

Prácticas de Infraestructura Informática

Bloque 1: Planificación y configuración de la infraestructura de una organización de ejemplo

Sesión 3 - Configuración de la Infraestructura de red

Objetivos

En esta práctica se despliega y configura la infraestructura de red para la organización de ejemplo. Asimismo, durante el desarrollo de la práctica se analiza detenidamente el funcionamiento de las redes virtuales en las plataformas de virtualización. De esta forma, se cumple un doble objetivo.

Introducción: Ethernet y TCP/IP

En el momento actual, en la definición de la arquitectura de red de las organizaciones, se utilizan dos tecnologías de forma sobresaliente, Ethernet y TCP/IP.

Ethernet cubre los niveles físico (1) y de enlace de datos (2) del modelo OSI de comunicaciones.

El objetivo del estándar Ethernet es conectar ordenadores en red local. Así, Ethernet proporciona un conjunto de protocolos que permiten intercomunicar ordenadores que se encuentran en una misma red.

Los dispositivos físicos utilizados para llevar a cabo las comunicaciones siguen (en su inmensa mayoría) el estándar Ethernet. Entre estos dispositivos se encuentran las tarjetas o Interfaces de red (también conocidas como NIC: *Network Interface Card*), los *switches* de comunicaciones y el cableado.

La infraestructura de virtualización de red proporcionada por Hyper-V ofrece un soporte completo a las comunicaciones Ethernet. Para ello, proporciona interfaces de red (virtuales) y switches (virtuales), ambos de tipo Ethernet, así como mecanismos de conexión entre las redes virtuales Ethernet internas a la plataforma de virtualización, y las redes físicas Ethernet externas a la misma.

TCP/IP es un conjunto de protocolos que cubren los niveles de red (3) y transporte (4) del modelo OSI. El objetivo de TCP/IP es interconectar redes. Utilizando estos protocolos, los ordenadores que están en una red local pueden comunicarse con los que están en otras redes locales diferentes. Además, utilizando puentes, unas redes se conectan con otras hasta formar una red de ámbito global como Internet.

En las plataformas Windows, el conjunto de protocolos TCP/IP es el utilizado de forma estándar para llevar a cabo las comunicaciones. Esto quiere decir que todos los servicios de red se montan sobre TCP/IP.

Desarrollo

• Definición de la arquitectura de red de la organización de ejemplo

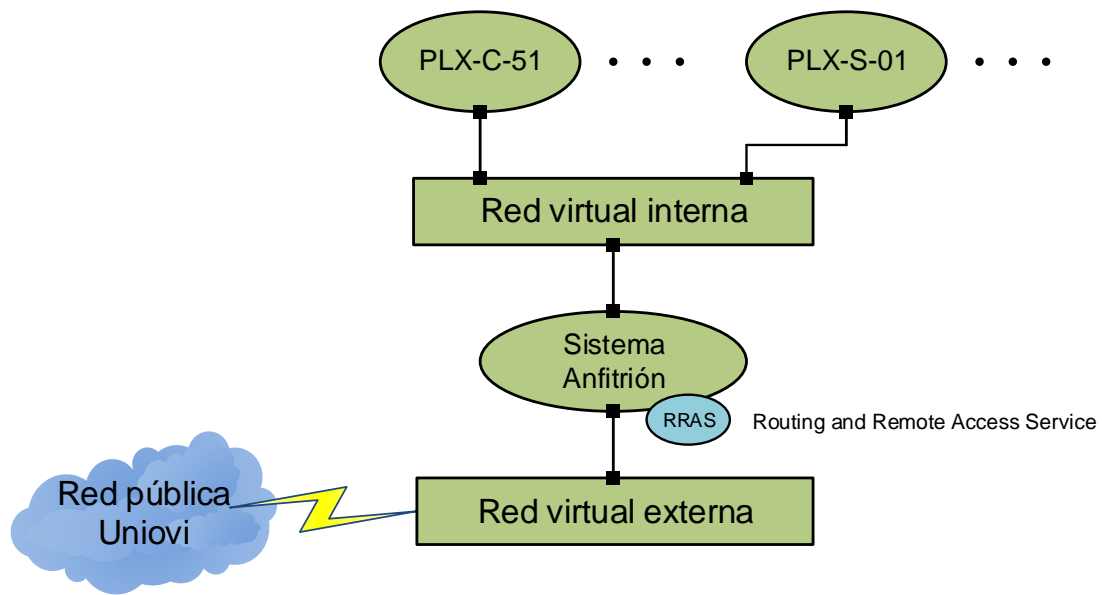


Figura 1. Arquitectura de red de la organización de ejemplo

• Infraestructura de red física: conexiones de red y *switches*

- Los equipos del laboratorio están equipados con varias interfaces de red. Cada interfaz proporciona un puerto de conexión de red. Una interfaz puede ir integrada en la placa base, o bien, implementada en una tarjeta de expansión PCI-E. En este último caso, suele recibir el nombre de NIC (Network Interface Card).
- Para ver el número de interfaces de red de cada tipo, observa el ordenador por la parte trasera. Entonces contesta las preguntas siguientes. No obstante, si tienes dudas, pregúntale a tu profesor.

(1) PREGUNTA. ¿Cuántas interfaces de red integradas hay en el equipo?

(2) PREGUNTA. ¿Cuántas NIC hay en el equipo?

- El sistema operativo muestra una *conexión de red* por cada interfaz de red detectada en el equipo.
- Para comprobar esto, en el sistema anfitrión, *Panel de control -> Redes e Internet -> Centro de redes y recursos compartidos -> Cambiar configuración del adaptador*. En la ventana que se abre se muestran las conexiones de red que se corresponden con las interfaces de red detectadas por el sistema operativo. Debes observar tantas conexiones como interfaces instaladas en el sistema.

(3) PREGUNTA. Indica los nombres de las dos conexiones de red disponibles en el equipo.

- Las interfaces de red físicas se conectan a *switches* físicos. En el caso del laboratorio, hay un *switch* en la parte trasera que da servicio a todos los equipos a través de las bocas de red ubicadas en la pared.

- **Infraestructura de red virtual: conexiones de red y switches**

Conexiones de red

- Exactamente igual que en el sistema físico, en la máquina virtual hay tantas conexiones de red como interfaces de red tenga la máquina virtual.
- En el *Administrador de Hyper-V*, selecciona PLX-S-PRUEBAS-YYY. Abre *Configuración* y en el apartado *Hardware*, observa que hay un *Adaptador de red*. Cierra *Configuración*. Arranca la máquina virtual y en *Conexiones de red*, observa que hay una conexión disponible. El aspa roja indica que la conexión no se encuentra conectada a ninguna red.

(4) PREGUNTA. Indica el nombre de esta conexión.

