

III.

Comunicación entre VLANs del Instituto Hospitalario

3.1 Grupos virtuales y optimización del ancho de banda

3.1.1 Grupos virtuales

Como ya se mencionó en los capítulos anteriores, las VLANs facilitan la administración de grupos lógicos o virtuales de estaciones de trabajo y servidores, para que éstos se puedan comunicar como si estuvieran en el mismo segmento físico de una LAN, lo cual permite limitar el tráfico broadcast y multicast, además de favorecer la administración de mudanzas, adiciones y cambios en los miembros de dichos grupos.

Un grupo virtual o grupo de trabajo en una VLAN, representa a un conjunto de usuarios que comparten un dominio de broadcast en común, independientemente de su ubicación física en la interconectividad de la red.

Mediante el uso de la tecnología VLAN, se pueden agrupar los puertos de un switch, así como los usuarios conectados en grupos de trabajo lógicamente definidos. Un ejemplo de clasificación de usuarios podría ser el siguiente:

- Compañeros de trabajo del mismo departamento.
- Grupos de producción interfuncional, es decir, aquellos formados por integrantes de distintos departamentos o unidades de la organización. A este tipo de equipos se les confiere la responsabilidad de planear y realizar proyectos que exigen coordinación, cooperación y aportaciones considerables de todas las partes relacionadas.
- Grupos autoadministrados, los cuales tienen la autoridad y responsabilidad de tomar decisiones administrativas, a fin de lograr los objetivos del conjunto. La cantidad de autoridad delegada varía de una organización a otra.
- Diferentes grupos de usuarios que comparten la misma aplicación de red o software.

Todos los usuarios del Instituto se asocian en grupos de trabajo, ya sea con uno o diversos switches conectados, al hacer esto las VLANs pueden abarcar infraestructuras contenidas en un solo edificio, edificios conectados entre sí o incluso redes WAN (*Wide Area Network – Redes de Área Amplia*).

En las empresas e instituciones actuales, existe una continua reorganización (aproximadamente del 20 al 40% de los trabajadores por año), esto supone que de la misma forma, la red requiere una continua renovación. Las VLANs ofrecen un mecanismo efectivo para controlar esos cambios y reducir en gran parte el costo asociado con las reconfiguraciones de hubs y routers. Los usuarios en una VLAN pueden compartir el mismo espacio de dirección de red (es decir, la subred IP), sin importar su ubicación.

Por otro lado, es bien sabido que el tráfico de broadcast se produce en todas las redes. La frecuencia de éste depende de los tipos de aplicaciones y servidores empleados, de la segmentación lógica y por supuesto del uso que se le da a los recursos de la red. Aunque las aplicaciones se han perfeccionado durante los últimos años para poder reducir la cantidad de broadcast que se envía, se siguen desarrollando nuevas aplicaciones multimedia que producen un exceso de tráfico.

La implementación de VLANs en el Instituto ha permitido extender la capacidad de los firewalls, desde los routers hasta la estructura de los switches, lo que a su vez proporciona la capacidad de protección contra la problemática de broadcast, que en ocasiones resulta ser potencialmente peligrosa.

Se pueden crear firewalls asignando puertos de switch o usuarios a grupos virtuales de VLAN específicos, ya sea dentro de switches individuales y/o a través de múltiples de estos dispositivos conectados. Así, el tráfico broadcast dentro de una VLAN no se transmite fuera de ella; por el contrario, los puertos adyacentes no reciben el tráfico generado desde otras VLANs. Este tipo de configuración reduce sustancialmente el broadcast producido, liberando de esta forma el ancho de banda para el tráfico real de los usuarios, y reduciendo

a su vez la vulnerabilidad general de la red ante circulación innecesaria de información.

También pueden asignarse VLANs basadas en el tipo de aplicación, lo cual permite agrupar a los usuarios que comparten una utilidad en común, y si fuera el caso de que ésta se encuentre produciendo tráfico no deseado, se puede optar por reunir a los usuarios en un mismo grupo perteneciente una VLAN en específico, y así distribuir la aplicación a través del campus o edificio.

