2 – 4, aplicado en la recepción de paquetes en los departamentos de Dirección y Gerencia, con dos (2) estaciones de trabajo, durante cinco (5) días, obteniendo los siguientes resultados:

Tabla 2 – 4 Conectividad VLAN Dirección – VLAN Gerencia

F. Var	Gl	S. Cuad	C. Medio	Fisher	P. Fisher	%
Total	19	8226,80				
Departamento	1	500,00	500,00	1,13	0,31	31
Maquinas	1	96,80	96,80	0,22	0,65	65
Días	4	1887,30	471,82	1,07	0,41	41
Error	13	5742,70	441,75			
CV %			0,22			
Media			9499,60			

Realizado por: Yungán, J. 2016

Recepción de paquetes de Departamentos: Dirección – Gerencia

Tabla 3 – 4 Promedio paquetes recibidos

Departamento	Media	Grupo
Dirección	9494,60	a
Gerencia	9504,60	a

Realizado por: Yungán, J. 2016

Entre Dirección y Gerencia, el promedio de mensajes recibidos fue de 9494,60 y 9504,60 valores entre los cuales no difieren significativamente, puesto que al aplicar la prueba ADEVA se calcula un valor de Probabilidad Fisher de treinta y uno por ciento (P = 31%) que es un valor de probabilidad mayor al uno por ciento (P > 1%) que plantea el análisis de varianza para evidenciar significancia. Esto quiere decir que la recepción de paquetes en los departamentos es equitativa, como se registra en la tabla 3 – 4, gráfico 1 – 4.

Recepción de paquetes de Estaciones de Trabajo: PC1 – PC2.

Tabla 4 – 4 Promedio paquetes PC1 – PC2

Máquinas	Media	Grupo
PC1	9501,80	a
PC2	9497,40	a

Realizado por: Yungán, J. 2016

Entre las estaciones de trabajo PC1 y PC2 de los departamentos de Dirección y Gerencia, el promedio de mensajes recibidos fue de 9501,80 y 9497,40 respectivamente. Los valores no expresan significancia. El valor de Probabilidad Fisher calculado es de sesenta y cinco por ciento (P = 65%) y es mayor a la probabilidad de uno por ciento (P > 1%) que plantea el análisis de varianza para evidenciar significancia. Esto quiere decir que la recepción de mensajes entre estaciones de trabajo es equitativa, como se registra en la tabla 4 – 4, gráfico 1 – 4.

Recepción de paquetes por día

Tabla 5 – 4 Promedio paquetes por día

Días	Media	Grupo
I	9493,75	a
II	9502,50	a
III	9504,25	a
IV	9513,00	a
V	9484,50	a

Realizado por: Yungán, J. 2016

Los días I, II, III, IV y V; se recibieron en promedio: 9493,75; 9502,50; 9504,25; 9513,00 y 9484,50 mensajes respectivamente entre las estaciones de trabajo de los departamentos. La probabilidad de Fisher calculada es de cuarenta y uno por ciento (P = 41%) y es mayor al uno por ciento (P > 1%) planteado por el análisis de varianza para demostrar significancia. Esto quiere decir que no existe diferencia trascendente por lo que se concluye que el trabajo en los cinco (5) días es equitativo, como se registra en la tabla 5 – 4, gráfico 1 – 4.

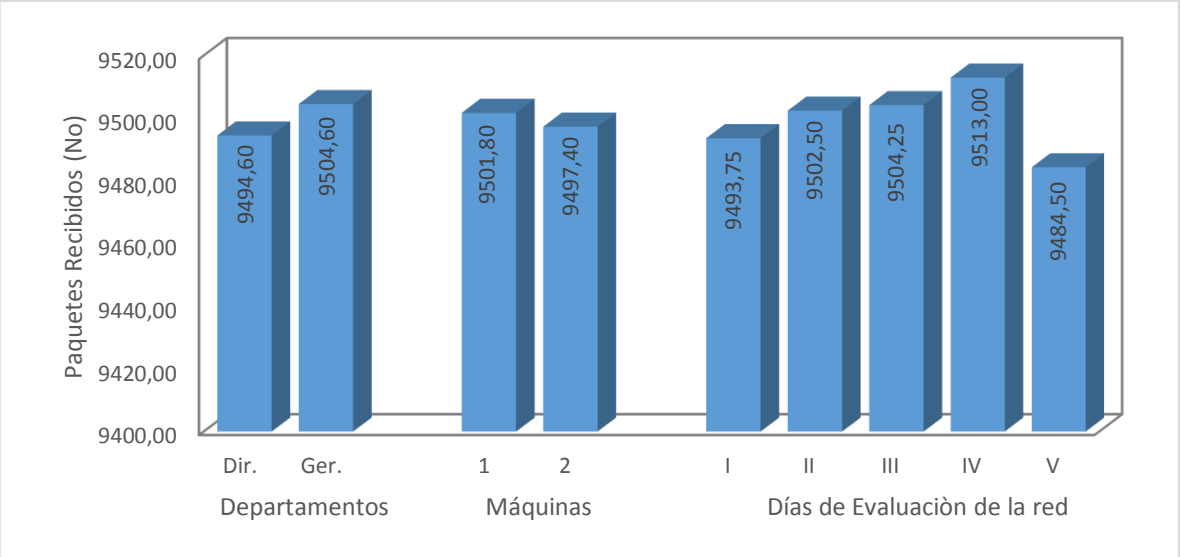


Gráfico 1 – 4 Conectividad VLAN Dirección y VLAN Gerencia
Realizado por: Yungán, J. 2016

Conectividad entre estaciones de trabajo de la VLAN Gerencia y VLAN Dirección

A continuación se plantea un estudio de Análisis de Varianza similar al anterior tomando como referencia el orden Gerencia – Dirección. Tabla 6 – 4.

Tabla 6 – 4 Conectividad VLAN Gerencia – VLAN Dirección

F. Var	gl	S. Cuad	C. Medio	Fisher	P. Fisher	%
Total	19	4808,80				
Departamento	1	5,00	5,00	0,02	0,89	89
Maquinas	1	1008,20	1008,20	3,85	0,07	7
Días	4	393,30	98,32	0,38	0,82	82
Error	13	3402,30	261,72			
CV %			0,17			
Media			9497,60			

Realizado por: Yungán, J. 2016

Recepción de mensajes de departamentos Gerencia – Dirección

Tabla 7 – 4 Promedio paquetes transmitidos

Departamento	Media	Grupo
Dirección	9498,10	a
Gerencia	9497,10	a

Realizado por: Yungán, J. 2016

El promedio de mensajes recibidos fue de 9498,10 y 9497,10; valores que no varían significativamente. Al aplicar ADEVA se calcula un valor de Probabilidad Fisher de ochenta y nueve por ciento (P = 89%) que es un valor de probabilidad mayor al uno por ciento (P >1%) que plantea el análisis de varianza para evidenciar significancia. Esto quiere decir que la recepción de mensajes en los departamentos es equitativa, como se registra en la tabla 7 – 4, gráfico 2 – 4.

Recepción de mensajes de Estaciones de Trabajo PC1 – PC2.

Tabla 8 – 4 Promedio paquetes PC1 – PC2

Máquinas	Media	Grupo
PC1	9490,50	a
PC2	9504,70	a

Realizado por: Yungán, J. 2016

Entre las estaciones de trabajo PC1 y PC2 de los departamentos de Gerencia y Dirección, el promedio de mensajes recibidos fue de 9490,50 y 9504,70 respectivamente. Los valores no expresan significancia. El valor de Probabilidad Fisher calculado es de siete por ciento (P = 7%) y es mayor a la probabilidad de uno por ciento (P > 1) que plantea el análisis de varianza para evidenciar significancia. Esto quiere decir que la recepción de mensajes entre estaciones de trabajo es equitativa, como se registra en la tabla 8 – 4, gráfico 2 – 4.

Recepción de mensajes por día

Tabla 9 – 4 Promedio paquetes por día

Días	Media	Grupo
I	9495,75	a
II	9503,25	a
III	9494,00	a
IV	9492,50	a
V	9502,50	a

Realizado por: Yungán, J. 2016

Los días I, II, III, IV y V; se recibieron en promedio: 9495,75; 9503,25; 9494,00; 9492,50 y 9502,50 mensajes respectivamente entre las estaciones de trabajo de los departamentos. La probabilidad de Fisher calculada es de ochenta y dos por ciento (P = 82%) y es mayor al uno por ciento (P > 1%) planteado por el análisis de varianza para demostrar significancia. Esto quiere decir que no existe diferencia trascendente por lo que se concluye que el trabajo en los cinco (5) días es equitativo, como se registra en la tabla 9 – 4, gráfico 2 – 4.

