El impacto de las redes virtuales en el campus

The impact of virtual networks on campus

X. Homs, J.C. Sánchez y Jean-Marc Uzé

Resumen

El punto de partida de este documento es la confirmación del éxito del nuevo paradigma de virtualización en todos los sistemas involucrados en las tareas de investigación. La virtualización se ha convertido en una poderosa herramienta de gestión de recursos y, por lo tanto, en una tecnología muy extendida en las redes de investigación.
La función clásica de una red ha sido la de difundir un servicio determinado (por ejemplo, los recursos en Internet) a la comunidad de usuarios y servidores interesada en participar en dicho servicio. Una red virtual, de manera análoga, se encargará de conectar entre sí aquellos usuarios, servidores y recursos en general que forman parte de una misma comunidad de interés.
Las redes virtuales aparecieron como un mecanismo de gestión que permitía dividir el parque de recursos en grupos de interés (red de docencia, red de investigación, red de alumnos, etc.) Esta aproximación tiene un fuerte componente de seguridad asociado y una característica tecnológica interesante: no importa, en absoluto, la tecnología utilizada para la construcción de las redes virtuales ya que los grupos son típicamente intracampus y compuestos por elementos físicos (accesibles vía un puerto ethernet). Este tipo de redes virtuales se empezó a construir con servicios de LAN emulada sobre ATM, para luego ser creados mediante VLANs ethernet y ahora, en algunos casos, se empiezan también a utilizar mecanismos sobre MPLS.
Pero en el nuevo paradigma, la red virtual asume el papel de vehículo de transporte que permita enlazar entre sí grupos de interés distribuidos (a nivel internacional en algunos casos) con recursos virtuales (por ejemplo, una instancia virtual de un supercomputador). El papel de los estándares se convierte en la clave del éxito de esta nueva generación de redes y tiene que abordar tanto el plano de control (señalización dinámica de pertenencia) como el plano de conmutación (funcionar en entornos de 10G+)

Palabras clave: virtualización, mecanismos MPLS, estándares.

Summary

This document begins by confirming the success of the new virtualisation paradigm in all systems involved in research tasks. Virtualisation has become a powerful resource management tool and, as a result, a very common technology in research networks.
The classic function of a network has been to disseminate a certain service (for example, internet resources) to a group of users and servers interested in participating in that service. Likewise, a virtual network is responsible for connecting users, servers and resources in general that are part of a single interest group.
Virtual networks came about as a management device capable of dividing a resource pool into interest groups (teaching network, research network, student network, etc.). This approach has a high level of associated security and an interesting technological characteristic: it does not matter in the least which technology is used to build the virtual networks, since the groups are typically intra-campus and comprised of physical elements (accessible via an ethernet port). This type of virtual network began with emulated LAN services over ATM and then moved on to ethernet VLANs. Now, in some cases, mechanisms are being used over MPLS.
However, in the new paradigm, the virtual network takes on the role of a transport vehicle that links distributed interest groups (internationally, in some cases) with virtual resources (such as a virtual instance of a supercomputer). The role of standards will be the key to the success of this new generation of networks, and it must cover both control (dynamic membership indicators) and switching (working in 10G+ environments).

Keywords: virtualisation, MPLS mechanisms, standards.

La red virtual asume el papel de vehículo de transporte que permita enlazar entre sí grupos de interés distribuidos con recursos vituales

El papel de los estándares se convierte en la clave del éxito de esta nueva generación de redes y tiene que abordar tanto el plano de control como el plano de conmutación

1. El sentido de las redes virtuales en entornos de investigación

La movilidad del personal de investigación, la búsqueda de la excelencia, la necesidad de trabajar en grupo y la competencia entre continentes no son más que algunos de los motivos que nos plantan frente a uno de los retos más importantes de las redes de investigación: interconectar de manera efectiva los diferentes miembros de un mismo grupo de investigación.
Estos miembros estarán, con toda probabilidad, distribuidos entre diferentes universidades europeas y, seguramente, requerirán servicios de algún proveedor de computación para sus cálculos. Se requerirá una coordinación entre los diferentes agentes involucrados (redes internacionales, redes

nacionales, redes regionales, redes universitarias y proveedores de computación) y el uso de estándares para poder, de alguna manera, enlazar un investigador en el campus de la Universidad Politécnica con otro investigador en campus de alguna universidad alemana y con algún trozo de algún supercomputador europeo.

Durante mucho tiempo las especificaciones que una red de investigación publicaba como mecanismo de acceso a sus potenciales miembros afectaban únicamente al protocolo de enlace (ATM, Ethernet...) y a la velocidad (STM-1, Gigabit, 10G...) Se daba por supuesto que el único servicio Interredes sería la red IP de producción (Internet).