Las cuatro situaciones principales para el uso de los grupos de trabajo, o bien grupos virtuales son las siguientes:

1. *VLAN inhabilitada*: La red no utiliza VLANs, pero es posible configurar el Acces Point para emplear varios SSID, es decir, varios códigos que son incluidos en todos los paquetes de una red inalámbrica para identificarlos como parte de la misma.
2. *VLAN habilitada con una sola etiqueta VLAN ID*: todos los grupos de trabajo pertenecientes a una red virtual usan una etiqueta única de VLAN ID.
3. *VLAN habilitada con etiquetas VLAN ID diferentes*: cada grupo de trabajo emplea una etiqueta VLAN ID distinta, para separarlos y distinguirlos entre sí.
4. *VLAN habilitada con o sin etiquetas*: una mezcla de grupos de trabajo que pueden estar etiquetados y sin etiquetar.

3.1.2 Optimización del ancho de banda

Se puede definir al ancho de banda como la cantidad de información que se envía a través de una conexión de red en un periodo de tiempo dado.

Se sabe que el término que corresponde a la unidad más básica de información es el bit e igualmente se conoce que la unidad básica de tiempo es el segundo; de manera que si se trata de describir la cantidad de información que fluye en un periodo determinado de tiempo, podrían

utilizarse las unidades “bits por segundo” para representar dicho flujo. Bits por segundo es una unidad de ancho de banda.

Por supuesto, si la comunicación en una empresa, institución o incluso en el hogar, se produjera a esta velocidad, la transmisión de información y el desempeño de la red sería muy lento, y por lo tanto, ineficiente para poder realizar las actividades deseadas. La **Tabla 3.1** proporciona un resumen de las diversas unidades de ancho de banda.

Tabla 3.1. Unidades de ancho de banda

Unidad que indica el ancho de banda	Abreviatura	Equivalencia
Bits por segundo	bps	1 bps
Kilobits por segundo	Kbps	1 Kbps = 1 000 bps
Megabits por segundo	Mbps	1 Mbps = 1 000 000 bps
Gigabits por segundo	Gbps	1 Gbps = 1 000 000 000 bps

En el Instituto Hospitalario que se trata en esta propuesta, el ancho de banda que se maneja es el de una red Gigabit Ethernet, también conocida como GigaE, la cual proporciona una capacidad de transmisión de 1 Gigabit por segundo, correspondiente a unos 1000 megabits por segundo de rendimiento.

El contar con este ancho de banda resulta ser de gran beneficio para el Instituto en general, ya que actualmente la necesidad de contar con mayor capacidad para transmitir más y más información ha ido en aumento; ya sea porque cada día existen mayores facilidades para que las personas cuenten con servicio de Internet, o porque las empresas e instituciones hacen uso de nuevas tecnologías que les permiten tener un crecimiento superior.

Los esquemas tradicionales de los servicios han evolucionado y ahora se requiere mayor ancho de banda o capacidad en ambos sentidos de transmisión, es decir, la velocidad con la que los datos pueden ser transferidos de un servidor a un cliente (*downstream*), así como la velocidad a la que se transfieren de cliente a servidor (*upstream*); tal es el caso de Internet. Las nuevas aplicaciones requieren de altas velocidades no solo para la descarga de

información, sino también para los datos que los clientes envían a través de la red.

Lo que es evidente, es que el ancho de banda muchas veces parece insuficiente, ya que el empleo de este recurso es cada día más necesario dado que los servidores y las nuevas aplicaciones empresariales demandan mayor capacidad. Así pues, es imprescindible que cada institución plantee cómo administrar de una mejor manera el ancho de banda disponible, para evitar en la medida de lo posible los inconvenientes de no tener caudal suficiente por el cual transmitir toda la información, sobre todo si la organización se encuentra en plena expansión y se necesitan utilizar nuevas aplicaciones que van a consumir más recursos, por la integración de nuevo personal, adquisición de nuevo equipo, etc.

Las redes virtuales resuelven este problema. Un dominio de broadcast en una buena implementación de red virtual puede desplegarse a un edificio, campus o ciudad, de tal manera que la necesidad de enrutamiento sea minimizada y el tráfico en la red sea mucho más rápido.

La función de las VLANs en el Instituto Hospitalario es restringir los broadcast a los dominios lógicos donde han sido generados.