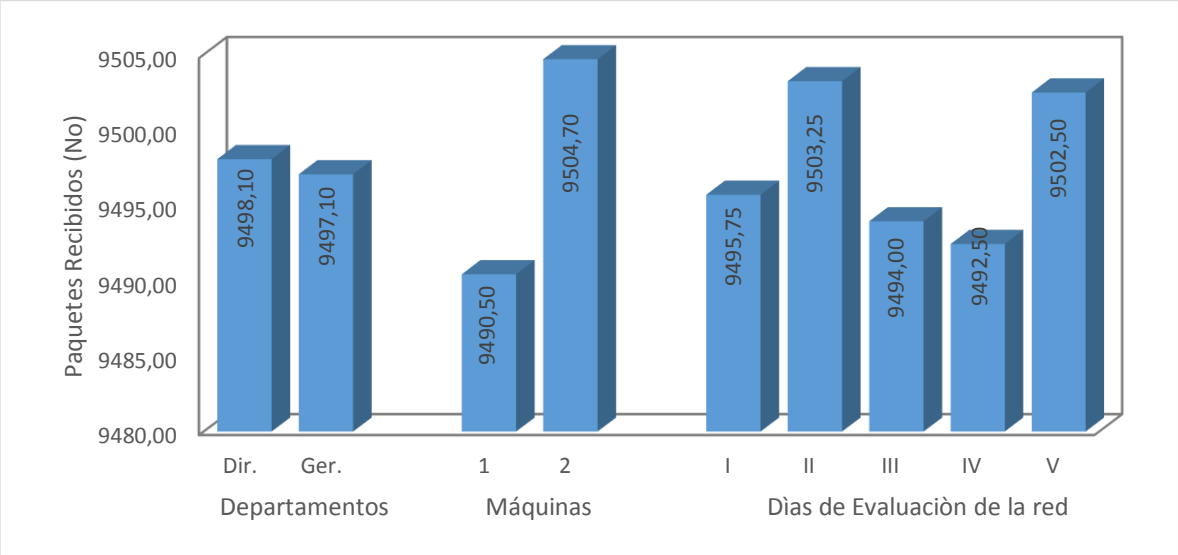


Gráfico 2 – 4 Conectividad VLAN Gerencia y VLAN Dirección
Realizado por: Yungán, J. 2016

4.5.3 Análisis de paquetes perdidos en la LAN Virtual Calidad

Para analizar el porcentaje de variabilidad de los mensajes perdidos que van de una estación de trabajo, se eligió la VLAN Calidad en la que al aplicar la prueba de Regresión Lineal de cuarto orden que muestra que la probabilidad de perdida e menor al uno por ciento (P > 1%), lo que implica a decir que el noventa y nueve por ciento (99%) de los paquetes enviados llegan a su destino, como se registra en la tabla 10 – 4, gráfico 3 – 4.

Tabla 10 – 4 Análisis de paquetes perdidos VLAN Calidad

Días	X^2	X^3	X^4	% Perdidos
1	1	1	1	5,11
2	4	8	16	4,95
3	9	27	81	4,91
4	16	64	256	5,15
5	25	125	625	4,99

Realizado por: Yungán, J. 2016

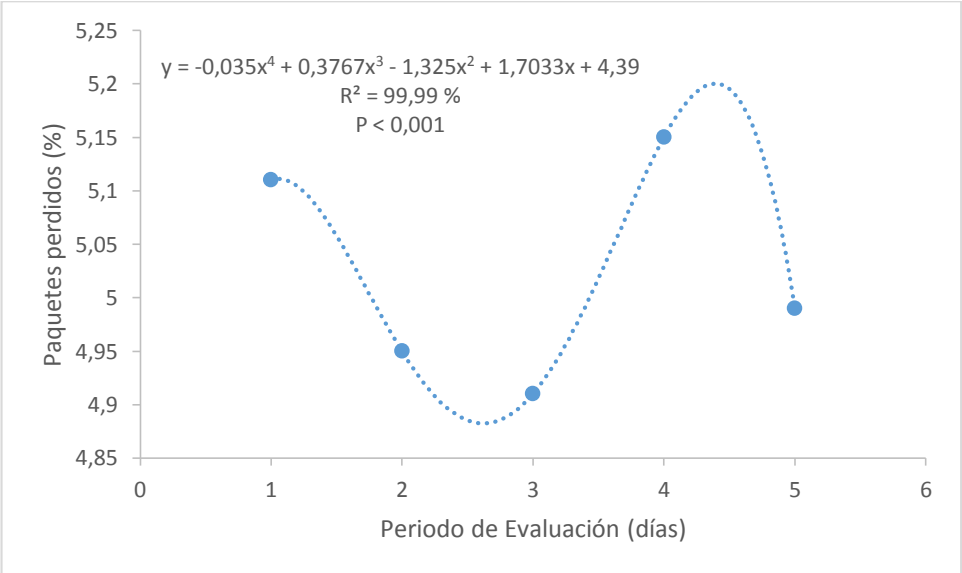


Gráfico 3 – 4 Paquetes perdidos VLAN Calidad
Realizado por: Yungán, J. 2016

4.5.4 Evaluación parámetro tiempo de respuesta Ping

Tabla 11 – 4 Registro tiempos Ping

VLAN	PC	Obs.				
		I	II	III	IV	V
1	1	86	85	88	86	89
1	2	100	94	96	124	152
2	1	112	119	163	166	172
2	2	169	162	172	164	143
3	1	117	129	139	145	126
3	2	188	228	204	138	234
4	1	267	188	196	296	260
4	2	277	228	181	173	261
SIN VLAN	1	392	306	353	439	482
SIN VLAN	2	263	443	635	319	399
SIN VLAN	3	371	337	598	589	585
SIN VLAN	4	402	385	865	438	446
SIN VLAN	5	374	318	589	421	490
SIN VLAN	6	362	404	401	599	383
SIN VLAN	7	433	483	264	315	672
SIN VLAN	8	401	599	383	433	483

Realizado por: Yungán, J. 2016

Tabla 12 – 4 ADEVA registro tiempos Ping

F. Var	gl	S. Cuad	C. Medio	Fisher	P. F.	Significancia
Total	79	2338624,49				
Trat.	8	1710069,39	213758,67	24,15	0,00	**
VLAN (A)	3	89077,48	29692,49	3,35	0,02	*
PC (B)	1	5267,02	5267,02	0,59	0,44	ns
Int. AB	3	9130,27	3043,42	0,34	0,79	ns
Ts vs Resto	1	1606594,61	1606594,61	181,48	0,00	**
Error	71	628555,10	8852,89			
CV %			0,31			
Media			304,64			

Realizado por: Yungán, J. 2016

Se compara el tiempo que incurre la prueba ping en comprobar la conectividad entre estaciones de trabajo que se encuentran en una red Wireless: 1. Sin segmentar y 2. Segmentada en cuatro VLANs y un servidor externo. Se registra que el tiempo de ping que toma una PC que se encuentra en una VLAN es menor al tiempo que toma una PC que se encuentra sin segmentar. Tablas 11 – 4 y 12 – 4.

Separación de medias según Tukey (P<0,05)

Tabla 13 – 4 Análisis de medias Ping

Para VLANs		
VLAN (A)	**Media**	**Rango**
1	100,00	c
2	154,20	b
3	164,80	b
4	232,70	a
Para PCs		
PC (B)	**Media**	**Rango**
1	151,45	b
2	174,40	a
Interacción VLANs – PCs		
Int. AB	**Media**	**Rango**
A1B1	86,80	a
A1B2	113,20	a
A2B1	146,40	a
A2B2	162,00	a
A3B1	131,20	a
A3B2	198,40	a
A4B1	241,40	a
A4B2	224,00	a
Contraste Sin VLAN – Con VLAN		
Contraste	**Media**	**Rango**
SIN VLAN	446,35	a
CON VLAN	162,93	b

Realizado por: Yungán, J. 2016

El análisis de separación de medias tabla 13 – 4, se considera que:

El tiempo promedio de ping en una VLAN es menor inicialmente VLAN 1 100 ms y va incrementando conforme se incrementa VLANs con PCs (VLAN 4 232.70 ms).

El tiempo promedio de ping que incurre una PC para la prueba ping en VLAN es de PC1 151, 45 ms y PC2 174,40 ms.

El tiempo promedio de todas las PCs que se encuentran en una red wireless sin segmenta alcanza el valor promedio 446,35 ms mientras que las PCs que se encuentran en la red wireless segmentada por cuatro VLANs alcanza el valor promedio 162,93 ms.

En conclusión, el tiempo es significativamente menor en redes wireless segmentadas por VLANs.

4.5.5 Evaluación parámetro Jitter

Tabla 14 – 4 Registro tiempos Jitter

VLAN	PC	Obs.				
		I	II	III	IV	V
1	1	7	6	8	6	12
1	2	11	2	5	8	36
2	1	9	31	12	33	23
2	2	29	10	16	18	8
3	1	7	8	29	42	8
3	2	52	21	23	52	9
4	1	40	34	62	68	99
4	2	75	152	41	47	114
SIN VLAN	1	183	194	134	202	176
SIN VLAN	2	175	202	210	156	168
SIN VLAN	3	130	149	201	257	273
SIN VLAN	4	149	139	1266	176	162
SIN VLAN	5	255	128	385	136	354
SIN VLAN	6	140	359	367	208	149
SIN VLAN	7	526	636	148	168	263
SIN VLAN	8	367	208	149	526	636

Realizado por: Yungán, J. 2016

Tabla 15 – 4 ADEVA registro Tiempos Jitter

F. Var	gl	S. Cuad	C. Medio	Fisher	P. F.	Significancia
Total	79	2911526,89				
Trat.	8	1163001,39	145375,17	5,90	0,00	**
VLAN (A)	3	23961,48	7987,16	0,32	0,81	ns
PC (B)	1	855,63	855,63	0,03	0,85	ns
Int. AB	3	1254,68	418,23	0,02	1,00	ns
Ts vs Resto	1	1136929,61	1136929,61	46,17	0,00	**
Error	71	1748525,50	24627,12			
CV %			1,04			
Media			151,04			

Realizado por: Yungán, J. 2016

Se compara el tiempo que incurre la prueba JITTER en comprobar el tiempo de retardo que experimentarían entre estaciones de trabajo que se encuentran en una red Wireless: 1. Sin segmentar y 2. Segmentada en cuatro VLANs y un servidor externo. Se registra que el tiempo de retardo que toma una PC que se encuentra en una VLAN es menor al tiempo que toma una PC que se encuentra sin segmentar. Tablas 14 – 4, 15 – 4.

Separación de medias según Tukey (P<0,05)

Tabla 16 – 4 Análisis de medias Jitter

Para VLANs		
VLAN	**Media**	**Rango**
1	10,10	c
2	18,90	b
3	25,10	b
4	73,20	a
Para PCs		
PC (B)	**Media**	**Rango**
1	27,20	a
2	36,45	a
Interacción VLANs – PCs		
Int. AB	**Media**	**Rango**
A1B1	7,80	a
A1B2	12,40	a
A2B1	21,60	a
A2B2	16,20	a
A3B1	18,80	a
A3B2	31,40	a
A4B1	60,60	a
A4B2	85,80	a
Contraste Sin VLAN – Con VLAN		
Contraste	**Media**	**Rango**
SIN VLAN	270,25	a
CON VLAN	31,83	b

Realizado por: Yungán, J. 2016

El análisis de medias tabla 16 – 4, se considera que:

El tiempo promedio de retardo jitter de una VLAN es menor inicialmente VLAN 1 10.10 ms y va incrementando conforme se incrementa VLANs con PCs (VLAN 4 73.20 ms).