- Apaga la máquina.
- Vas a agregar una segunda interfaz de red a la máquina virtual. Selecciona *Configuración*. En el apartado *Hardware*, selecciona *Agregar Hardware*. En el cuadro de diálogo de la derecha, selecciona *Adaptador de red* y *Agregar*. En el cuadro de diálogo de la derecha deja las opciones por defecto y *Acepta*. Se crea así un segundo adaptador de red en la máquina virtual. Arranca la máquina y observa que hay una nueva conexión de red disponible.

(5) PREGUNTA. Indica el nombre de la nueva conexión de red.

- Ahora se procederá a dejar las cosas como estaban.
- Apaga la máquina.
- En la configuración de la máquina, elimina el segundo adaptador de red (el que se encuentra en posición inferior de los dos), que es el que se acaba de crear. Para ello, se utiliza el botón *Quitar* y después *Aceptar*. Arranca de nuevo y comprueba que la última conexión de red creada en la máquina (la que contestase en la pregunta 5) ha desaparecido.
- Apaga la máquina.

Switches / conmutadores virtuales

La infraestructura de virtualización proporciona el concepto de *switch virtual*, denominado *conmutador* en la versión española del sistema operativo. El *switch /conmutador* virtual funciona conceptualmente igual que un *switch físico*. La única diferencia es que el *switch virtual* proporciona un número de puertos dinámico. Cuando se conecta a él la interfaz de red de una máquina virtual se crea un puerto en el *switch*, y cuando se desconecta una interfaz, se elimina un puerto.

- Para crear, configurar y, en general, administrar estos dispositivos se utiliza el *Administrador de conmutadores virtuales*, accesible desde el panel *Acciones* del *Administrador de Hyper-V*. Abre el *Administrador de conmutadores virtuales*.
- En la parte izquierda del *Administrador de conmutadores virtuales*, en el apartado *Conmutadores virtuales*, observa la opción *Nuevo conmutador virtual*. Se utiliza esta opción para crear nuevos *conmutadores virtuales*. Al tener seleccionada esta opción, se muestran a la derecha los tipos de conmutadores virtuales que se pueden crear, que se describen a continuación:

Existen tres **tipos de conmutadores**, que son ofrecidos por el *Administrador de conmutadores virtuales* cuando se crea un nuevo conmutador. Estos tipos son los siguientes:

- **Externo:** Está ligado a una interfaz de red física. Permite conectar máquinas virtuales a la red física conectada a dicha interfaz. El equipo anfitrión puede conectarse o no a este conmutador, según se desee o no que el anfitrión se conecte a la red física.
- **Interno:** Sirve para interconectar máquinas virtuales y el equipo anfitrión. No permite canalizar tráfico de red hacia redes físicas.

- **Privado:** Sirve para interconectar exclusivamente máquinas virtuales, por lo que el anfitrión queda desconectado de este conmutador. Este conmutador tampoco permite canalizar tráfico de red hacia redes físicas.

La figura 2 muestra la situación de la plataforma de virtualización antes de crear redes virtuales (se representan solo 3 máquinas, aunque en realidad se van a utilizar 4 máquinas en esta práctica).

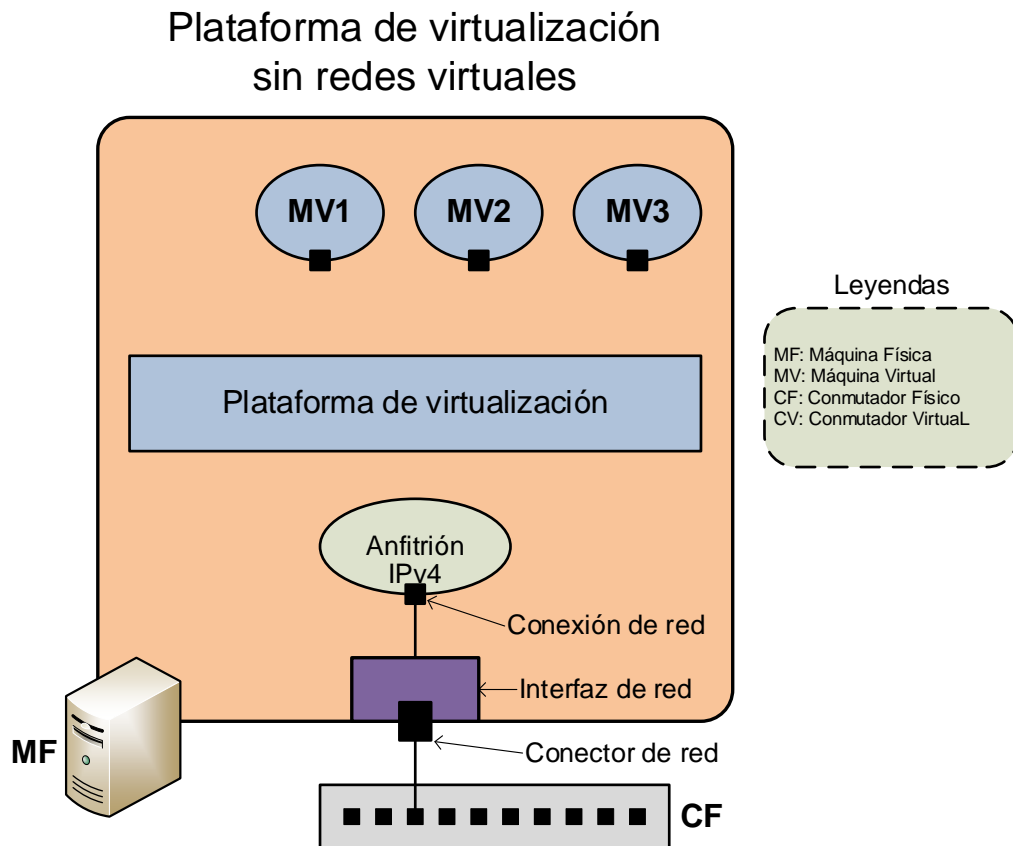


Figura 2. Situación de la plataforma de virtualización antes de crear redes virtuales

Creación de conmutadores virtuales

El objetivo final de esta sesión de prácticas es crear las redes necesarias para conformar la arquitectura de red de la organización de ejemplo (figura 1).

(6) PREGUNTA. Con relación a la figura 1, ¿de qué tipo debe ser el conmutador para *Red virtual interna*? Si tienes dudas, pregúntale a tu profesor.

(7) PREGUNTA. Asimismo, ¿de qué tipo debe ser el conmutador para *Red virtual externa*?

Creación de Red virtual interna

Red virtual interna requiere un conmutador virtual interno. No obstante, para ver la diferencia entre un conmutador interno y un conmutador privado, crearás inicialmente un conmutador privado para esta red, y después, lo transformarás en interno. En todo este proceso observarás si la creación de estos conmutadores tiene algún efecto en la configuración de red del anfitrión.

- En primer lugar, observa que en el sistema anfitrión hay dos conexiones de red, denominadas Ethernet y Ethernet 2. Se trata de las conexiones correspondientes a las interfaces físicas de red del ordenador.