Pero, independientemente de qué herramientas usar, hay puntos que no deben perderse de vista al momento de afrontar un aspecto crítico como es el ancho de banda del que se dispone. Aunque parezca obvio, al establecer normas en cuanto a este tema, siempre se tienen que tomar en cuenta las necesidades específicas de cada departamento, así como las de los individuos que los componen. Por lo tanto, es importante abordar la asignación de prioridades, que permitan anteponer unos recursos frente a otros, sin afectar las actividades realizadas por las diferentes áreas de trabajo.

Para lograr lo anterior se debe estudiar a fondo cuáles son las necesidades reales de tráfico de la institución y realizar una jerarquía de cada tipo de tráfico en importancia.

3.2 Distribución de VLANs en las áreas del Instituto Hospitalario.

En el Instituto Hospitalario existen diversos departamentos enfocados ya sea a la atención médica, educación, investigación, administración, comunicación, planeación, etc. Sin embargo, cada uno de dichos departamentos se encuentra ubicado en diferentes áreas del Instituto.

El Instituto Hospitalario se divide físicamente en las siguientes áreas:

- Hospitalización
- Urgencias
- Rehabilitación/Ortopedia
- Toma de productos
- Planeación
- Residencia médica
- Administración
- Torre de investigación
- Archivo general
- Banco de Sangre
- Publicaciones
- Casa de máquinas
- Transportes

En la **Figura III.1** se presenta un plano visto desde arriba (azoteas) en el cual se pueden observar las áreas antes mencionadas, que son todas con las que cuenta el Instituto Hospitalario.

Sin embargo, en la **Figura III.2** se muestran más a detalle las divisiones con las que cuenta cada área, el caso mostrado en esta imagen representa la planta baja general, que como se puede observar, al ser un número considerable de subdivisiones, es evidente que la cantidad de usuarios que las ocupan también es abundante. Cada una de estas áreas cuenta con usuarios pertenecientes a diferentes departamentos los cuales son asignados a VLANs específicas.