El tiempo promedio jitter que incurre una PC en VLAN es de PC1 27.20 ms y PC2 36.45 ms.

El tiempo promedio de jitter de todas las PCs que se encuentran en una red wireless sin segmenta alcanza el valor promedio 270.25 ms mientras que las PCs que se encuentran en la red wireless segmentada por cuatro VLANs alcanza el valor promedio 31,83 ms.

En conclusión, el tiempo de jitter es significativamente menor en redes wireless segmentadas por VLANs.

4.5.6 Evaluación parámetro Paquetes Perdidos

Tabla 17 – 4 Registro paquetes perdidos

VLAN	PC	Obs.				
		I	II	III	IV	V
1	1	0	1	0	0	0
1	2	1	0	0	0	0
2	1	0	1	0	0	0
2	2	0	1	0	0	0
3	1	0	1	0	0	0
3	2	1	0	0	0	0
4	1	0	0	1	0	0
4	2	0	1	0	0	0
SIN VLAN	1	0	1	0	1	0
SIN VLAN	2	0	0	1	0	1
SIN VLAN	3	0	0	0	0	0
SIN VLAN	4	0	1	0	0	0
SIN VLAN	5	0	1	1	1	0
SIN VLAN	6	0	1	0	1	0
SIN VLAN	7	0	0	3	0	0
SIN VLAN	8	2	0	1	0	0

Realizado por: Yungán, J. 2016

Tabla 18 – 4 ADEVA registro de Paquetes perdidos

F. Var	gl	S. Cuad	C. Medio	Fisher	P. F.	Significancia
Total	79	24,80				
Trat.	8	0,80	0,10	0,30	0,97	ns
VLAN (A)	3	0,00	0,00	0,00	1,00	ns
PC (B)	1	0,00	0,00	0,00	1,00	ns
Int. AB	3	0,00	0,00	0,00	1,00	ns
Ts vs Resto	1	0,80	0,80	2,37	0,13	ns
Error	71	24,00	0,34			
CV %			1,94			
Media			0,30			

Realizado por: Yungán, J. 2016

Se compara los paquetes perdidos que experimentan las estaciones de trabajo que se encuentran en una red Wireless: 1. Sin segmentar y 2. Segmentada en cuatro VLANs y un servidor externo. Se registra que el número de paquetes perdidos en PCs que se encuentra en una VLAN es igual al número de paquetes perdidos en PCs que se encuentra sin segmentar. Tablas 17 – 4 y 18 – 4.

Separación de medias según Tukey (P<0,05)

Tabla 19 – 4 Análisis paquetes perdidos

Para VLANs		
VLAN	Media	Rango
1	0,20	a
2	0,20	a
3	0,20	a
4	0,20	a
Para PCs		
PC (B)	Media	Rango
1	0,20	a
2	0,20	a
Interacción VLANs – PCs		
Int. AB	Media	Rango
A1B1	0,20	a
A1B2	0,20	a
A2B1	0,20	a
A2B2	0,20	a
A3B1	0,20	a
A3B2	0,20	a
A4B1	0,20	a
A4B2	0,20	a
Contraste Sin VLAN – Con VLAN		
Contraste	Media	Rango
SIN VLAN	0,40	a
CON VLAN	0,20	a

Realizado por: Yungán, J. 2016

El análisis de medias tabla 19 – 4, se considera que:

El número de paquetes perdidos en ambos escenarios no es significativo. Existe una diferencia de perdida de paquetes entre el escenario no segmentado y el segmentado en VLANs que no es evidencia para concluir que la perdida de paquetes es menor en redes segmentadas con VLAN. Se justificaría que el escenario y la disposición de los equipos, sumado a las condiciones ambientales han sido favorables en la toma y registro de datos.

4.5.7 Evaluación parámetro tasa de Descarga

Tabla 20 – 4 Registro de tasa de Descarga

Repeticiones	VLAN 1		VLAN 2		VLAN 3		VLAN 4	
	PC1	PC2	PC1	PC2	PC1	PC2	PC1	PC2
1	2,60	1,97	2,05	1,74	2,80	3,16	3,01	2,37
2	2,07	2,00	1,40	1,62	2,88	3,02	2,92	2,07
3	2,04	2,04	1,96	1,70	1,84	3,02	2,53	2,07
4	2,02	2,07	2,06	2,66	3,01	2,77	2,79	1,46
5	2,07	2,02	1,93	2,42	2,95	2,91	3,44	2,05
6	2,05	2,05	1,50	2,05	2,86	3,17	3,11	1,74
7	2,24	2,07	2,07	3,16	3,1	3,18	3,08	1,62
8	2,07	1,83	2,07	1,73	2,86	2,68	2,92	1,70
9	1,35	1,94	1,46	3,17	3,18	3,00	2,99	2,92
10	2,07	1,91	2,05	3,23	2,93	2,94	3,14	2,99

Realizado por: Yungán, J. 2016

Tabla 21 – 4 ADEVA tasa de Descarga

F. Var	gl	S. Cuad	C. Medio	Fisher	P. Fisher	Significancia
Total	79	25,71				
VLAN (A)	3	10,30	3,43	24,53	0,00	**
PC (B)	1	0,13	0,13	0,94	0,33	ns
Int AB	3	5,21	1,74	12,40	0,00	**
Error	72	10,08	0,14			
CV %			15,61			
Media			2,40			

Realizado por: Yungán, J. 2016

Del análisis de varianza se puede definir que la tasa de descarga es altamente significativa en las LAN Virtuales; también se nota que la tasa de descarga al momento de relacionar las LAN Virtuales con las PC también es altamente significativa. Tablas 20 – 4 y 21 – 4.

Separación de medias según Tukey (P<0,05)

Tabla 22 – 4 Análisis tasa de Descarga

Para VLANs		
VLAN	Media	Rango
1	2,02	c
2	2,10	c
3	2,91	a
4	2,55	b
Para PCs		
PC (B)	Media	Rango
1	2,44	a
2	2,36	a
Interacción VLANs – PCs		
Int. AB	Media	Rango
A1B1	2,06	bc
A1B2	1,99	bc
A2B1	1,86	c
A2B2	2,35	b
A3B1	2,84	a
A3B2	2,99	a
A4B1	2,99	a
A4B2	2,10	bc

Realizado por: Yungán, J. 2016

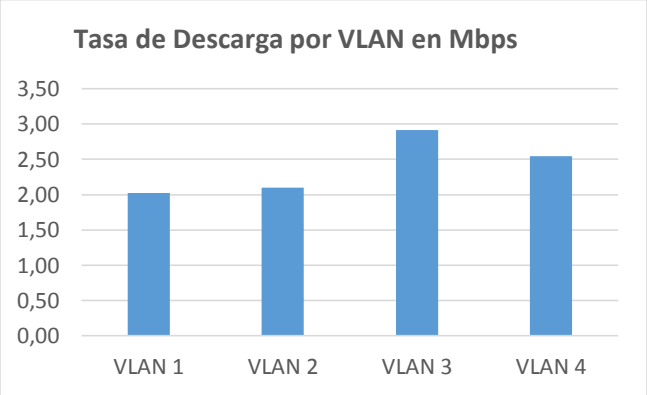


Gráfico 4 – 4 Tasa de Descarga por VLAN en Mbps
Realizado por: Yungán, J. 2016

Como se muestra en el grafico 4 – 4, en la VLAN 3 (2.91 Mbps) y la VLAN 4 (2.55 Mbps) disponen del mayor ancho de banda para la descarga; esto se debe a que son las primeras redes virtuales que se hicieron de la propiedad del recurso. Tabla 22 – 4.

4.5.8 Evaluación parámetro tasa de Subida

Tabla 23 – 4 Registro de tasa de Subida

Repeticiones	VLAN 1		VLAN 2		VLAN 3		VLAN 4	
	PC1	PC2	PC1	PC2	PC1	PC2	PC1	PC2
1	0,38	0,53	0,49	0,21	0,3	0,53	0,17	0,5
2	0,5	0,46	0,52	0,33	0,34	0,31	0,48	0,44
3	0,42	0,53	0,52	0,5	0,17	0,41	0,25	0,35
4	0,52	0,27	0,44	0,38	0,33	0,34	0,47	0,23
5	0,54	0,52	0,53	0,32	0,25	0,15	0,47	0,31
6	0,45	0,22	0,29	0,5	0,28	0,53	0,52	0,21
7	0,51	0,53	0,44	0,42	0,31	0,27	0,47	0,33
8	0,43	0,29	0,35	0,2	0,27	0,22	0,49	0,5
9	0,51	0,5	0,23	0,43	0,5	0,5	0,5	0,49
10	0,52	0,27	0,31	0,3	0,25	0,39	0,54	0,5

Realizado por: Yungán, J. 2016

Tabla 24 – 4 ADEVA registro tasa de Subida

F. Var	gl	S. Cuad	C. Medio	Fisher	P. Fisher	Significancia
Total	79	1,07				
VLAN (A)	3	0,13	0,04	3,74	0,01	*
PC (B)	1	0,01	0,01	1,12	0,29	ns
Int AB	3	0,06	0,02	1,55	0,21	ns
Error	72	0,87	0,01			
CV %			27,87			
Media			0,39			

Realizado por: Yungán, J. 2016

Del análisis de varianza se puede definir que la tasa de subida es significativa en las LAN Virtuales; para las demás variables no tiene significado. Tablas 23 – 4 y 24 – 4.