- Crea el conmutador privado. Para ello, *Administrador de conmutadores virtuales -> Privado -> Crear conmutador virtual*. En el campo *Nombre*, escribe *Red virtual interna*. En la sección *Tipo de conexión*, mantén *Red privada*. *Aplica y Acepta*.
- En el anfitrión, abre *Conexiones de red* y observa que no ha habido ningún cambio en las conexiones disponibles.
- La figura 3 muestra la arquitectura de una red virtual privada, basada en un conmutador virtual privado. Como se puede observar, el anfitrión no tiene conexión al conmutador virtual.

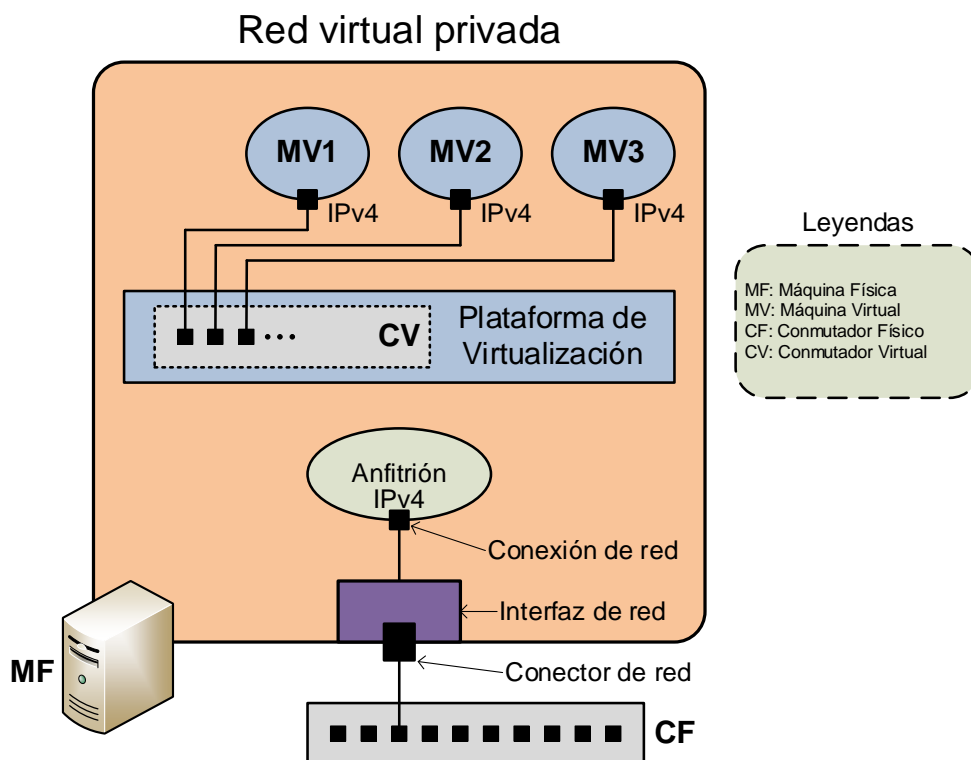


Figura 3. Arquitectura de una red virtual privada

- Como el objetivo final es que *Red virtual interna* sea de tipo interno, ahora transformarás este conmutador virtual para que sea de tipo interno. Para ello, abre *Administrador de conmutadores virtuales* y seleccionar el conmutador *Red virtual interna*. Entonces en la sección *Tipo de conexión* cambiar el tipo de *Red privada* a *Red interna*. *Aplica y Acepta*.
- Abre *Conexiones de red* del anfitrión y observa que se ha creado una nueva conexión.

(8) PREGUNTA. Indica el nombre de dicha conexión

- Con relación al nombre de esta conexión, la 'v' indica que la conexión es virtual (a diferencia de las conexiones sin la 'v', que corresponden a conexiones físicas). Entre paréntesis se indica el conmutador virtual al que se ha conectado la conexión virtual creada. En este caso, dicho conmutador es *Red virtual interna*.
- La figura 4 muestra la arquitectura de una red virtual interna, basada en un conmutador virtual interno. Como se puede observar, el anfitrión tiene una conexión al conmutador virtual (representada en rojo), lo que le permite comunicarse con las máquinas virtuales.

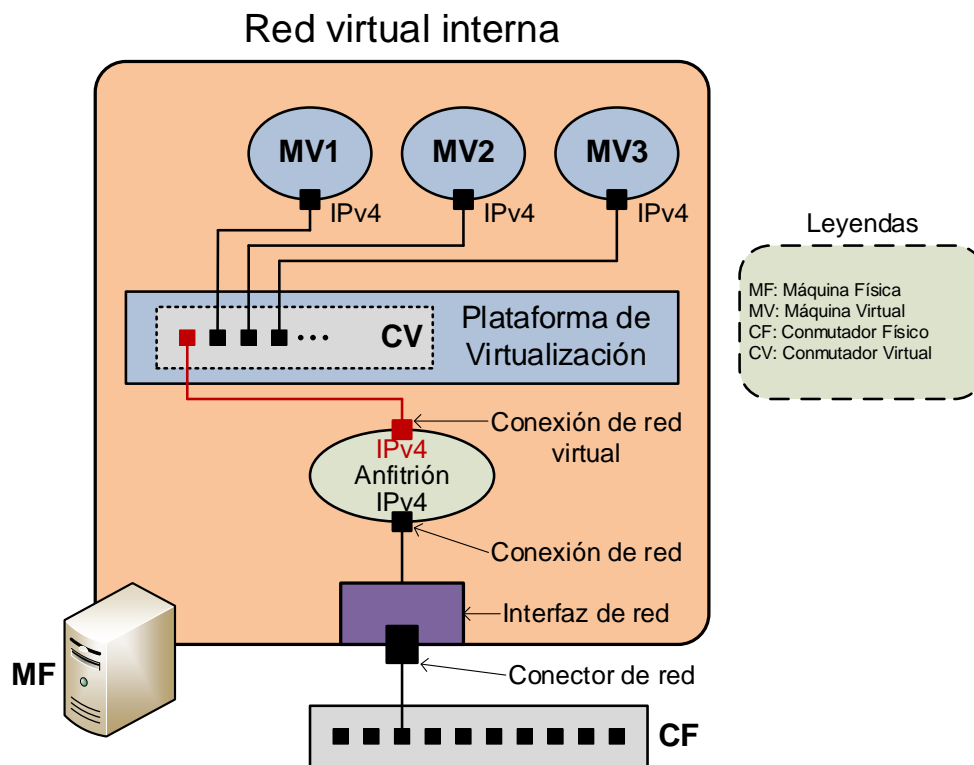


Figura 4. Arquitectura de una red virtual interna

Creación de Red virtual externa

El objetivo de esta red es conectar la infraestructura virtual con la red física. Por consiguiente esta red debe estar basada en un conmutador de tipo *Externo*.