III. Comunicación entre VLANs del Instituto Hospitalario

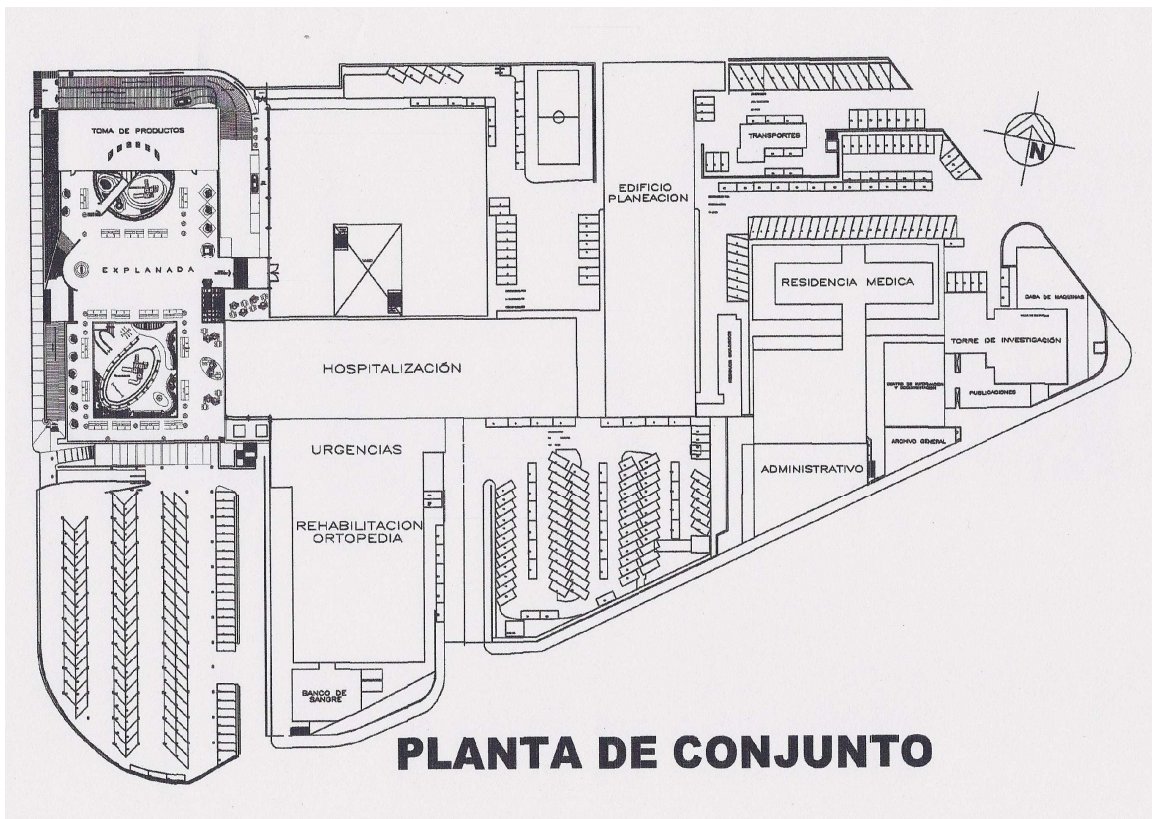


Figura III.1 Planta de conjunto del Instituto Hospitalario

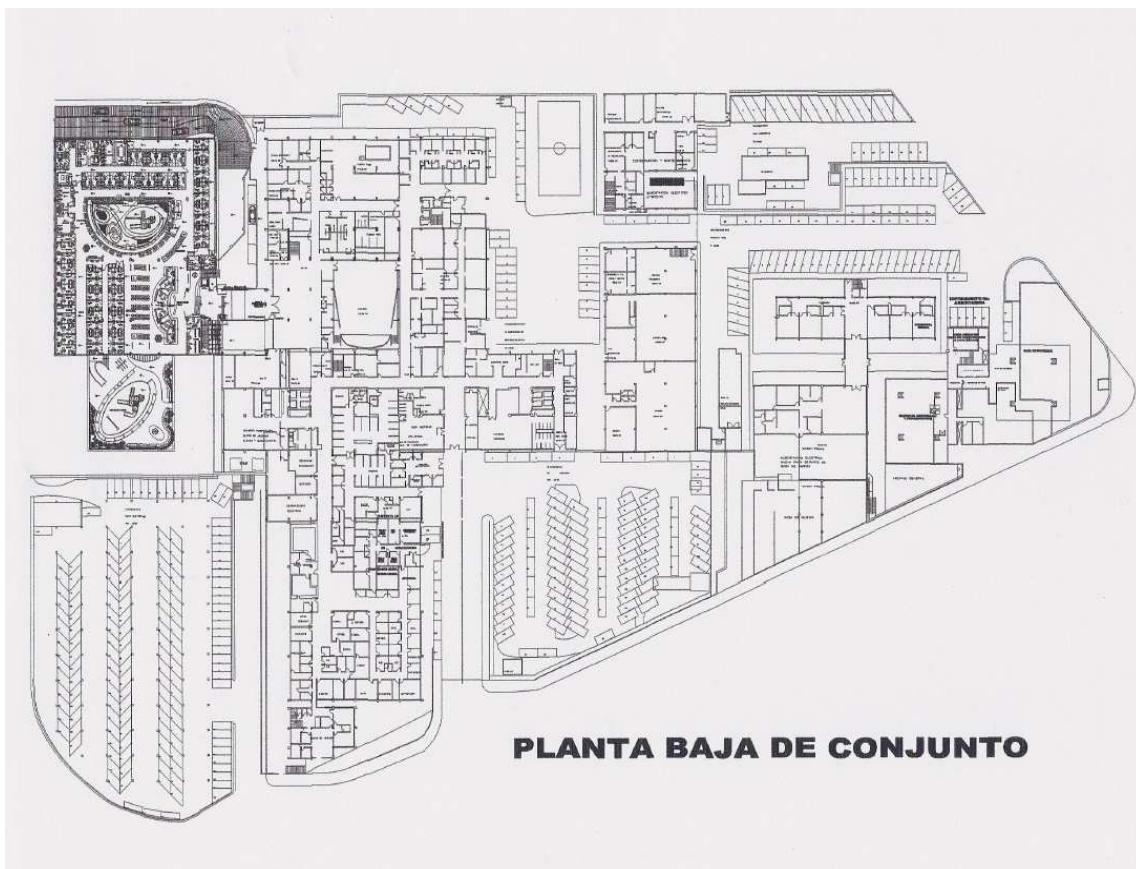


Figura III.2 Planta baja de conjunto del Instituto Hospitalario

III. Comunicación entre VLANs del Instituto Hospitalario

En el Instituto Hospitalario se encuentran implementadas 9 VLANs, cada una identificada por un ID. La **Tabla 3.2** muestra los IDs y nombres de dichas redes virtuales.