Separación de medias según Tukey (P<0,05)

Tabla 25 – 4 Tasa de Subida

Para VLANs		
VLAN	Media	Rango
1	0,45	a
2	0,39	ab
3	0,33	b
4	0,41	ab
Para PCs		
PC (B)	Media	Rango
1	0,41	a
2	0,38	a
Interacción VLANs – PCs		
Int. AB	Media	Rango
A1B1	0,48	a
A1B2	0,41	a
A2B1	0,41	a
A2B2	0,36	a
A3B1	0,30	a
A3B2	0,37	a
A4B1	0,44	a
A4B2	0,39	a

Realizado por: Yungán, J. 2016

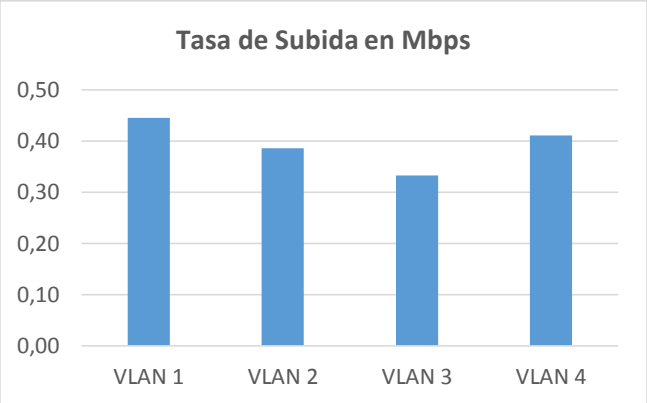


Gráfico 5 – 4 Tasa de Subida por VLAN en Mbps
Realizado por: Yungán, J. 2016

Como se muestra en el grafico 5 – 4, se puede observar que en la VLAN 3 es la que menor promedio de ancho de banda dispone para la subida de datos (0.33 Mbps). Las VLAN restantes se mantienen entre 0,39 a 0,45 Mbps. Tabla 25 – 4.

4.5.9 Evaluación parámetro Latencia

Tabla 26 – 4 Registro de tiempos de Latencia

Repeticiones	VLAN 1		VLAN 2		VLAN 3		VLAN 4	
	PC1	PC2	PC1	PC2	PC1	PC2	PC1	PC2
1	74	16	18	15	56	23	83	14
2	14	14	14	13	46	96	80	13
3	16	16	15	16	47	75	86	13
4	14	14	13	99	35	87	69	54
5	17	15	19	47	73	77	56	20
6	14	16	14	63	67	22	23	15
7	17	13	13	67	78	67	24	13
8	14	16	13	63	58	88	25	16
9	86	51	54	51	23	55	22	25
10	19	20	56	38	81	77	25	22

Realizado por: Yungán, J. 2016

Tabla 27 – 4 ADEVA Latencia

F. Var	gl	S. Cuad	C. Medio	Fisher	P. Fisher	Significancia
Total	79	58675,55				
VLAN (A)	3	15436,65	5145,55	10,53	0,00	**
PC (B)	1	16,20	16,20	0,03	0,86	ns
Int AB	3	8055,70	2685,23	5,50	0,00	**
Error	72	35167,00	488,43			
CV %			56,92			
Media			38,83			

Realizado por: Yungán, J. 2016

Del análisis de varianza se puede definir que la latencia es altamente significativa en las LAN Virtuales; también se nota que la latencia al momento de relacionar las LAN Virtuales con las PC también es altamente significativa. Tablas 26 – 4 y 27 – 4.

Separación de medias según Tukey (P<0,05)

Tabla 28 – 4 Análisis de medias Latencia

Para VLANs		
VLAN	Media	Rango
1	23,80	b
2	35,05	b
3	61,55	a
4	34,90	b
Para PCs		
PC (B)	Media	Rango
1	39,28	a
2	38,38	a
Interacción VLANs – PCs		
Int. AB	Media	Rango
A1B1	28,50	bcd
A1B2	19,10	d
A2B1	22,90	cd
A2B2	47,20	abc
A3B1	56,40	ab
A3B2	66,70	a
A4B1	49,30	abc
A4B2	20,50	d

Realizado por: Yungán, J. 2016

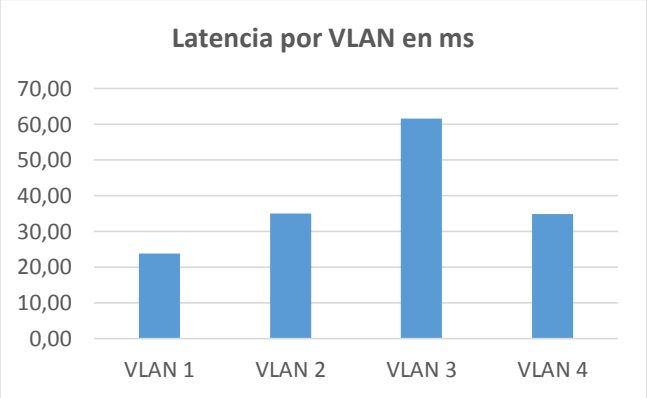


Gráfico 6 – 4 Latencia
Realizado por: Yungán, J. 2016

Como se muestra en el grafico 6 – 4, se puede observar que en la VLAN 1 es la que menor promedio de latencia tiene con 23,80 ms; la VLAN 4 con 34,90ms; la VLAN 2 con 35,05 ms; y por último la VLAN 3 con 61,55. Tabla 28 – 4.

4.6 Conclusión de Hipótesis

Se definieron tanto la hipótesis nula (Ho) como la hipótesis de investigación (Hi).

Ho. La Aplicación del Protocolo 802.1Q con el uso de Software Libre no permite la implementación de VLANs en entornos Wireless.

Hi. La Aplicación del Protocolo 802.1Q con el uso de Software Libre permite la implementación de VLANs en entornos Wireless.

Tabla 29 – 4 Resumen de conectividad

Variables			Paquetes			
			Recibidos	**Perdidos**	**% Recibidos**	**% Perdidos**
LAN VIRTUALES	**Calidad**	**PC1**	9488,20	511,80	94,8820	5,1180
		PC2	9497,80	502,20	94,9780	5,0220
	Gestión	**PC1**	9515,80	484,20	95,1580	4,8420
		PC2	9501,80	498,20	95,0180	4,9820
	Dirección	**PC1**	9499,00	501,00	94,9900	5,0100
		PC2	9490,20	509,80	94,9020	5,0980
	Gerencia	**PC1**	9492,40	507,60	94,9240	5,0760
		PC2	9501,80	498,20	95,0180	4,9820
Promedios			9498,38	501,63	94,98375	5,01625

Realizado por: Yungán, J. 2016

La prueba de conectividad permite concluir que es aplicable el protocolo 802.1Q en entornos Wireless. La función del protocolo es segmentar la red física en redes lógicas. Esto quiere decir que existe conectividad entre estaciones de trabajo de la misma LAN Virtual y conectividad entre estaciones de trabajo de diferentes LAN Virtuales con una ruta definida.

Para tal efecto se han transmitidos en ambos casos diez mil paquetes y lo importante es que han sido recibidos en un noventa y cinco por ciento (95%) y se han registrado perdida de paquetes alrededor del cinco por ciento (5%), este indicador nos permite inferir que existe conectividad.

Los paquetes enviados entre estaciones de trabajo que no pertenecen a la LAN Virtual o no tienen definida ruta de destino a otra LAN Virtual, han sido descartados en un cien por ciento (100%), es decir, no existe conectividad.

Por tanto la Hipótesis Nula (Ho) es descartada y se acepta la Hipótesis de Investigación (Hi).

CONCLUSIONES

Una LAN Virtual es una red conmutada que está segmentada lógicamente. Permite mejorar la administración. Incrementa niveles de seguridad. Mejora el rendimiento al reducir los dominios de Multidifusión.

El protocolo 802.1Q incorpora en la trama Ethernet dos campos de dos bytes cada uno. Un campo de dos bytes permite identificar el protocolo de LAN Virtual registrado como 0x8100 y el segundo es el más importante puesto que 12 bits de este corresponde al VID. Una trama 802.1Q alcanza un tamaño de1522 bytes en relación a la trama Ethernet de 1518 bytes. Sin embargo es mucho más ligera que la trama ISL con un tamaño máximo de 1548 bytes.

La evaluación del protocolo 802.1Q está en función a la operación que realiza con la información contenida en las Base de Datos de Filtrado (direcciones MAC, VID, etc.). Los parámetros de evaluación considerados como REENVÍO, FILTRADO Y REGISTRO definen el destino de cada trama que entra y/o sale de un puerto.

Las LAN Virtuales también son configurables en las redes inalámbricas. El estándar IEEE 802.1Q es un protocolo que tiene relación directa con Ethernet IEEE 802.3. Para que haya la posibilidad de implementarlo en entornos wireless IEEE 802.11b/g/n es necesario que el equipo ruteador inalámbrico permita la conexión física de la interfaz wireless a una interfaz Ethernet, además debe estar provisto de un Firmware con soporte para protocolo 802.1Q.

La creación de múltiples SSIDs en los concentradores inalámbricos permite tener un ambiente de varias LAN Virtuales. Cada SSID es mapeado a través de un puente a una LAN Virtual. Las LAN Virtuales tienen un ID de VLAN o nombre, de ahí que, cada SSID de un concentrador inalámbrico reconoce un ID de LAN Virtual específico.

El protocolo 802.1Q aplica la función de RELAY para encaminar tramas que entran a un puerto, en tal virtud, se ha aplicado pruebas de conectividad para confirmar su correcta configuración. La prueba se remite a solo una respuesta de dos posibles “Hay conexión o No hay conexión”. La prueba de conectividad aplicada en el ambiente de pruebas planteado evidencia que existe el 95 % de efectividad en el envío y recepción de mensajes ICMP con una pérdida del 5 %.

A través de la segmentación de red en LAN Virtuales, se evidencia incremento significativo en índices tales como tiempo de PING (sin VLAN 446,35 ms y con VLAN 162,93 ms), JITTER (sin VLAN 270,25 ms y con VLAN 31,83 ms) y PERDIDA DE PAQUETES (sin VLAN 0,40 y con VLAN 0,20) esto se debe a la reducción de dominios de colisión y focalización de tráfico.