- Un conmutador de tipo externo se asocia siempre con una interfaz de red del equipo anfitrión. El conmutador se comunica con la red externa a través de dicha interfaz de red. Según se vio anteriormente, los ordenadores de los puestos de trabajo tienen dos interfaces, si bien es la interfaz de red integrada en la placa base del equipo la que se utiliza para conectar los ordenadores a la red del laboratorio.
- Antes de crear el conmutador virtual, hay que revisar las conexiones de red disponibles en el anfitrión (cada una de ellas asociada a una interfaz de red), con objeto de determinar cuál de ellas debe asociarse con el conmutador virtual que se va a crear.
- Abre *Centro de redes y recursos compartidos* -> *Conexiones de red*
- Observa las dos conexiones de red físicas disponibles en el equipo (nótese que también hay una conexión virtual). Según se observó anteriormente, una de las dos conexiones físicas corresponde a la interfaz de red integrada en la placa base, y la otra, a una NIC PCI-E.
- Ahora hay que identificar cuál es la conexión de red que se asocia con la interfaz de red integrada en la placa base. Dicha conexión de red es la que está conectada a la red del laboratorio, y, por consiguiente, es la que debe asociarse al conmutador *Red virtual externa*, en el momento de la creación de éste. La conexión de red correspondiente a la interfaz de red de la placa base es fácilmente identificable, ya que al estar conectada, no muestra el aspa roja, que sí se muestra en la otra conexión.

(9) PREGUNTA. Indica el nombre de la conexión de red correspondiente a la interfaz de red integrada en la placa base (o sea, la que está conectada y no muestra el aspa roja).

- Selecciona la conexión de red anterior y abre *Propiedades*.

(10) PREGUNTA. En el campo *Conectar con*, se indica el nombre de la interfaz de red con la que se encuentra asociada esta conexión. Escribe a continuación el nombre de dicha interfaz.

- Observa que las conexiones físicas disponibles en el equipo (*Ethernet* y *Ethernet 2*) se nombran añadiendo números correlativos, o sea, ningún número en el caso de *Ethernet*, y #2 en el caso de *Ethernet 2*. Si hubiera más conexiones, se llamarían *Ethernet 3*, *Ethernet 4*, y así sucesivamente.
- Pon de nuevo tu atención en las propiedades de la conexión de red conectada (la que no muestra el aspa roja). Observa el cuadro de diálogo *Esta conexión utiliza los siguientes elementos*. Entonces contestar la siguiente pregunta:

(11) PREGUNTA. ¿Cuántos elementos se encuentran activados? Si tienes duda, pregúntale a tu profesor.

(12) PREGUNTA. ¿Cuál es la IP pública asociada a esta conexión?

- Una vez revisada la conexión de red que se asociará al conmutador *Red virtual externa*, se procede a la creación de éste. Para ello, *Administrador de conmutadores virtuales* -> *Nuevo conmutador virtual* -> *Externo* -> *Crear conmutador virtual*. En el campo *Nombre*, escribe *Red virtual externa*. Ahora hay que elegir la conexión de red con la que enlazar este conmutador virtual. Esto se elige en la lista desplegable ubicada justo debajo de *Red externa*. Despliega esta lista. Observarás las dos interfaces de red físicas disponibles en el equipo. Selecciona la interfaz integrada en la placa base, o sea, lo que contestaste en la pregunta 10. Mantén activada la casilla de verificación *Permitir que el sistema operativo de administración comparta este adaptador de red*. Esto es esencial para que el sistema anfitrión no pierda su conexión con la red externa. Aplica esta configuración. El sistema avisa de que se puede deteriorar la conectividad de la red. Continúa para aplicar esta configuración. El anfitrión pierde la conexión de red unos instantes, pero enseguida, la conexión vuelve a estar operativa.
- Ahora, observarás los cambios ocurridos en las conexiones de red del anfitrión.
- En *Conexiones de red*, selecciona la conexión asociada a *Red virtual externa*, o sea, *Ethernet 2*, que es la conexión correspondiente a la interfaz *Intel(R) Ethernet Connection (7) I219-LM*. Entonces, abre *Propiedades*. Observa el cuadro de diálogo *Esta conexión utiliza los siguientes elementos*.
- Observarás que, ahora, solo hay dos elementos seleccionados. Uno de ellos es *Controlador de protocolo LLDP de Microsoft*. Este elemento siempre está seleccionado y está orientado al descubrimiento de dispositivos en la red, pero no tiene interés desde el punto de vista de esta práctica. Sin embargo, el otro elemento seleccionado sí es muy importante.

(13) PREGUNTA. ¿Cuál es dicho elemento?

- ¿Qué ha ocurrido con la configuración de la conexión *Ethernet 2*?
Sin tener en cuenta *Controlador de protocolo LLDP de Microsoft*, que siempre está activado, se han desactivado todos los demás elementos de configuración de red salvo uno: *Hyper-V Extensible Virtual Switch*. ¿Qué significa esto? Básicamente significa que dicha conexión deja de ser utilizable por parte del sistema anfitrión y pasa a ser de uso exclusivo de Hyper-V. Éste utiliza dicha conexión para enlazar el conmutador virtual externo con el conmutador físico al que se encuentra conectada la interfaz física asociada al conmutador virtual externo, según se representa en la figura 5, en color verde. Así los conmutadores CV y CF quedan enlazados formando una misma LAN. De esta forma, cualquier máquina virtual que se conecte a CV se conecta a la misma LAN a la que pertenece CF, y por tanto, a la red física.