Tabla 3.2. VLANs en el Instituto Hospitalario

VLAN	VLAN Nombre
1	Default_VLAN
2	Sistemas
3	Meds
4	InUn
5	Rx-Lab
6	InSalud
7	Maxc
8	IN
9	Pacs

La VLAN 1, “Default_VLAN” es una red virtual que se encuentra predefinida en todos los switches que cuentan con esta tecnología; y en ella se encuentran agregados todos los puertos del dispositivo. A medida que se crean nuevas VLAN y los puertos son asignados a las mismas, éstos serán desconectados de la Default_VLAN.

La VLAN creada para sistemas, es la asignada precisamente, como su nombre lo indica a los sistemas que se emplean en el Instituto Hospitalario, generalmente éstos se enfocan a la administración de recursos financieros, farmacéuticos, mantenimiento, registro de personal e investigación; muchos de los cuales son creados por los programadores de sistemas dentro del Instituto; sin embargo, también se manejan algunos pertenecientes a proveedores externos a la organización. Los usuarios que emplean esta VLAN se encuentran ubicados en diferentes áreas del hospital, como son: torre de investigación, toma de productos, administración, archivo general, etc.

Meds es una VLAN creada exclusivamente para el uso de un solo sistema, el cual consiste en llevar la historia clínica de cada uno de los pacientes que acuden al Instituto, es por ello, que al ser un gran número de personas las

que se registran y asisten diariamente al hospital, existe una VLAN enfocada únicamente para dicho tráfico.

Las VLANs 4,6 y 7, que son InUn, InSalud y Maxc respectivamente, son redes virtuales que proveen servicio de red a los diversos usuarios que laboran en el Instituto, ya sea para consultas de investigación, correos, contacto con otras organizaciones, información de los sistemas, etc. En este caso, los usuarios también se encuentran en distintos edificios, pero al ser considerable la cantidad de personas que requieren el servicio de internet, dicho recurso es repartido entre las 3 VLANs mencionadas.

La VLAN 5, Rx-lab, se encarga de administrar y proveer información entre los usuarios que se encuentran asignados a ella, los cuales son principalmente médicos y/o enfermeras, que hacen uso de rayos “X”, ecocardiografías, ecocardiogramas, ultrasonidos etc.

IN es una VLAN con la cual se están llevando a cabo diversas pruebas, las cuales consisten en reunir todos los segmentos de red del Instituto en una sola red, y así asignar a todos los usuarios IP’s dinámicas, para ser administradas en servidores DHCP.

La VLAN 9 “PACS” es un sistema otorgado por proveedores externos, que consiste en lo último en tecnología para sustituir el uso de radiografías impresas en placas o películas fotográficas. En lugar de analizar las radiografías como se conocen comúnmente, se guardan directamente en un equipo que se encarga únicamente de almacenar las mismas, pero de manera digital, permitiendo realizar un análisis con mayor exactitud y profundidad.

Cuando se comenzó a utilizar esta tecnología en el Instituto (principios de 2009), fue muy difícil para los médicos acostumbrarse a ella, y en diversas ocasiones muchos de ellos se negaban a emplearla, sin embargo, observando las facilidades que puede otorgar, y el avance científico comparado con las antiguas radiografías, su utilidad es totalmente favorable, eficaz y agradable para los usuarios. En la **Figura III.3** puede observarse un ejemplo de dicha

tecnología, en donde un médico analiza estudios en una plataforma de este tipo.



Figura III.3 PACS Plataforma para médicos

Una vez que se ha explicado la asignación de cada VLAN, es necesario aclarar de qué manera se lleva a cabo la conectividad entre ellas. Lo cual se trata en el siguiente punto.

3.3 Tipos de conectividad entre VLANs

En general, cuando una institución hace uso de la tecnología de redes virtuales, es necesario que los dispositivos de los usuarios alcancen los host que no son locales. De la misma forma es evidente, como ya se ha mencionado, que no todos los usuarios se encuentran ubicados en la misma área de trabajo, y por ello dependiendo de las funciones que realicen son asignados a una VLAN específica, por lo tanto, también se requiere que los host pertenecientes a diferentes VLANs puedan comunicarse entre sí.