RECOMENDACIONES

Las exigencias de tener redes convergentes, con capacidad de transportar grandes volúmenes de información de todo tipo en tiempo real es un reto para los diseñadores de red. Por esto es necesario recomendar a los profesionales que en sus diseños se considere que para alcanzar redes con altos niveles de rendimiento diseñen considerando la segmentación física de la red en varias LAN Virtuales.

Si se necesita aplicar Calidad de Servicio con tráfico en Tiempo Real, el formato de trama del protocolo 802.1Q incluye un campo de tres bits denominado de Prioridad.

Los entornos de red inalámbrica van incrementándose cada día. Los usuarios exigen redes rápidas y seguras en ambientes móviles para ejercer su trabajo. Para alcanzar este requerimiento es necesario tener flexibilidad al momento de configurar y administrar los dispositivos de red, por lo que se recomienda analizar más a fondo la propuesta que plantea Firmware Libre.

La funcionalidad de las LAN Virtuales en entornos inalámbricos es muy dependiente de la tecnología inalámbrica. Para lo cual se recomienda analizar la Arquitectura Hardware de los dispositivos de red inalámbricos para encontrar una alternativa ideal de Software a ser implantada.

Tomar en cuenta el tamaño de las tramas. Se recuerda que hay un incremento de 4 bytes en las tramas Ethernet, por lo que dependiendo de la tecnología de conmutación que se utilice estas serán más grandes por lo cual se recomienda que en el dispositivo que gestione la conmutación se incremente el tamaño de la MTU (Unidad Máxima de Transferencia).

Al momento de evaluar el rendimiento de las redes de inalámbricas, se recomienda considerar factores tales como los tecnológicos, topológicos, ambientales; ya que en el presente trabajo no han sido considerados.

Como trabajos de futuros se plantea investigar: La relación de los protocolos de puenteo y protocolos que evitan lazos, la Convergencia en redes inalámbricas segmentadas en múltiples SSIDs, La Evaluación comparativa entre protocolo 802.1q e ISL, Firmware y sistemas operativos de distribución libre para configurar y administrar seguridades y calidad de servicio en redes inalámbricas.

GLOSARIO DE TÉRMINOS

ACCESS POINT

Un punto de acceso inalámbrico es un dispositivo de red que interconecta equipos de comunicación alámbrica para formar una red inalámbrica que interconecta dispositivos móviles o con tarjetas de red inalámbricas.

AD HOC

Una red ad hoc inalámbrica es un tipo de red inalámbrica descentralizada.

AFTERBURNER

También conocido como SpeedBooster, SuperSpeed, TurboG, 125Mbps, HSP125, y G+ es una característica integrada en algunos routers que, teóricamente, aumentan el rendimiento mediante el uso de software o Firmware.

ASUS

Es una compañía con sede en Taiwán (República de China), dedicada a la producción de placas base, tarjetas gráficas, dispositivos ópticos, PDA, computadoras portátiles, productos hardware para la gestión de redes, teléfonos celulares, tablets, gabinetes para computadora y sistemas de refrigeración para computadoras.

BINDING

Un binding es una adaptación de una biblioteca para ser usada en un lenguaje de programación distinto de aquél en el que ha sido escrita.

BITORRENT

Protocolo diseñado para el intercambio de archivos punto a punto (peer-to-peer) en Internet. Es uno de los protocolos más comunes para la transferencia de archivos grandes.

BRIDGES

Es el dispositivo de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI.

BRIDGING

Puentes de red es la acción tomada por el equipo de red para crear una red global de cualquiera de dos o más redes de comunicación, o dos o más segmentos de red.

BROADBAND

La banda ancha es una amplia anchura de banda de trasmisión de datos con una capacidad de trasportar simultáneamente múltiples señales y tipos de tráfico.

BROADCAST

La transmisión de datos que serán recibidos por todos los dispositivos en una red. Envía información a todos los dispositivos que se encuentren conectados en la misma red.

BROADCASTING

Difusión es la distribución de audio y/o vídeo de contenido a una dispersa público a través de cualquier medio electrónico medio de comunicación de masas, pero por lo general uno usando el espectro electromagnético.

BROADCOM

Broadcom Corporation es uno de los principales fabricantes de circuitos integrados para comunicaciones de banda ancha de los Estados Unidos.

BUILDROOT

Herramienta que se utiliza para crear el entorno de compilación cruzada (cross-compilation environment) y el sistema de archivos raíz.

BYTES

Es la unidad de información de base utilizada en computación y en telecomunicaciones, y que resulta equivalente a un conjunto ordenado de bits (generalmente 8 bits, por lo que en español también se le denomina octeto).

CONMUTADORES

Dispositivo de red analógico de lógica de interconexión de redes de computadoras.

CHIP

Estructura de pequeñas dimensiones de material semiconductor, de algunos milímetros cuadrados de área, sobre la que se fabrican circuitos electrónicos generalmente mediante fotolitografía y que está protegida dentro de un encapsulado de plástico o de cerámica.

DD-WRT

Firmware libre para diversos routers inalámbricos o WiFi, es muy común observarlo en equipos Linksys WRT54G (Incluyendo los modelos WRT54GL, WRT54GS y WRT54G2).

DIFFSERV

Los Servicios Diferenciados (DiffServ) proporcionan un método que intenta garantizar la calidad de servicio en redes de gran tamaño, como puede ser Internet.

DNSMASQ

Sistema de nombres de dominio (DNS) del promotor de Dynamic host configuration protocol (dhcp) del servidor para pequeñas redes de computadoras, creado como software libre.

DOT1Q

Proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking).

DUPLEX

Término utilizado en telecomunicación para definir a un sistema que es capaz de mantener una comunicación bidireccional, enviando y recibiendo mensajes de forma simultánea.

ETHERNET

Estándar de redes de área local para computadores con acceso al medio por detección de la onda portadora y con detección de colisiones (CSMA/CD).

FASTETHERNET

Estándares de IEEE de redes Ethernet de 100Mbps (megabits por segundo). El nombre Ethernet viene del concepto físico de ether. En su momento el prefijo fast se le agregó para diferenciarla de la versión original Ethernet de 10 Mbps.

FIREWALL

El nombre de una serie de una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

FIRMWARE

Programa informático que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.

FORWARDER

Redirección de puertos, a veces llamado tunelado de puertos, es la acción de redirigir un puerto de red de un nodo de red a otro. Esta técnica puede permitir que un usuario externo tenga acceso a un puerto en una dirección IP privada (dentro de una LAN) desde el exterior vía un router con NAT activado.

GLIBC

Biblioteca estándar de lenguaje C de GNU. Se distribuye bajo los términos de la licencia GNU LGPL.

HALF DUPLEX

Una conexión semi-dúplex (a veces denominada una conexión alternativa) es una conexión en la que los datos fluyen en una u otra dirección, pero no las dos al mismo tiempo.

HANDOVER

Traspaso (también handoff o transferencia) al sistema utilizado en comunicaciones móviles celulares con el objetivo de transferir el servicio de una estación base a otra cuando la calidad del enlace es insuficiente en una de las estaciones.

HOTSPOT

Es un lugar que ofrece acceso a Internet a través de una red inalámbrica y un enrutador conectado a un proveedor de servicios de Internet.

HUB

Concentrador o Ethernet hub, un dispositivo para compartir una red de datos o de puertos USB de una computadora

HYPERWRT

Es una GPL firmware proyecto para el Linksys WRT54G y WRT54GS inalámbricas routers basados en el stock de Linksys firmware.

JFFS2

Sistema de ficheros con soporte para transacciones especializado en memorias Flash, nace como sucesor de JFFS y será sucedido por JFFS3.

KERNEL

Software que constituye una parte fundamental del sistema operativo, y se define como la parte que se ejecuta en modo privilegiado (conocido también como modo núcleo).

LIBPCAP

La implementación del pcap para sistemas basados en Unix se conoce como libpcap.

LINK

Anglicismo correspondiente a 'enlace' e hipertexto a otro documento o recurso.

LINKSYS

Linksys es una empresa estadounidense que fabrica productos de hardware de red, principalmente para los usuarios domésticos y pequeñas empresas.

LOGS

Registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información.

MULTICAST

Es el envío de la información en múltiples redes a múltiples destinos simultáneamente.

NETGEAR

Es una empresa estadounidense fundada en 1996 con sede en Santa Clara, California, especializada en la producción y venta de sistemas de redes para particulares y empresas de tamaño reducido.

NGINX

Es un servidor web/proxy inverso ligero de alto rendimiento y un proxy para protocolos de correo electrónico (IMAP/POP3).

OPENSOURCE

Es la expresión con la que se conoce al software o hardware distribuido y desarrollado libremente. Se focaliza más en los beneficios prácticos (acceso al código fuente) que en cuestiones éticas o de libertad que tanto se destacan en el software libre.

OPENWRT

Es un firmware basado en una distribución de Linux empotrada en dispositivos tales como routers personales.

PLUG AND PLAY

Es la tecnología o cualquier avance que permite a un dispositivo informático ser conectado a una computadora sin tener que configurar, mediante jumpers o software específico (no controladores) proporcionado por el fabricante, ni proporcionar parámetros a sus controladores.

PORT FORWARDING

La redirección de puertos permite que las computadoras remotas se conecten a un computador en concreto dentro de una LAN privada.

PORT TRIGGERING

La activación de puertos es una opción de configuración en un NAT habilitado enrutador que permite a un ordenador central que forma dinámica y automática hacia adelante un puerto específico de nuevo a sí mismo. La activación de puertos abre un puerto entrante cuando el equipo del usuario está utilizando un determinado puerto de salida para el tráfico específico.

REDES MESH

La red inalámbrica mallada es una red en malla (mesh) implementada sobre una red inalámbrica LAN.

RELAY

Es el responsable de reenviar el mensaje a los puertos de salida en función del ID de VLAN y la dirección de destino transportada en el mensaje.