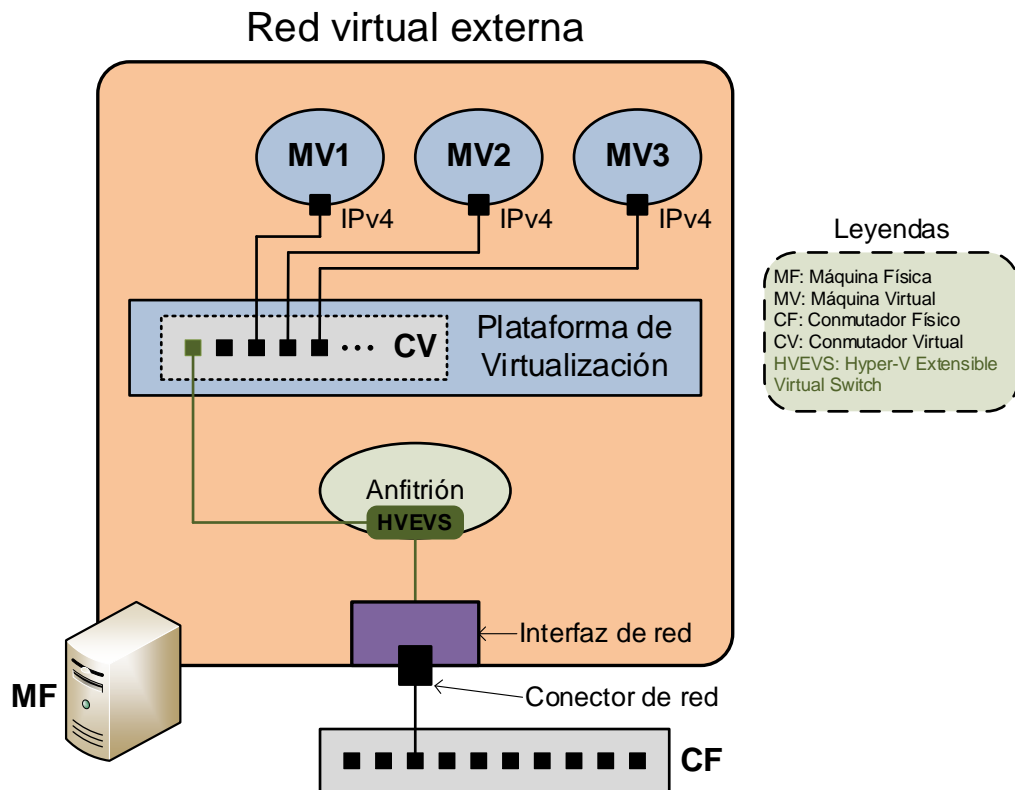


Figura 5. Arquitectura de una red virtual externa

Por otra parte, al crear *Red virtual externa*, has mantenido activada la casilla de verificación *Permitir que el sistema operativo de administración comparta este adaptador de red*. Esto hace que se cree una conexión virtual en el anfitrión, conectada al conmutador *Red virtual externa*.

- Retorna a conexiones de red para comprobar que se ha creado dicha conexión.

(14) PREGUNTA. ¿Cuál es el nombre de esta conexión?

- Abre las propiedades del protocolo TCI/IP de esta conexión y observa que son las siguientes:
 - *IP*: 156.35.151.XXX (donde XXX es el número de identificación del equipo anfitrión).
 - *Máscara de subred*: 255.255.255.0.
 - *Puerta de enlace*: 156.35.151.205
 - *DNS preferido*: 156.35.14.2

Se comprueba que esta conexión virtual ha heredado la configuración IP de la conexión física correspondiente, o sea, del puerto denominado *Ethernet2*.

- Comprueba que el anfitrión se mantiene conectado a la red externa. Para ello, abre una consola de comandos y haz *ping* al DNS de Uniovi (156.35.14.2).
- La figura 6 representa la conexión del anfitrión a la red externa, mediante la conexión virtual creada a tal efecto.

Conexión de Anfitrión a Red virtual externa

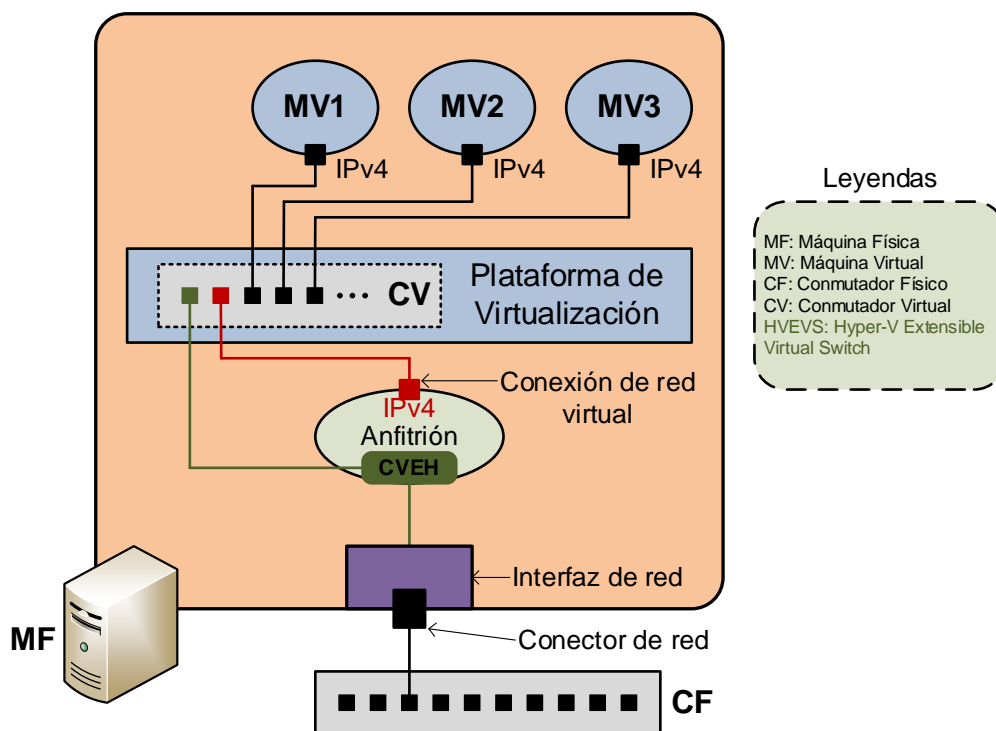


Figura 6. Conexión de anfitrión a red externa

• Conexión de máquinas virtuales a redes virtuales

Conectar una máquina virtual a un conmutador virtual es conceptualmente idéntico a conectar una máquina física a un puerto de un conmutador físico.

En este apartado se van a utilizar 4 de las máquinas virtuales creadas hasta este momento: PLX-S-01, PLX-S-02, PLX-C-51 y PLX-C-52.

- Comenzarás comprobando que las máquinas virtuales no se encuentran conectadas a ninguna red. Para ello, selecciona cada máquina, y en cada máquina seleccionada elige *Configuración* (en el panel de acciones), selecciona el *Adaptador de red* y en el campo *Conmutador virtual* debe mostrarse la opción *No conectado*.

Conexión de servidores a Red virtual interna

Se empezará conectando las máquinas PLX-S-01 y PLX-S-02 a *Red virtual interna*. Después se configurará el protocolo TCP/IP de sus conexiones de red y se probará que se comunican.

- Arranca PLX-S-01. Observa que el icono de red de la barra de tareas indica el estado de desconexión mediante el aspa roja. Si abres el icono, observarás que el sistema indica *No está conectado*. Esto es idéntico a un puerto de red físico desconectado.
- Usando el *Administrador de Hyper-V*, conecta la interfaz de red de PLX-S-01 a *Red virtual interna*. Recuerda que esto se lleva a cabo seleccionando el adaptador de red, y en el campo *Conmutador virtual*, seleccionado la red deseada (*Red virtual interna*, en este caso). Retorna, a continuación, a la máquina virtual y observa que el aspa roja ha desaparecido, debido a que el sistema operativo detecta que hay conexión de red.
- Conecta la interfaz de red de PLX-S-02 a *Red virtual interna* y arranca la máquina. Observa que el icono de red de la barra de tareas NO muestra el aspa roja, lo que significa que Sí hay conexión a una red. No obstante, el signo de exclamación amarillo en el icono de red de ambas

máquinas indica que no hay acceso a Internet. Esto se debe a que, de momento, la red aún no está configurada para proporcionar acceso a Internet.