La conectividad entre VLANs se clasifica en dos tipos:

1. Conectividad lógica.
2. Conectividad física.

La conectividad lógica involucra una conexión única, o un enlace troncal desde el switch hasta el router, dicho enlace admite la implementación de diversas VLANs. Esta topología es también denominada “router en palo” porque existe una sola conexión al router. Sin embargo, hay también diversas conexiones lógicas entre el router y el switch.

De esta manera el tráfico que viaja a través de las diferentes VLANs atraviesa un backbone de capa 2, lo que le permite llegar al router; una vez que esto sucede, el tráfico podrá desplazarse entre las múltiples redes virtuales, por supuesto, este funcionamiento tiene que ver con el protocolo 802.1Q del cual se hablo a detalle en el capítulo anterior, sin embargo se presenta aquí de una manera gráfica para un mejor entendimiento. Posteriormente, el tráfico viaja de vuelta hacia la estación final utilizando el método de envío de capa 2 normal. En la **Figura III.4** se ejemplifica este tipo de conectividad.

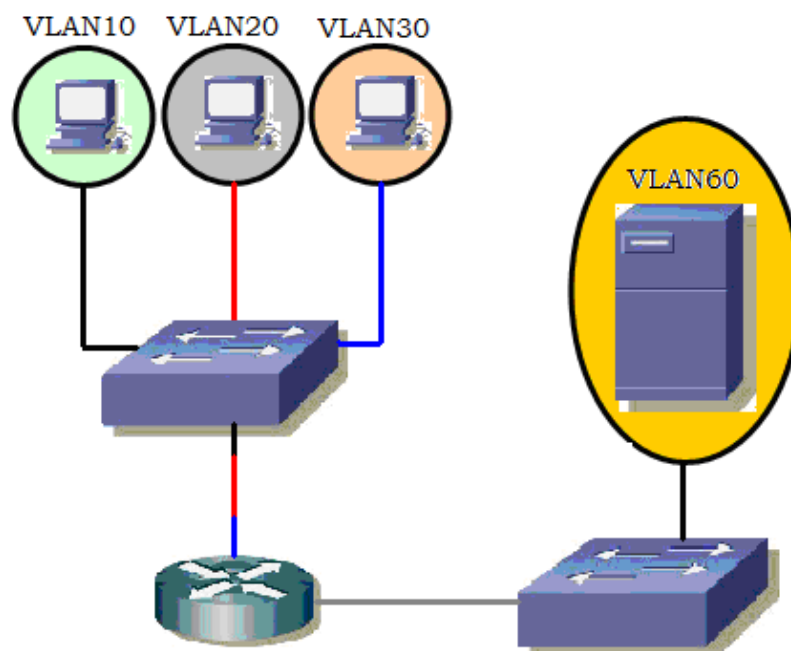


Figura III.4 Un enlace troncal puede admitir varias VLANs

Por otro lado la conectividad física, como su nombre lo indica, implica una conexión física para cada VLAN que se tenga implementada, lo que significa que el número de interfaces físicas debe ser igual al número de VLANs con las que se cuente. Por ejemplo una red con cuatro VLANs requeriría cuatro conexiones físicas entre el switch y el router externo, esto puede visualizarse en la Figura III.5.