Con el tiempo se ha visto la necesidad de crear redes virtuales intercampus, interregionales o incluso internacionales y la falta de previsión ha llevado, en algunos casos, a dedicar recursos extremadamente escasos como fibras ópticas a proyectos que "técnicamente" no los requerían.

El nuevo paradigma de virtualización está obligando a las redes de investigación a cambiar las especificaciones de sus interfaces de acceso para añadir una categoría de redes virtuales (VPN Toolkit). Un ejemplo de estas nuevas especificaciones podría ser el siguiente:

- **Capa física:** Fibra óptica, STM-1, STM-4, STM-16
- **Protocolo de enlace:** Ethernet. ATM, POS
- **Velocidad:** 155Mbps, 622Mbps, 1G, 2.5G y 10G
- **VPN Toolkit:** 802.1Q, 802.1ad, ATM PVC, MPLS RFC 2917, MPLS VPLS,
- **Red IP de producción:** IPv4, IPv6, OSPF, BGP-4

El nuevo paradigma de virtualización está obligando a las redes de investigación a cambiar las especificaciones de sus interfaces de acceso para añadir una categoría de redes virtuales

2. Ancho de banda y redes virtuales basadas en etiquetas

Algunos proyectos de investigación pueden realizarse mediante redes virtuales construidas como capas (overlays) sobre la red IP de producción. Tecnologías como las VPNs IPsec, GRE o SSL-VPN pueden usarse para crear entornos virtuales donde sólo los miembros del grupo de investigación pueden acceder.

Pero no tiene ningún sentido, por ejemplo, usar este tipo de redes para proyectos de investigación en redes en los que el ancho de banda y los protocolos utilizados pueden, simplemente, no operar sobre la red IP de producción. Otros proyectos, como la interconexión de los supercomputadores europeos, son ejemplos de escenarios donde las redes virtuales "overlay" no pueden ser utilizadas.

La alternativa más sensata para la construcción de redes virtuales en entornos de investigación es el etiquetaje de los paquetes. El procesado de etiquetas es una tarea que se puede realizar fácilmente en hardware y a velocidades elevadas de conmutación (10G+).

Hay diferentes tipos de etiquetas y todos ellos cubiertos por algún estándar.

- Etiquetas Ethernet (802.1Q, 802.1ad)
- Etiqueta ATM (VPI / VCI)
- Etiqueta MPLS

El uso de etiquetas plantea algunas dudas en los terrenos de escalabilidad y de gestión. Principalmente en las redes nacionales e internacionales que deben participar de un elevado número de redes virtuales. Por este motivo es importante pensar no sólo en el tipo de etiquetas que se van a soportar sino también en qué protocolos de señalización pueden usarse para crear un plano de control de redes virtuales interredes. Etiquetas como el VLAN TAG (IEEE 802.1Q) tienen limitaciones evidentes de escalabilidad que limitan su aplicación a únicamente entorno de campus pequeños.

El uso de etiquetas plantea algunas dudas en los terrenos de escalabilidad y de gestión

En el momento de definición de una nueva red de investigación deben evaluarse el tipo de etiquetas que se van a soportar y la eventual asociación entre las mismas (tag mapping). En una red "extremo" (como la red campus de una universidad) el soporte de un único tipo de etiquetas puede ser suficiente. Pero en las redes "núcleo" (como por ejemplo las nacionales) se hace evidente la necesidad del soporte de diferentes tipos de etiquetas, de tablas de asociación entre tipos y protocolos de señalización de redes virtuales abiertos que permitan simplificar y agilizar el mantenimiento de las mismas.