- El siguiente objetivo es conectar los servidores entre ellos. Para conseguir esto, hay que configurar el protocolo TCP/IP en las conexiones de red de ambas máquinas.
- En PLX-S-01 abre *Conexiones de red* y, después, *Ethernet* -> *Propiedades* -> *Protocolo de internet (v4)* -> *Propiedades*. La conexión está configurada para obtener la IP dinámicamente, pero no puede obtenerla porque no hay un servidor DHCP en esta red. Entonces hay que configurar la conexión con una IP estática.
- Hay que asignar a la conexión de red una dirección IP y una máscara de subred.

Hay dos posibilidades: utilizar DIRECCIONES PÚBLICAS O PRIVADAS. Una dirección pública es una dirección única de Internet. Con una dirección pública y un enrutamiento adecuado el ordenador sería directamente visible y accesible en Internet. Para asignar una dirección pública, hay que tenerla, y estas direcciones escasean. En estas prácticas, se va a trabajar en una red interna, así que no tiene mucho sentido usar direcciones públicas. Por lo tanto, se utilizarán direcciones privadas. Por convenio, se han definido 3 rangos de direcciones para redes privadas. En estas prácticas se utilizará el rango correspondiente a la subred 192.168.0.0/24.

- En la configuración del protocolo TCP/IPv4, asigna a esta máquina la dirección 192.168.0.1, con la máscara 255.255.255.0.

(15) PREGUNTA. ¿Tiene sentido configurar el campo *Puerta de enlace predeterminado*? Justifica tu respuesta. Si tienes dudas, pregúntale a tu profesor.

- Tampoco será necesario configurar el DNS, ya que, de momento, desde la red interna no es posible alcanzar ningún servidor DNS.
- Guarda la configuración IP de PLX-S-01.
- Pasa tu atención a PLX-S-02. Configura su conexión de red con la dirección IP 192.168.0.2 y la máscara 255.255.255.0. Fíjate que esta dirección se encuentra en la misma subred que la de PLX-S-01. Esta es la condición indispensable para que ambas máquinas se puedan comunicar.

Prueba de conexión

Para ello se utiliza el comando ping, que se ejecuta desde la consola de comandos.

- En PLX-S-01 haz *ping* a la dirección IP de PLX-S-02. Comprueba que no hay respuesta. El comando *ping* indica la falta de respuesta mediante alguno de los mensajes siguientes: *“Host de destino inaccesible”* o *“Tiempo de espera agotado para esta solicitud”*.

La explicación de la falta de respuesta es debida al *firewall*, que bloquea totalmente el acceso al sistema. Para recibir paquetes de *ping*, que utiliza el protocolo ICMP (*Internet Control Message Protocol*), hay que abrir los puertos y protocolos necesarios en el *firewall*.

- En PLX-S-02 se procede a establecer una regla de entrada en el *firewall* para permitir las solicitudes de *ping*. Para ello, *Herramientas administrativas* -> *Windows Defender Firewall con seguridad avanzada*. Entonces, selecciona *Reglas de entrada*. Botón derecho sobre *Reglas de entrada*. Selecciona *Nueva regla*. Se abre el *Asistente para nueva regla de entrada*. En *Tipo de regla*, selecciona *Personalizada*. En *Programa*, selecciona *Todos los programas*. En *Protocolo y puertos*, en el campo *Tipo de protocolo*, elige *ICMPv4*. En *Ámbito*, elige *Cualquier dirección IP* en ambos cuadros de diálogo. En *Acción*, selecciona *Permitir la conexión*. En *Perfil*, selecciona los tres perfiles (*Dominio*, *Privado* y *Público*), y, por último, en *nombre*, debes indicar un nombre para la nueva regla. Un nombre apropiado puede ser *Permitir ICMPv4*. Finalmente la nueva regla aparecerá activada en la fila superior del panel de reglas de entrada. A partir de este momento *ping* responderá satisfactoriamente.

- En PLX-S-01 se comprueba que *ping* responde con PLX-S-02.
- En PLX-S-01, en su *firewall*, se genera una regla idéntica a la anterior.
- Se comprueba en PLX-S-02 que *ping* responde con PLX-S-01.

Si bien las conexiones de red ya han sido configuradas en PLX-S-01 y PLX-S-02, el icono de red de la barra de tareas en ambas máquinas sigue mostrando la exclamación amarilla (red no identificada). Esto se debe a que las máquinas aún no tienen salida a Internet.

Conexión de clientes a *Red virtual interna*

- Repetir todo lo anterior con las máquinas PLX-C-51 y PLX-C-52.
- Las interfaces de red de ambas máquinas deben conectarse a *Red virtual interna*.
- En el caso de estos equipos, las direcciones IP a utilizar son la 192.168.0.51 y la 192.168.0.52.
- Habilitar las reglas necesarias en los *firewall* de ambos equipos. NOTA: En Windows 11, la carpeta de *Herramientas administrativas* ha pasado a llamarse *Herramientas de Windows*. En esta carpeta encontrarás, entre otras muchas herramientas, un enlace a *Windows Defender Firewall con seguridad avanzada*.
- Comprueba que *ping* responde de forma satisfactoria entre ambos equipos y también hacia los servidores.

Configuración de la conexión *vEthernet (Red virtual interna)* del anfitrión

- Repasa las conexiones de red del sistema anfitrión. Recuerda que *vEthernet (Red virtual interna)* es una conexión de red conectada a *Red virtual interna*.
- Con objeto de poder hacer las necesarias pruebas de conexión, configura el firewall del anfitrión para permitir el acceso a él mediante *ping*.
- Configuración y prueba de *vEthernet (Red virtual interna)*
 - Configura el protocolo TCP/IP
 - IP: 192.168.0.100
 - Máscara: 255.255.255.0
 - Utilizando *ping* comprueba la conexión entre PLX-S-01 y el sistema anfitrión. Haz la comprobación en ambos sentidos.
 - Comprueba también la conexión entre PLX-C-51 y el anfitrión.
- En este punto el anfitrión se comunica con los equipos de *Red virtual interna*.

• Configuración del sistema anfitrión como enrutador NAT

En este momento, las máquinas virtuales pueden comunicarse entre sí y con el sistema anfitrión mediante *Red virtual interna*. Sin embargo, las máquinas virtuales no tienen conexión con la infraestructura de red pública, ya que para ello, deben pasar por *Red virtual externa*, y en este momento, no tienen conexión con esta red.

Para establecer la conexión entre las máquinas virtuales y *Red virtual externa* se va a configurar un enrutador NAT en el sistema anfitrión. Para ello será necesario establecer un determinado rol, que se verá a continuación.