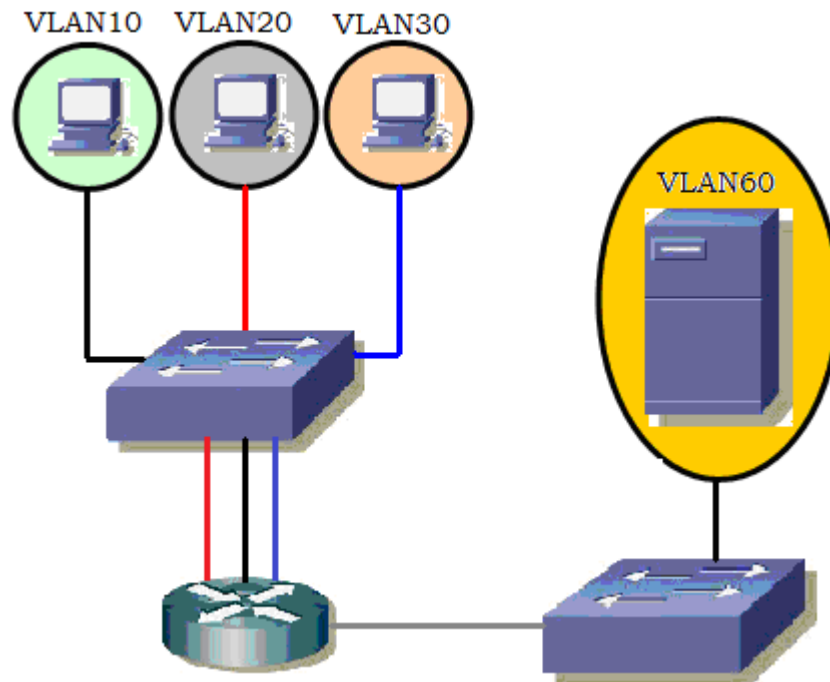


Figura III.5 Se admite una VLAN por interfaz.

Por lo tanto, es conveniente que redes que cuentan con muchas VLANs utilicen enlaces troncales, para asignar más de una red virtual a una sola interfaz de router, el cual podrá admitir varias interfaces lógicas en enlaces físicos individuales.

Lo anterior ayuda a reducir la cantidad de puertos a utilizar, tanto de los routers, como de los switches empleados; y por consiguiente es posible un ahorro en lo que respecta a costos, así como la disminución en la complejidad de la configuración.

3.4 Enrutamiento de VLANs

En un entorno VLAN, los paquetes se conmutan únicamente entre puertos designados para residir en el mismo dominio de broadcast. Las VLANs llevan a cabo peticiones en la red y separación de tráfico en la capa 2. Por consiguiente, la comunicación entre VLANs no puede tener lugar sin un dispositivo de capa 3, como un router, responsable de establecer comunicación entre distintos dominios de difusión.

De manera predeterminada, los usuarios asignados a redes virtuales no podrían comunicarse. Existe únicamente una manera para que éstos puedan hacerlo: El enrutamiento entre VLANs.

Se define al enrutamiento entre VLANs como el proceso que permite reenviar el tráfico de la red desde una VLAN a otra, haciendo uso de un router.

Para llevar a cabo funciones de enrutamiento entre las redes virtuales, deben de considerarse las siguientes circunstancias:

- El router debe de contar con la tecnología necesaria para llegar a todas las VLANs interconectadas, y de esta forma determinar cuáles son los dispositivos finales, incluyendo las redes que están conectadas a alguna VLAN. Cada dispositivo final debe estar dirigido con una dirección IP.
- Todos los routers empleados deben conocer la ruta hasta cada red LAN destino. El dispositivo, una vez configurado, cuenta con la información referente a las redes que se encuentran conectadas directamente, lo que le permite aprender las rutas hacia las redes que por el contrario, no están conectadas de esa forma.
- Debe existir una conexión física en el router para cada VLAN, o en el mejor de los casos, y dependiendo del número de VLANs configuradas, se debe tener una conexión lógica, habilitando un enlace troncal en una conexión física individual.

III. Comunicación entre VLANs del Instituto Hospitalario

Las VLANs están asociadas a subredes IP únicas en la red. Esta configuración de subred facilita el proceso de enrutamiento en un entorno de múltiples VLANs.

Cuando se utiliza un router para facilitar el enrutamiento entre las diferentes redes virtuales, las interfaces del mismo pueden conectarse a VLANs separadas. Los dispositivos en dichas VLANs envían el tráfico a través del router hasta llegar a las otras redes.

Por ejemplo en la **Figura III.6** se muestra como el tráfico de la PC1 en la VLAN 10 está enrutado por medio del router R1 para llegar a PC3 en la VLAN 30.