3. Redes virtuales de nivel 2 y de nivel 3

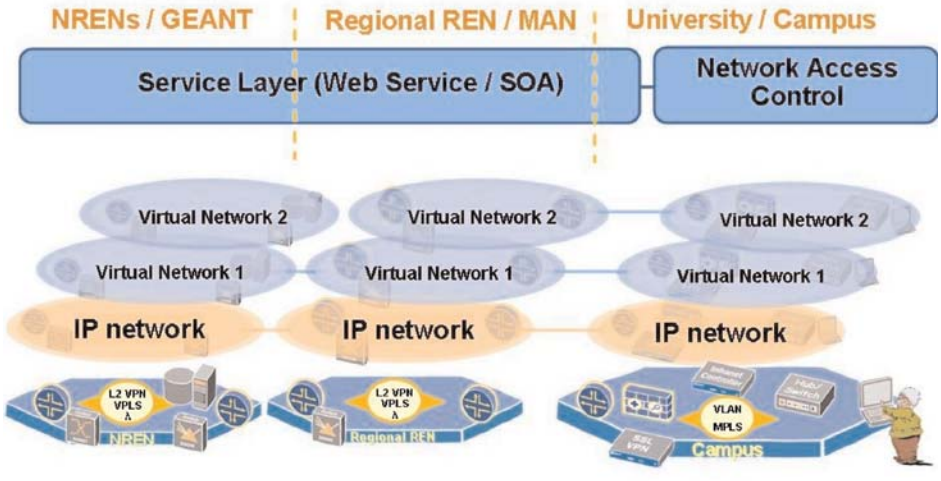
Las redes privadas virtuales de nivel 3 aparecieron en las infraestructuras de los operadores como una manera efectiva y muy escalable de mantener la una separación lógica entre los entornos de diferentes clientes.
En entornos de investigación la redes privadas de nivel 3 plantean muchos inconvenientes. Por ejemplo, los proyectos de investigación en redes requieren redes totalmente transparentes. La tendencia generalizada entre los grupos de trabajo es apostar por redes virtuales tan transparentes como sea posible.
Las redes virtuales de nivel 2 ofrecen una perspectiva muy atractiva para el investigador y su grupo de trabajo y la tecnología actual permite establecer servicios tanto punto a punto como todos-con-todos (Transparent LAN Service).
De entre todas las aproximaciones destaca por su escalabilidad y simplicidad operativa el servicio VPLS (Virtual Private LAN Service) sobre redes MPLS. Hay definiciones y estándares para la señalización de pertenencia a redes VPLS usando tanto BGP-4 como LDP. El primero (BGP-4) aplica principalmente a redes nacionales e internacionales por, entre otras cosas, conceptos como el servicio VPLS interdominio. La señalización de pertenencia a red VPLS mediante LDP puede ser una alternativa en las redes regionales o en el router de acceso de las universidades.

La señalización de pertenencia a red VPLS mediante LDP puede ser una alternativa en las redes regionales o en el router de acceso de las universidades

4. El papel de la red regional de investigación

Una red regional de investigación suele plantearse como un recurso compartido entre diferentes miembros que, de alguna manera, financian la red para maximizar sus capacidades como colectivo. En este sentido, muchos de los proyectos que se abordan en las redes regionales van orientados a centralizar servicios comunes como el servidor de nombres (DNS), directorios corporativos (LDAP), servicios de voz sobre IP, servidores de autenticación (RADIUS), servidores de acceso remoto, etc.

FIGURA 1. EL PAPEL DE LOS DIFERENTES AGENTES EN LA TRANSMISION DE REDES VIRTUALES



Todos estos proyectos aplican, exclusivamente, a la llamada "red de producción" y no aportan ningún valor a otras redes virtuales que puedan existir

Todos estos proyectos aplican, exclusivamente, a la llamada "red de producción" y no aportan ningún valor a otras redes virtuales que puedan existir.
En cuanto a estas redes virtuales se refiere, el papel fundamental de una red regional de

investigación es el de no convertirse en un elemento inhabilitador a la participación de sus miembros en proyectos que se puedan gestar a nivel nacional o internacional. Dicho de otra manera: la red regional de investigación tiene que ser capaz de enlazar aquellas redes virtuales que existan a nivel nacional / internacional con las equivalentes a nivel de campus en las que, finalmente, se encuentran los investigadores que deben participar en los proyectos.
En la defincón de la red regional de investigación se han de contemplar y acordar el conjunto de tecnologías que compondrán el "VPN Toolkit".

5. La conexión del campus al sistema de redes virtuales

En un escenario ideal, todas las redes de investigación, desde las internacionales hasta las de campus universitario, pasando por las regionales y nacionales, acordarían una única tecnología de señalización para la creación de redes virtuales de nivel 2. Pero en el mundo real esto es muy poco probable que ocurra.
En la red de campus universitario destaca el uso de redes virtuales ethernet (Ethernet VLAN – IEEE 802.1Q) para la separación de entornos de investigación y docencia. Ya existen algunas experiencias de redes de campus con virtualización mediante tecnología MPLS. Y es probable que MPLS avance significativamente dentro del campus en los próximos años.
En cualquier caso, el router (o routers) de acceso a la red regional de investigación es el punto clave donde el administrador de la red de campus asocia aquellas redes virtuales que lo requieran con sus homónimas en la red de investigación. Es, por lo tanto, muy importante que este router sea capaz de convertir tantas tecnologías de redes virtuales como sea posible:

- De VLAN TAG a VLAN TAG (802.1Q retagging)
- De ATM VPI/VCI a VLAN TAG
- De MPLS LDP a VLAN TAG
- De MPLS VPLS a VLAN TAG
- De MPLS VPLS a MPLS VPLS (VPLS interdomain)