- El despliegue de un rol requiere habitualmente realizar transformaciones significativas en el software del servidor. Debido a ello, antes de desplegar el rol en el anfitrión, resultará conveniente apagar todas las máquinas virtuales que se encuentran en ejecución en el equipo.
- APAGA todas las máquinas en ejecución (PLX-S-01, PLX-S-02, PLX-C-51 y PLX-C-52).

Roles, servicios de rol y características

- En este punto, pon tu atención en el sistema anfitrión (todas la MV están apagadas).

- Para gestionar roles, servicios de rol y característica, se utiliza el *Administrador del servidor*, al que se accede mediante un enlace en el menú *Inicio* o bien desde *Herramientas administrativas*. En el anfitrión, abre *Administrador del servidor*. En el panel izquierdo, selecciona *Servidor local*. Observa la información obtenida. Pon tu atención en la sección *Propiedades*. Se ve el nombre del equipo, grupo de trabajo, conexiones de red, etc. También puede observarse información sobre el sistema operativo instalado, hardware del equipo, etc.
- En la parte inferior del panel informativo se encuentra la sección *Roles y Características*. Ordena por *Tipo*, para que los roles instalados sean fácilmente localizables.

Un ROL instala en el servidor un conjunto de componentes software que proporcionan al mismo un grupo de funcionalidades que llevan una determinada orientación. Por ejemplo, preparar al servidor como servidor de ficheros, como servidor de funciones de red, como controlador de dominio, etc. Alrededor de un rol puede haber muchas funcionalidades diferentes, como se verá más adelante. Las CARACTERÍSTICAS son funciones simples.

- Comprueba que en el momento actual hay dos roles instalados, *Hyper-V* y *Servicios de archivos y almacenamiento*. De todos los roles, Hyper-V es el más especial, ya que cuando se instala genera una transformación total en el sistema.
- Vas a analizar los roles que hay disponibles. En el menú superior, pulsa en *Administrar* y entonces en *Agregar roles y características*. Se abre el asistente correspondiente. En tipo de instalación, elige *Instalación basada en características o en roles*. En *Selección del servidor*, elige el servidor actual. Entonces se muestran los *roles de servidor*, como por ejemplo Hyper-V, servicios de archivos y servidor web. Para mostrar el concepto de *Servicios de rol*, despliega el rol *Servicios de archivo y almacenamiento*. Debajo de este rol se ven todos los servicios que lo integran, que pueden desplegarse por separado. Pulsa en *Siguiente* sin seleccionar nada, ya que no se va a instalar ningún rol, ni servicio de rol adicional a los ya instalados.
- En este punto el asistente se encuentra en el apartado *Características*. Observa las características que se muestran. Se trata de funciones simples. Por ejemplo, una característica es *Asistencia remota*. La instalación de esta característica habilita al equipo para que un usuario externo se pueda conectar al equipo y mostrar al usuario local cómo realizar cualquier operación o procedimiento. *Cancelar* para abandonar el asistente.

Instalación del rol *Acceso remoto*

Los servicios de enrutamiento, que incluyen la funcionalidad de *router* NAT, se instalan mediante el rol *Acceso remoto*. Para instalar este rol, debe hacer lo siguiente:

- Abre *Agregar roles y características*. En *Roles de servidor*, selecciona *Acceso remoto*. Fíjate que al seleccionar este rol, debajo de *Características* se inserta una nueva entrada con el nombre de este rol, y debajo de la misma, se inserta una entrada más indicando *Servicios de rol*. Esto significa que el rol que se va a desplegar está formado por varios servicios de rol que habrá que configurar en los siguientes pasos del asistente. Pulsa *Siguiente* para pasar a *Características*. Pulsa *Siguiente* para llegar a *Acceso remoto*. En este punto se proporciona una ventana informativa sobre las funcionalidades proporcionadas por este rol. Pulsa *Siguiente* para llegar a *Servicios de rol*. El asistente muestra los servicios de rol que integran el rol *Acceso remoto*.

(16) PREGUNTA. Indica los servicios de rol que forman el rol *Acceso remoto*.

- | |
|----|
| 1) |
| 2) |
| 3) |

- El servicio de rol que se requiere es *Enrutamiento*, pero éste depende de *DirectAccess* y *VPN (RAS)*, por lo que es necesario agregar ambos. Comienza agregando *DirectAccess* y *VPN (RAS)*. El asistente indica que se necesita agregar un conjunto de características. Esto es bastante habitual. Un rol o servicio de rol necesita características para poder desplegarse. Mantén seleccionada la casilla de verificación *Incluir herramientas de administración (si es aplicable)*, y

pulsa en *Agregar características* para aceptar la sugerencia del asistente. En este punto el servicio de rol *DirectAccess* y *VPN (RAS)* queda seleccionado. Ahora selecciona también el servicio de rol *Enrutamiento*. El despliegue de *DirectAccess* y *VPN (RAS)* requiere de algunos servicios de rol correspondientes al *Rol de servidor web (IIS)*. Avanza hasta los servicios de rol indicados y pulsa *Siguiente* para confirmar la instalación de estos servicios. En este punto, el asistente se encuentra en la ventana *Confirmar selecciones de instalación*, en la que se muestran todos los elementos que se van a instalar. Como norma general, marca la casilla de verificación *Reiniciar automáticamente el servidor de destino en caso necesario*. Pulsa en *Instalar* para completar la instalación de los servicios de rol requeridos. Cuando se completa la instalación, debajo de la barra de progreso de la instalación se indica “Requiere configuración, instalación correcta en 1S31-XXX”. Esto indica que para que el rol desplegado funcione se requieren acciones de configuración adicionales. Pulsa *Cerrar* para cerrar la ventana del asistente.

- En el *Administrador del servidor*, en la sección *Roles y características*, comprueba que el rol *Acceso remoto* ha sido instalado.
- Cierra el *Administrador del servidor*.

Configuración del servicio NAT en el anfitrión

- La instalación del rol *Acceso remoto* ha agregado nuevas herramientas de administración al sistema. En concreto, se ha agregado la herramienta *Enrutamiento y acceso remoto*, accesible desde el menú *Herramientas administrativas*. Abre *Enrutamiento y acceso remoto*. Esta consola permite administrar esta funcionalidad para todos los servidores de la red. Por defecto, solo se muestra el servidor local.
- En el servidor local se muestra una flecha roja hacia abajo. Esto indica que el servicio aún no está operativo.
- Selecciona 1S31-XXX (local). En el panel derecho aparece el mensaje *Configurar el Servidor de enrutamiento y acceso remoto*, lo que indica que todavía no se ha configurado.
- Botón derecho sobre 1S31-XXX (local) y selecciona *Configurar y habilitar Enrutamiento y acceso remoto*. Se abre el *Asistente para la instalación del servidor de enrutamiento y acceso remoto*. Selecciona *Traducción de direcciones de red (NAT)*. En la ventana *Conexión a Internet NAT*, debe indicarse la interfaz de red que está conectada a la red pública. Selecciona *vEthernet (Red virtual externa)*, que es la que está configurada con la IP pública (156.35.151.XXX). En la siguiente ventana (*Selección de red*), debe indicarse la interfaz de red que está conectada a la red privada. Selecciona *vEthernet (Red virtual interna)*, que está configurada con la IP privada (192.168.0.100). A continuación, se muestra la ventana *Servicios de traducción de nombres y direcciones*. Selecciona *Habilitar servicios básicos de nombre y direcciones*. Esto permite al router NAT enviar hacia la red externa solicitud de direcciones DHCP y consultas DNS. En la ventana *Intervalo de asignación de direcciones*, pulsa *Siguiente* para aceptar el intervalo proporcionado por defecto. Pulsa *Finalizar* para completar el asistente. Unas ventanas informativas muestran la puesta en marcha del servicio de enrutamiento.
- En este punto, el servicio NAT ya está operativo. Observa la flecha verde hacia arriba sobre el servidor local.
- Cierra *Enrutamiento y acceso remoto*.