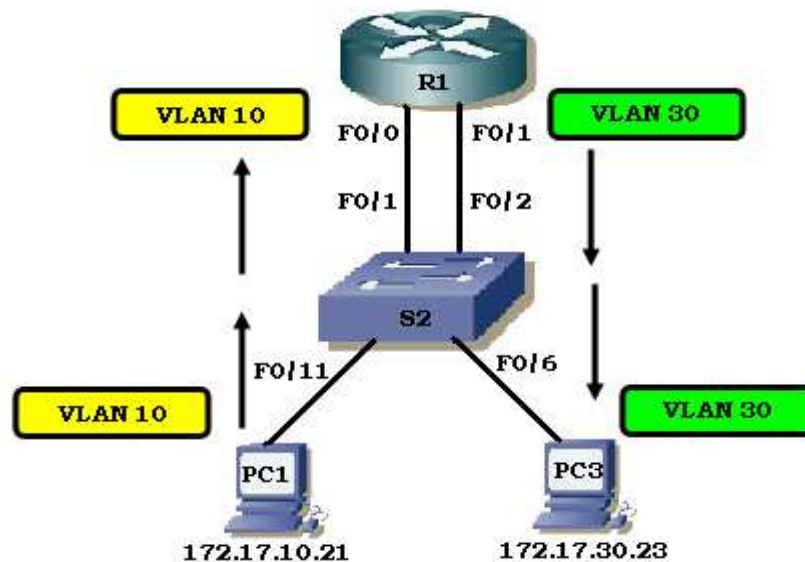


Figura III.6 Enrutamiento entre 2 VLANs

El enrutamiento entre VLANs requiere de múltiples interfaces físicas en los routers y switches.

Sin embargo no todas las configuraciones del enrutamiento entre VLANs requieren de diversas interfaces físicas; ya que hoy en día existe software que ya viene incluido en algunos routers, el cual permite configurar interfaces del dispositivo como enlaces troncales. Esto abre nuevas posibilidades para el enrutamiento a través de VLANs.

Existen también las llamadas subinterfaces, que son múltiples interfaces virtuales asociadas a una interfaz física, las cuales se encuentran configuradas de manera independiente en el router, con una asignación de VLAN y dirección IP, para funcionar en una red específica.

Las subinterfaces están configuradas en diferentes subredes que corresponden a la VLAN estipulada a cada una de ellas, esto facilita el enrutamiento lógico, antes de que la VLAN etiquete las tramas de datos y las reenvíe por la interfaz física.

Algunos switches pueden realizar funciones de capa 3, lo que reemplaza la necesidad de utilizar routers dedicados a realizar el enrutamiento básico en una red, tal es el caso de los switches multicapa.

En cuanto al aspecto económico, resulta menos costoso utilizar subinterfaces, en lugar de interfaces físicas separadas. Por lo tanto si se tuviera un router con un número considerable de interfaces físicas, esto provocaría que cada una de ellas requiriera la conexión a un puerto del switch por separado, lo cual evidentemente se reflejaría en el uso de una mayor cantidad de puertos físicos del dispositivo en cuestión, que bien podrían ser considerados puertos adicionales para ser usados en caso de que se llegue a generar algún cambio importante en la red, o para ocuparlos en la realización de pruebas.

Los puertos de un switch resultan ser un recurso costoso, especialmente en switches de alto rendimiento, como es el caso de algunos utilizados en el Instituto Hospitalario.

El uso de subinterfaces para llevar a cabo el enrutamiento entre VLANs tiene como resultado una configuración física menos compleja que en el caso del uso de interfaces físicas separadas. Esto se debe a que la cantidad de cables que interconectan los switches y routers es menor.

Al disminuir el número de cables empleados, es posible evitar problemas de ubicación y conexiones pertenecientes a enlaces y puertos en un switch determinado.

En la **Tabla 3.3** se muestra una comparación entre una interfaz y una subinterfaz en un router.

Tabla 3.3. Comparación entre interfaz y subinterfaz de un router

Interfaz física	Sub-interfaz
Una interfaz física por VLAN	Una sola interfaz física para múltiples VLANs
No existe contención de ancho de banda	Contención de ancho de banda
Conectado para acceder a través de determinado puerto de un switch	Conectado para establecer un enlace troncal
Más costoso	Menos costoso
Configuración de la conexión física más compleja	Configuración de la conexión física menos compleja

Dado que generalmente las VLANs en el Instituto son interconectadas mediante enlaces troncales en un enlace físico único, resulta más fácil resolver el problema de las conexiones físicas.