RESILIENT PACKET RING

Resilient Packet Ring (RPR) es relativamente una nueva tecnología de red por el estándar IEEE 802.17 se ha especificado. Es un protocolo de red diseñado específicamente para el transporte optimizada de tráfico de datos a través de fibra óptica anillos fue diseñado.

ROUTING

Encaminamiento (o enrutamiento, ruteo) es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad.

SHUTDOWN

Para apagar o apagar una computadora es eliminar el poder de los componentes principales de una computadora de una manera controlada.

SPANNING TREE PROTOCOL

Es un protocolo de red que asegura un libre de bucles de topología delas redes Ethernet. La función básica de STP es evitar bucles de puente y de la radiación de emisión que resulta de ellos.

SPEEDBOOSTER

Es una herramienta de optimización que nos permitirá aumentar la velocidad de procesamiento de nuestro terminal Android, y limpiar la memoria interna de archivos inútiles que tan sólo estén ocupando espacio, sin proporcionarnos ningún beneficio.

STREAMER

Un dispositivo para transferir datos de los sistemas informáticos en cinta magnética para su archivo.

SUBLAYER

La Interconexión de sistemas abiertos - Modelo de referencia, una subdivisión de una capa determinada, por ejemplo, un grupo conceptualmente completa de los servicios, funciones y protocolos incluidos en la capa dada.

SWITCH

Dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada esta.

TOKEN RING

Una arquitectura de red desarrollada por IBM en los años 1970 con topología física en anillo y técnica de acceso de paso de testigo, usando un frame de 3 bytes llamado token que viaja alrededor del anillo. Token Ring se recoge en el estándar IEEE 802.5. En desuso por la popularización de Ethernet; actualmente no es empleada en diseños de redes.

TRAMAS

Una trama es una unidad de envío de datos. Es una serie sucesiva de bits, organizados en forma cíclica, que transportan información y que permiten en la recepción extraer esta información.

TRUNK

En telecomunicaciones, trunking es un método para un sistema para proporcionar acceso de red a muchos clientes mediante el intercambio de un conjunto de líneas o frecuencias en lugar de proporcionar de forma individual.

UCLIBC

uClibc es una pequeña biblioteca en C diseñada para sistemas con Linux embebido. Es software libre con licencia LGPL.

UNIX

Sistema Operativo portable, multitarea y multiusuario; desarrollado, en principio, en 1969, por un grupo de empleados de los laboratorios Bell de AT&T, entre los que figuran Dennis Ritchie, Ken Thompson y Douglas McIlroy

WEB

Entramado, sistema de documentos (o páginas web) interconectados por enlaces de hipertexto, disponibles en Internet.

WIRELESS

La comunicación inalámbrica es la transferencia de información entre dos o más puntos que no están conectadas por un conductor eléctrico.

WORKING

Estación de trabajo es un computador de altas prestaciones destinado para trabajo técnico o científico. En una red de computadoras, es una computadora que facilita a los usuarios el acceso a los servidores y periféricos de la red.

ZEROSHELL

Es una distribución libre para servidores y dispositivos embebidos o integrados, cuyo objetivo es ofrecer los principales servicios que una WIRELESS LAN requiere.

BIBLIOGRAFÍA

[1.]. **TANENBAUM**, A. S. (2012). *Redes de computadoras, 5ta Ed*. Pearson.

[2.]. **IEEE STANDARDS ASSOCIATION.** (2012). IEEE Std 802.11™-2012. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. USA.

[3.]. **IEEE STANDARDS ASSOCIATION.** (2014). 802®. *Standard for Local and Metropolitan Area Networks: Overview and Architecture*. USA.

[4.]. **IEEE STANDARDS ASSOCIATION.** (2014). IEEE Std 802.1Q™-2014. *Standard for Local and metropolitan area networks—Bridges and Bridged Networks*. USA.

[5.]. **ANDERSEN, E.** (2012). *A C library for embedded Linux*. Retrieved from µ C l i b c: https://uclibc.org/about.html (16 de noviembre de 2015)

[6.]. **BARKER**, K. (2011. *What is control plane and data plane*. Retrieved from The Cisco Learning Network : https://learningnetwork.cisco.com/thread/33735 (16 de noviembre de 2015)

[7.]. **BARTHLE, A.** (2013). *DDWRT - Múltiples SSID con VLAN*. Retrieved from SPICEWORKS : https://community.spiceworks.com/how_to/32549-ddwrt-multiple-SSIDs-with-VLANs (16 de noviembre de 2015)

[8.]. **BUILDROOT**. (n.d.). *Making Embedded Linux Easy*. Retrieved from https://buildroot.uclibc.org/ (16 de noviembre de 2015)

[9.]. **COMUNITY DD-WRT**. (n.d.). *FEATURE OVERVIEW AND CONFIGURATION GUIDE*. Retrieved from http://www.dd-wrt.com/wiki/index.php/%C2%BFQu%C3%A9_es_DD-WRT%3F (16 de noviembre de 2015)

[10.]. **COMUNITY DD-WRT**. (n.d.). *Wiki DD-WRT*. Retrieved from http://www.dd-wrt.com/wiki/index.php/Espanol (16 de noviembre de 2015)

[11.]. **FIREWALL.CX.** (n.d.). *VLAN - ANÁLISIS IEEE 802.1Q PROTOCOLO DE ENLACE TRONCAL*. Retrieved from http://www.firewall.cx/networking-topics/vlan-networks.html (16 de noviembre de 2015)

[12.]. **JÁNOS FARKAS,** S. H. (2014). Software Defined Networking Supported by IEEE 802.1Q. Retrieved from http://www.ieee802.org/1/files/public/docs2014/Q-farkas-SDN-support-0314-v01.pdf (16 de noviembre de 2015)

[13.]. **JMHALEGRE**. (2012,). *CCNP SWITCH 642-813 Official Certification Guide (Part II – Chapter 4.2 VLAN Trunks)*. Retrieved from https://juanmhalegre.wordpress.com/2012/01/12/ccnp-switch-642-813-official-certification-guide-part-ii-chapter-4-2-vlan-trunks/ (16 de noviembre de 2015)

[14.]. **OPENWRT, C.** (n.d.). *OpenWrt Wireless Freedom*. Retrieved from https://wiki.openwrt.org/es/start (16 de noviembre de 2015)

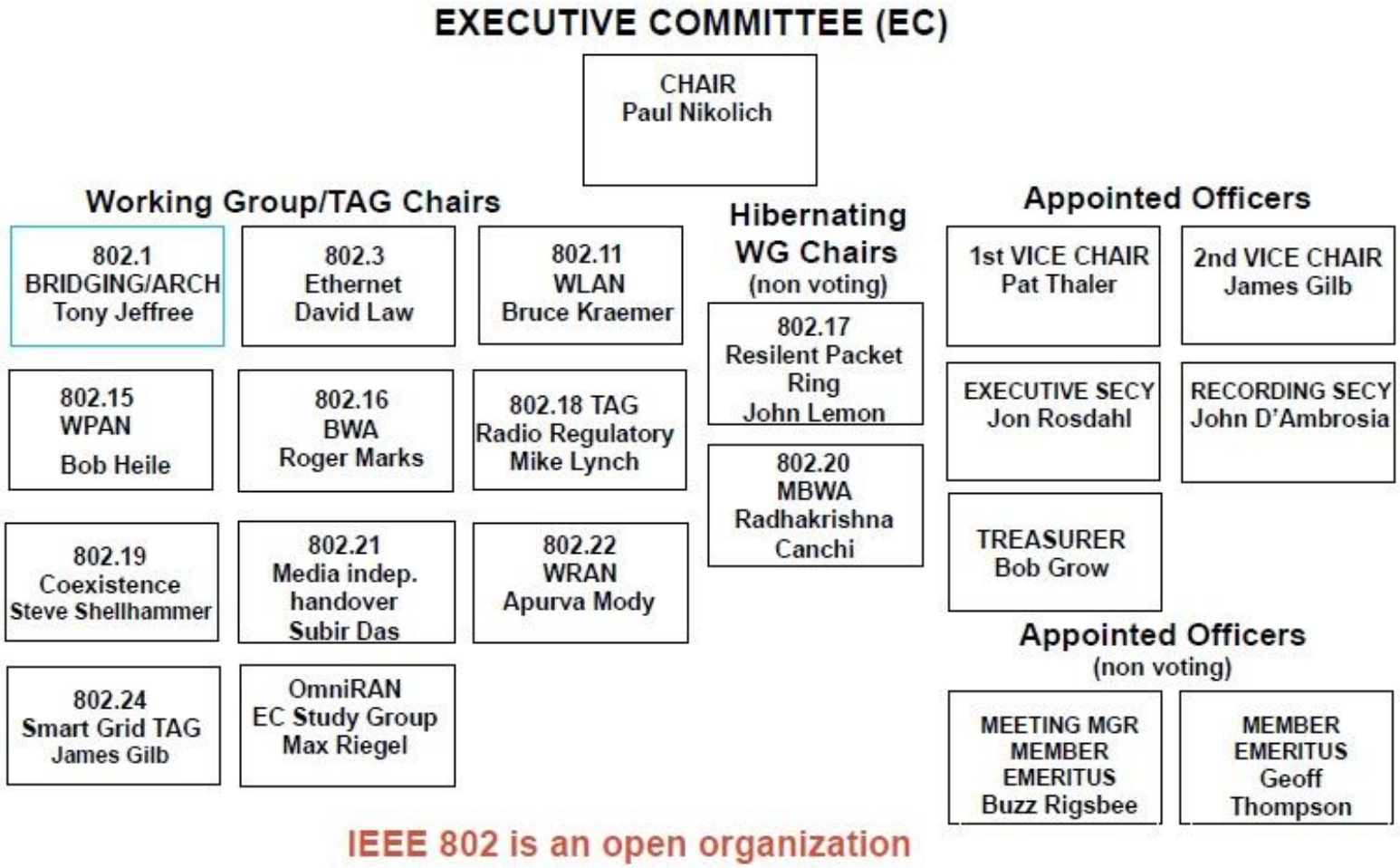
[15.]. **THALER P, N. F.** (2013). *IEEE 802.1Q* . Retrieved from Media Access Control Bridges and Virtual Bridged Local Area Networks: https://www.ietf.org/meeting/86/tutorials/86-IEEE-8021-Thaler.pdf (16 de noviembre de 2015)