Configuración de las puertas de enlace de las máquinas virtuales y pruebas

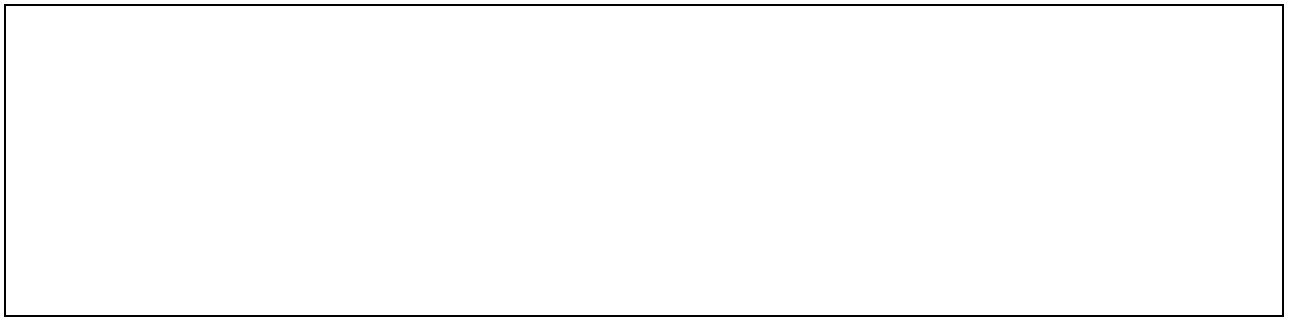
- Arranca en secuencia las máquinas PLX-S-01, PLX-S-02, PLX-C-51 y PLX-C-52. Inicia sesión con el *Administrador* en las máquinas de tipo servidor, y con *Alumno*, en las máquinas de tipo cliente.
- Configura las puertas de enlace de los servidores:
 - Configura la puerta de enlace de PLX-S-01 con la IP 192.168.0.100. Al configurar la puerta de enlace de la interfaz de red, el sistema se conecta a una red pública por primera vez. En este punto, el sistema pregunta *¿Quieres permitir que otros PC y dispositivos de esta red*

puedan detectar tu PC? Esto puede tener sentido en redes domésticas, pero no en el entorno de una red empresarial, que es el que se emula en estas prácticas. Contesta NO.

- De igual forma que en el caso de PLX-S-01, configura la puerta de enlace de PLX-S-02 con la IP del *router*, 192.168.0.100.
- Configura las puertas de enlace de los clientes:
 - PLX-C-51 -> 192.168.0.100
 - PLX-C-52 -> 192.168.0.100
- Pruebas de conexión de NAT.
 - Comprueba que todas las máquinas hacen ping correctamente al DNS de Uniovi (156.35.14.2). Esto implica que tienen conectividad con la red externa.
 - En el anfitrión, detener el servicio de *routing*. Para ello, abre la herramienta *Enrutamiento y acceso remoto*. Botón derecho sobre *IS31-XXX (local)* -> *Todas las tareas* -> *Detener*. Observa la flecha roja hacia abajo en *IS31-XXX (local)*. Entonces comprueba que las MV dejan de tener conexión a la red externa.
 - Vuelve a iniciar el servicio de *routing*. Observa la flecha verde hacia arriba en *IS31-XXX (local)*. Entonces comprueba que las MV vuelven a tener a conexión a la red externa.
 - Apaga todas las máquinas virtuales.
 - Finalmente, de nuevo, detén el servicio de *routing*. Habitualmente, se mantendrá este servicio detenido, salvo cuando sea necesario que se las MV se conecten a Internet. De esta forma, evitamos que las MV se actualicen.

(17) EJERCICIO COMPLEMENTARIO. El objetivo de este ejercicio es practicar sobre diversos aspectos de las redes virtuales y la configuración de red de las máquinas virtuales. Durante esta práctica, has conectado dos servidores (PLX-S-01 y PLX-S-02) y dos clientes (PLX-C-51 y PLX-C-52) a *Red virtual interna*. Has configurado el protocolo TCP/IP de todas estas máquinas y has comprobado que existe conectividad entre todas ellas. A continuación, se indica lo que debes hacer en este ejercicio.

- Debes poner en marcha la máquina PLX-S-PRUEBAS-YYY, cuya red no ha sido aún configurada, y debes conseguir que tenga conectividad con la máquina PLX-C-52, pero solamente con esta máquina. Es decir, PLX-S-PRUEBAS-YYY debe tener conectividad con PLX-C-52, pero no puede tener conectividad ni con PLX-S-01, ni con PLX-S-02, ni con PLX-C-51.
- Para conseguir la conectividad indicada, puedes crear conmutadores virtuales, interfaces de red y establecer configuraciones IP, según estimes oportuno.
- Para resolver este ejercicio, no es necesario cambiar la configuración de ninguno de los elementos de red (conmutadores virtuales, interfaces virtuales, etc.) que has creado durante la práctica. De hecho, no debes cambiar nada. El ejercicio se resuelve agregando nuevos elementos y configurándolos correctamente.
- Realiza las configuraciones necesarias y valida experimentalmente que consigues la conectividad solicitada.
- Describe a continuación las acciones que has llevado a cabo para resolver este ejercicio



Revertir las configuraciones realizadas en este ejercicio

- Para resolver este ejercicio has tendido que agregar una segunda interfaz de red a PLX-C-52. Elimina dicha interfaz. Asegúrate de que la interfaz que eliminas es la que has agregado para este ejercicio.
- Asimismo, has tendido que agregar un conmutador virtual, que eliminarás ahora. No obstante, antes de eliminarlo, desconecta de él la interfaz de red de PLX-S-PRUEBAS-YYY. Entonces, elimina dicho conmutador. No “toques” los conmutadores virtuales correspondientes a *Red virtual interna* y *Red virtual externa*, que forman parte de la infraestructura que se utilizará en las siguientes prácticas.
- Revierte la configuración IP de PLX-S-PRUEBAS-YYY a modo dinámico.
- Apaga PLX-S-PRUEBAS-YYY.