En la red de campus universitario destaca el uso de redes virtuales ethernet para la separación de entornos de investigación y docencia

6. Control de acceso a red (802.1x) para gestionar a los investigadores

La virtualización puede llegar hasta el PC del investigador sin que ello requiera participación alguna por parte del administrador de la red del campus

Las redes virtuales que se gestaron en el núcleo de las redes nacionales e internacionales tienen que, finalmente, llegar a los investigadores que forman los grupo de trabajo.
Parece absurdo, después de tanta virtualización, pensar que el investigador debe tener dos ordenadores: el PC de producción (email, web...) conectado a la VLAN de gestión y el PC de investigación conectado a la VLAN de "pruebas".
¿No debería el investigador ser capaz de señalizar, de alguna manera, su condición de investigador / docente a la red para que ésta asigne su PC a la VLAN correspondiente en cada momento? La respuesta a esta pregunta reside en los modernos sistemas de control de acceso a red y estándares como el 802.1x de autenticación en LAN Ethernet.
Organismos como el Trusted Computing Group[1] trabaja en la defincón de interfaces abiertos (como los que se presentan en el Trusted Network Connect[2]) que permiten a un controlador de acceso a red condicionar su política de seguridad a variables del sistema en el PC del usuario. Y esta política de seguridad puede incluir, entre otras cosas, la VLAN en la que ese PC debería estar conectado en cada momento.
De esta manera la virtualización puede llegar hasta el PC del investigador sin que ello requiera participación alguna por parte del administrador de la red del campus. El mecanismo sería parecido al siguiente:

- El investigador conecta su PC a la red.
- El Switch Ethernet pide credenciales (802.1x).

- El controlador de acceso a la red (Policy Decision Point) pide variables del sistema del PC del investigador para saber si tiene que asignarlo a VLAN 10 (gestión) o a VLAN 110 (pruebas).
- Las variables presentan un "PC de gestión" y el controlador de acceso instruye al switch para que asigne el PC a la VLAN 10.
- El investigador cambia una variable en su sistema (hace click sobre el botón "voy a investigar"). El controlador de acceso a red detecta el cambio y renegocia el acceso a red. Ahora el switch asignará el PC a la VLAN 110.

En todo este ejemplo sólo falta incluir la programación del router de acceso que asocia la VLAN 110 del campus con la instancia 110 VPLS en la red regional que se corresponde con el grupo de trabajo al que pertenece el investigador afectado.

7. Servicios de seguridad informática

Los dispositivos de protección frente a ataques informáticos no suelen ser habituales en las redes virtuales de investigación

En la red de producción existen elementos activos de protección frente a ataques informáticos como Firewalls, IDPs, Antivirus, etc. Este tipo de dispositivos no suelen ser habituales en las redes virtuales de investigación.

Al permitir que un investigador conmute libremente entre la red de investigación y la red de producción se está asumiendo el riesgo de que amenazas que se propagan libremente por la red de investigación se extiendan a la red de producción a través de la infección del PC del investigador.

Para mitigar estos efectos aparece una nueva generación de dispositivos de seguridad (Firewalls) que aportan funcionalidades como:

- **Virtualización:** Implementación de diferentes instancias de firewall virtual. Una de ellas para la red de producción y otra para cada red de investigación que se asocia a redes virtuales internacionales.
- **Doble Stack IPv4 / IPv6:** Para proteger de todo tipo de amenazas.
- **Transparencia:** Capacidad de inspeccionar sólo el tráfico IP y dejar pasar transparentemente cualquier otro tráfico que pueda existir en una red en la que, por ejemplo, se estén investigando nuevos protocolos (IPv12?).

8. Conclusiones

No deberían olvidarse elementos activos de protección en las redes de investigación

Las redes virtuales aparecen en las redes de investigación nacionales e internacionales como vehículo para fomentar la investigación e interconectar recursos distribuidos. Las redes regionales de investigación, a parte de enfocarse en la potenciación de la red de producción, no deben convertirse en un factor inhabilitador a la libre asociación de investigadores a nivel campus con sus proyectos a nivel internacional. En la red de campus, el router de acceso es el punto clave de asociación de redes virtuales (VPN Toolkit) y la existencia de un controlador de acceso red puede facilitar la conmutación del investigador entre red de gestión y red de pruebas. Y, por último, no deberían olvidarse elementos activos de protección en las redes de investigación.

Referencias

[1] *https://www.trustedcomputinggroup.org/*
[2] *https://www.trustedcomputinggroup.org/groups/network/*

Xavier Homs Agesta
Jean-Marc Uzé
Juniper

Joan Carles Sánchez del Barrio
BSC