[16.]. **SERVICIO MESOAMERICANO SOBRE AGRICULTURA SOSTENIBLE** (SIMAS). (n.d.). *Linksys WRT54G y DD-WRT - Guía práctica.* Retrieved from https://onairosjs.files.wordpress.com/2008/02/wrt54g_guia_practica.pdf (16 de noviembre de 2015)

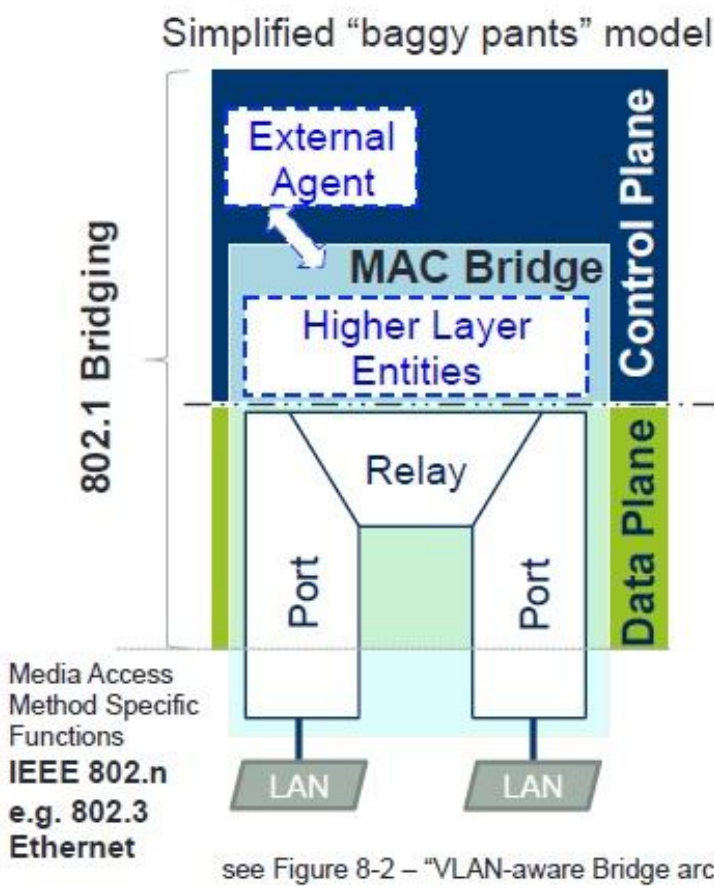
[17.]. **JEFFREE T**. (2011). *The IEEE 802.1 Standards*.

[18.]. **VELÁSQUEZ, K**. a. (2014). *Network Performance Evaluation Based on Three Processes*. Retrieved from Science and Education Publishing: http://pubs.sciepub.com/jcsa/2/2/1/ (16 de noviembre de 2015)

IEEE 802 Organization



Control Plane Separated from Data Plane

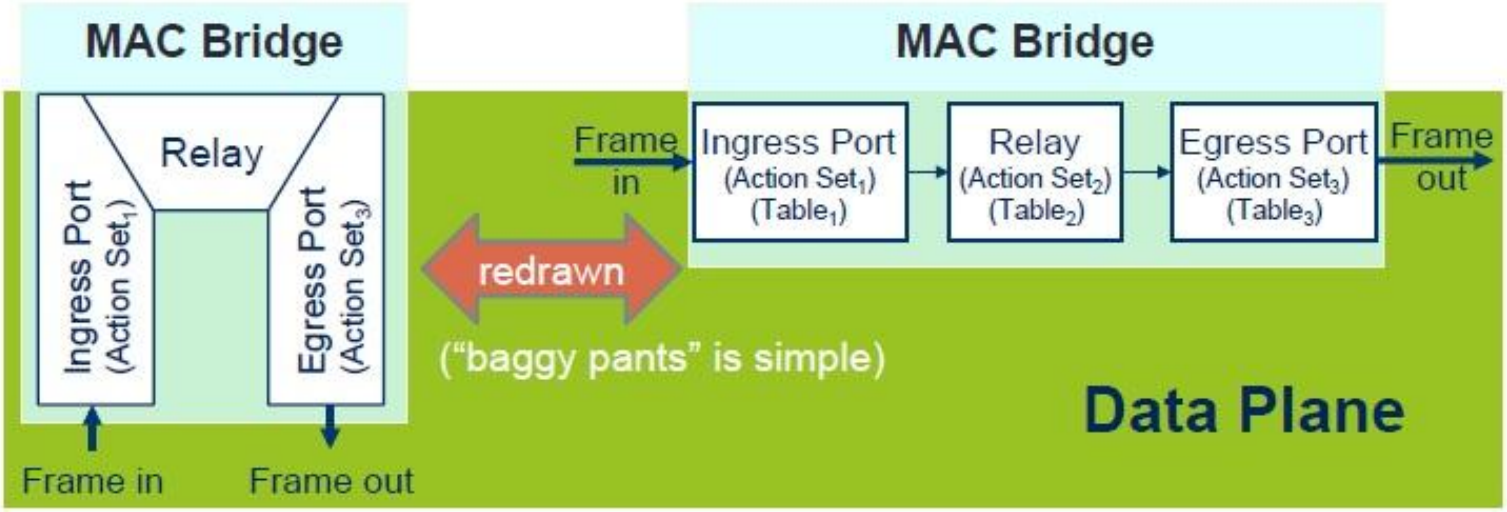


- Control protocols are implemented as Higher Layer Entities
- External Agent may provide control instead of the distributed protocols

- The data plane is comprised of
  - A MAC Relay and
  - At least two ports

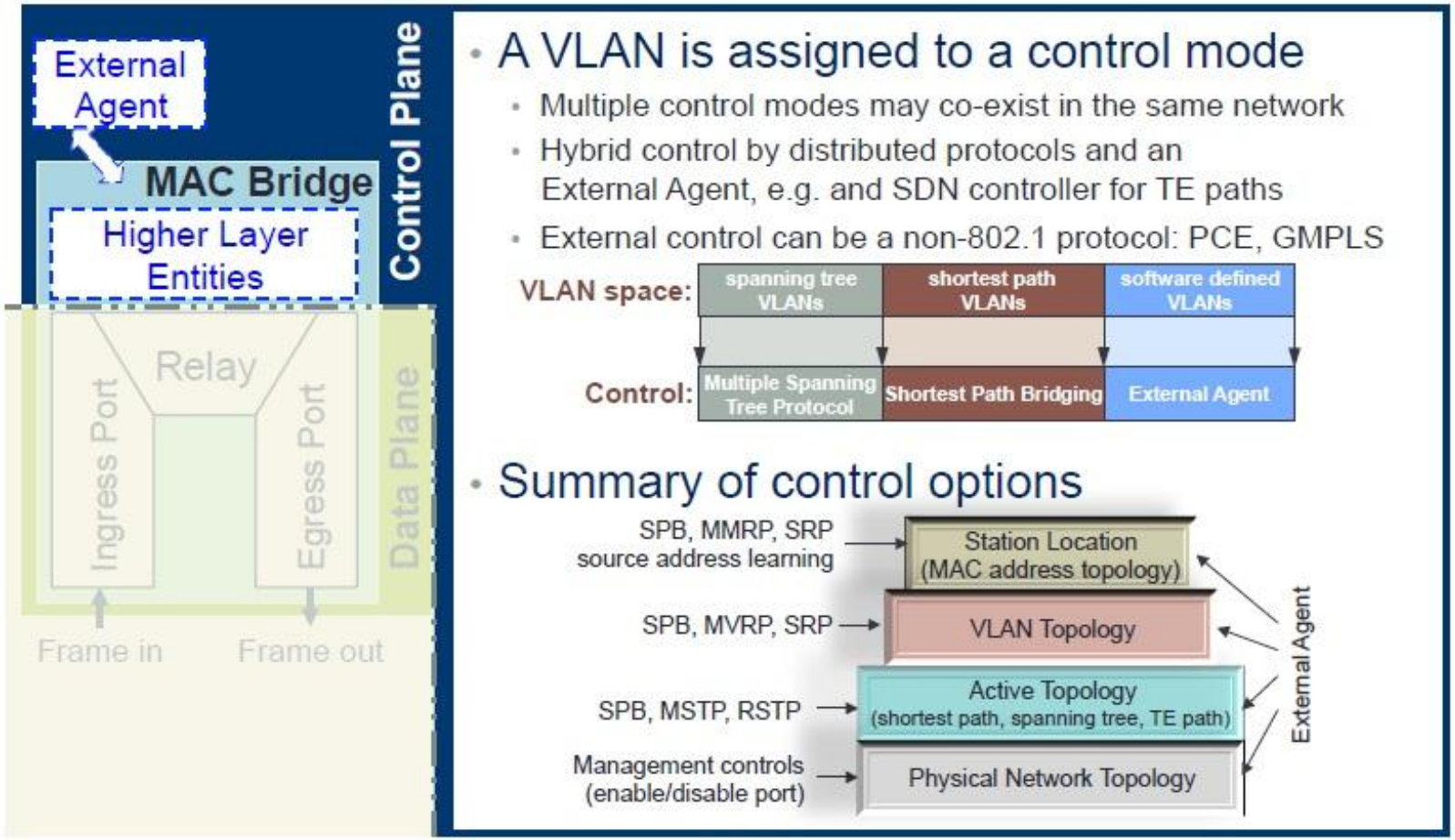
see Figure 8-2 – "VLAN-aware Bridge architecture" of 802.1Q for more details

Data Plane Actions

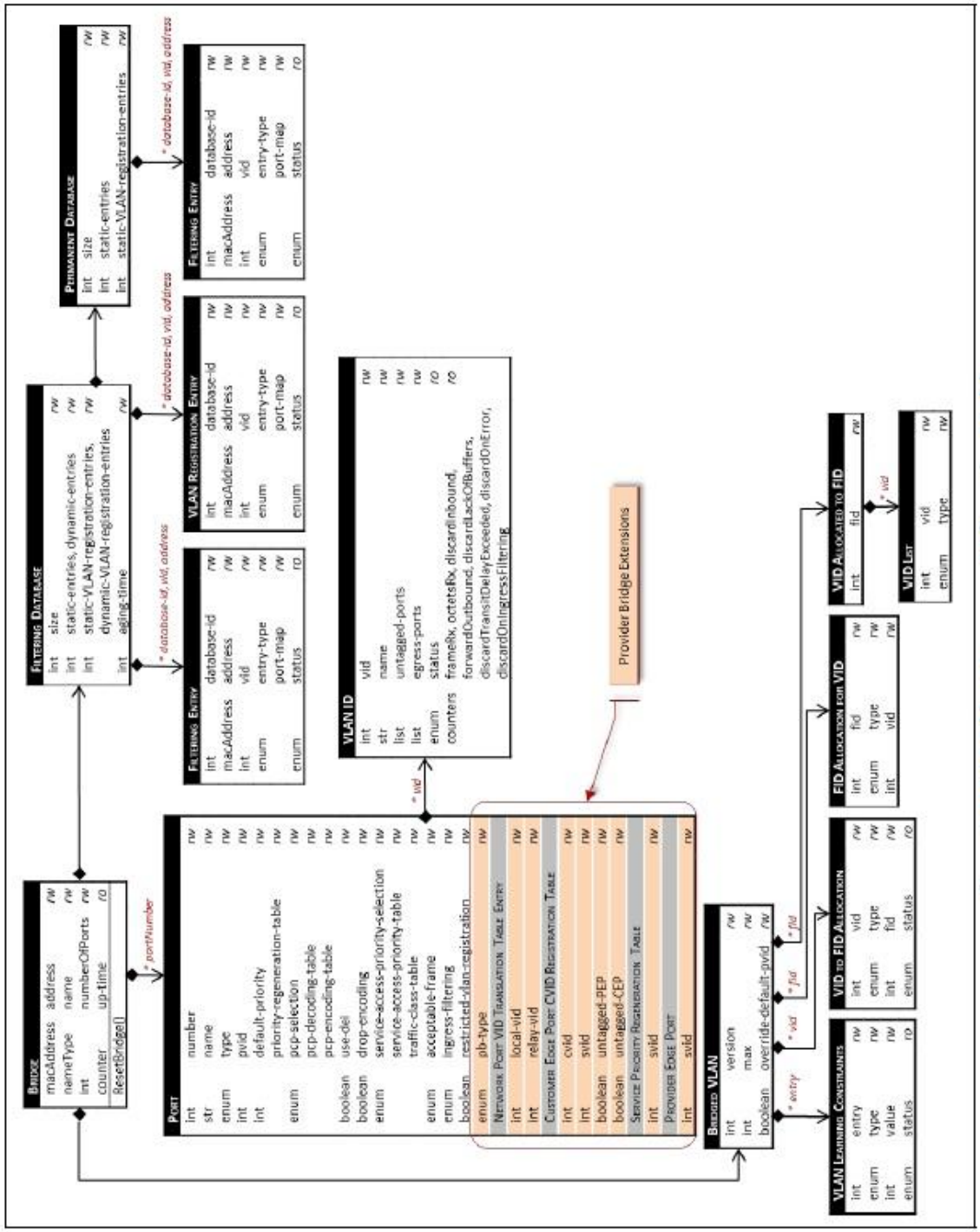


- Ingress Port (Action Set$_1$)
  - Filtering (drop), (un)tagging, VID translation, de/en-capsulation
- Relay (Action Set$_2$)
  - Forwarding, filtering
- Egress Port (Action Set$_3$)
  - Filtering, (un)tagging, VID translation, de/en-capsulation, metering, queuing, transmission selection

Control Plane Overview



Anexo E: Modelos De Datos IEEE 802.1Q



Anexo F: Registro de resultados de conectividad

VLAN CALIDAD		Estadísticas de ping para 192.168.3.3:		
DIAS	ENVIADOS	RECIBIDOS	PERDIDOS	% PERDIDOS
1	10000	9505	495	4,95
2	10000	9491	509	5,09
3	10000	9485	515	5,15
4	10000	9501	499	4,99
5	10000	9459	541	5,41

VLAN CALIDAD		Estadísticas de ping para 192.168.3.2:		
DIAS	ENVIADOS	RECIBIDOS	PERDIDOS	% PERDIDOS
1	10000	9489	511	5,11
2	10000	9505	495	4,95
3	10000	9509	491	4,91
4	10000	9485	515	5,15
5	10000	9501	499	4,99

VLAN CALIDAD		Estadísticas de ping para demás redes		
DIAS	ENVIADOS	RECIBIDOS	PERDIDOS	% PERDIDOS
1	10000	0	10000	100,00
2	10000	0	10000	100,00
3	10000	0	10000	100,00
4	10000	0	10000	100,00
5	10000	0	10000	100,00

VLAN GESTIÓN		Estadísticas de ping para 192.168.1.3:		
DÍAS	ENVIADOS	RECIBIDOS	PERDIDOS	% PERDIDOS
1	10000	9489	511	5,11
2	10000	9554	446	4,46
3	10000	9531	469	4,69
4	10000	9505	495	4,95
5	10000	9500	500	5

VLAN GESTIÓN		Estadísticas de ping para 192.168.2.2:		
DÍAS	ENVIADOS	RECIBIDOS	PERDIDOS	% PERDIDOS
1	10000	9500	500	5,00
2	10000	9498	502	5,02
3	10000	9522	478	4,78
4	10000	9474	526	5,26
5	10000	9515	485	4,85

VLAN GESTIÓN		Estadísticas de ping para demás redes		
DIAS	ENVIADOS	RECIBIDOS	PERDIDOS	% PERDIDOS
1	10000	0	10000	100,00
2	10000	0	10000	100,00
3	10000	0	10000	100,00
4	10000	0	10000	100,00
5	10000	0	10000	100,00

VLAN DIRECCIÓN		Estadísticas de ping para 192.168.4.3:		
DIAS	ENVIADOS	RECIBIDOS	PERDIDOS	% PERDIDOS
1	10000	9479	521	5,21
2	10000	9505	495	4,95
3	10000	9493	507	5,07
4	10000	9493	507	5,07
5	10000	9525	475	4,75

VLAN DIRECCIÓN		Estadísticas de ping para 192.168.4.2:		
DIAS	ENVIADOS	RECIBIDOS	PERDIDOS	% PERDIDOS
1	10000	9458	542	5,42
2	10000	9517	483	4,83
3	10000	9502	498	4,98
4	10000	9507	493	4,93
5	10000	9467	533	5,33

VLAN DIRECCIÓN		Estadísticas de ping para demás redes		
DIAS	ENVIADOS	RECIBIDOS	PERDIDOS	% PERDIDOS
1	10000	0	10000	100,00
2	10000	0	10000	100,00
3	10000	0	10000	100,00
4	10000	0	10000	100,00
5	10000	0	10000	100,00

VLAN DIRECCIÓN A VLAN GERENCIA			Estadísticas de ping para 192.168.2.2:	
DÍAS	ENVIADOS	RECIBIDOS	PERDIDOS	% PERDIDOS
1	10000	9519	481	4,81
2	10000	9494	506	5,06
3	10000	9511	489	4,89
4	10000	9526	474	4,74
5	10000	9473	527	5,27

VLAN DIRECCIÓN A VLAN GERENCIA			Estadísticas de ping para 192.168.2.3:	
DÍAS	ENVIADOS	RECIBIDOS	PERDIDOS	% PERDIDOS
1	10000	9519	481	4,81
2	10000	9494	506	5,06
3	10000	9511	489	4,89
4	10000	9526	474	4,74
5	10000	9473	527	5,27

VLAN GERENCIA		Estadísticas de ping para 192.168.2.3:		
DIAS	ENVIADOS	RECIBIDOS	PERDIDOS	% PERDIDOS
1	10000	9512	488	4,88
2	10000	9496	504	5,04
3	10000	9474	526	5,26
4	10000	9494	506	5,06
5	10000	9486	514	5,14

VLAN GERENCIA		Estadísticas de ping para 192.168.2.2:		
DIAS	ENVIADOS	RECIBIDOS	PERDIDOS	% PERDIDOS
1	10000	9500	500	5,00
2	10000	9498	502	5,02
3	10000	9522	478	4,78
4	10000	9474	526	5,26
5	10000	9515	485	4,85

VLAN GERENCIA		Estadísticas de ping para demás redes		
DIAS	ENVIADOS	RECIBIDOS	PERDIDOS	% PERDIDOS
1	10000	0	10000	100,00
2	10000	0	10000	100,00
3	10000	0	10000	100,00
4	10000	0	10000	100,00
5	10000	0	10000	100,00

VLAN GERENCIA A VLAN DIRECCIÓN			Estadísticas de ping para 192.168.4.2:	
DÍAS	ENVIADOS	RECIBIDOS	PERDIDOS	% PERDIDOS
1	10000	9472	528	5,28
2	10000	9512	488	4,88
3	10000	9482	518	5,18
4	10000	9478	522	5,22
5	10000	9499	501	5,01

VLAN GERENCIA A VLAN DIRECCIÓN			Estadísticas de ping para 192.168.4.3:	
DÍAS	ENVIADOS	RECIBIDOS	PERDIDOS	% PERDIDOS
1	10000	9499	501	5,01
2	10000	9507	493	4,93
3	10000	9498	502	5,02
4	10000	9524	476	4,76
5	10000	9510	490	4,9