Infraestructura de soporte a la Terena Networking Conference

Support infrastructure for the Terena Networking Conference

Maribel Cosín, Vicente Giles, Enrique de Andrés, José Manuel Macías y José María Fontanillo.

Resumen

Terena es la asociación que se encarga de fomentar el uso de nuevas tecnologías dentro de la comunidad académica y de investigación. Cada año organiza el Terena Networking Conference en un país distinto y es la red académica nacional la que se encarga de alojarlo y dar el soporte técnico. Esta conferencia, de grandes dimensiones y con requisitos técnicos específicos, acoge aproximadamente quinientos asistentes, además de organizar demostraciones de proyectos en marcha.

Este año hemos afrontado el reto de alojar esta conferencia de manera conjunta, RedIRIS y la Universidad de Málaga, lo cuál ha supuesto un esfuerzo de coordinación entre distintas entidades y áreas técnicas. En este artículo describimos el montaje multidisciplinar que se preparó para dar soporte al evento, desde la red inalámbrica y los sistemas de autenticación, conexión con el exterior y recursos utilizados, la arquitectura de servidores y su configuración, y todo el soporte multimedia, tanto el despliegue en las salas como las herramientas dedicadas a la retransmisión. Todo ello se ha llevado a cabo con recursos propios de UMA y RedIRIS.

Palabras clave: TNC, conexión dedicada, red inalámbrica, arquitectura de sistemas virtualizados, split horizon, eduroam, radsec, streaming, retransmisión, Wowza Media Server.

Summary

Terena is the association responsible for promoting the use of new technologies within the academic and research community. Every year the Terena Networking Conference is organised in a different country where the national academic network takes on the task of hosting it and providing technical support. This large-scale conference, attended by some five hundred delegates, has specific technical requirements and organises demonstrations of ongoing projects.

This year RedIRIS and the University of Málaga have stepped up to the challenge of jointly hosting this conference, which has involved major coordination for both organisations and a number of technical departments. In this article we describe the multidisciplinary arrangements made for providing support for the event, ranging from the wireless network and authentication systems, connection with the outside world, server architecture and configuration, and all the multimedia support, both for equipment installed in the meeting rooms and the tools required for retransmission. All this has been done with existing UMA and RedIRIS resources.

Keywords: TNC, dedicated connection, wireless network, virtual systems architecture, split horizon, eduroam, radsec, streaming, retransmission, Wowza Media Server.

Terena es la asociación que se encarga de fomentar el uso de nuevas tecnologías dentro de la comunidad académica y de investigación

En la Terena Networking Conference se dan cita profesionales de las distintas redes académicas europeas

1. Introducción

Terena (Trans-European Research and Education Networking Association) asociación que se encarga de ofrecer un foro para colaborar, innovar y compartir conocimiento con el objetivo de fomentar el uso de nuevas tecnologías dentro de la comunidad académica y de investigación, organiza cada año el Terena Networking Conference, que tiene lugar en un país distinto y la red académica nacional se encarga de alojarlo y dar el soporte técnico.

Se trata de un evento de grandes dimensiones en el cuál se citan profesionales de las distintas redes académicas europeas así como del ámbito empresarial, relacionados con el mundo de las redes. En él

se realizan presentaciones y demostraciones sobre las últimas novedades que se han desarrollado y proyectos en los que se está trabajando.

En junio de este año, RedIRIS y la Universidad de Málaga, de manera conjunta, han tenido la oportunidad de alojar un TNC, lo cuál ha supuesto todo un reto debido a la envergadura del evento y las necesidades técnicas y logísticas que requiere.

Se decidió que la sede fuera la Facultad de Derecho, en el Campus de Teatinos, por la distribución de espacios. Todos ellos estaban cercanos y esto permitía que los asistentes se movieran por un área espaciosa y bien definida: un salón de actos de gran capacidad en el que se celebrarían las sesiones plenarias además de las de apertura y clausura, una zona de aulas para alojar tanto las sesiones técnicas paralelas como otras reuniones privadas que tuvieron lugar, y un amplio vestíbulo en el que se ubicaron los stands de los patrocinadores y las demostraciones que estaban programadas.

La Facultad de Derecho de la Universidad de Málaga acogió en junio la TNC 2009

En total las salas ocupadas fueron las siguientes: salón de actos, cuatro salas para las sesiones técnicas paralelas, tres salas para reuniones privadas, una sala de terminales y otra de uso interno para la organización, que servía tanto de almacén como de centro de operaciones.

Desde el punto de vista técnico, el edificio hubo que equiparlo para dar cobertura a los requisitos del evento. El reparto de responsabilidades se hizo de la siguiente manera: RedIRIS se encargaría de proporcionar conectividad al evento, direccionamiento IP, el hardware necesario para alojar los servicios así como la electrónica de red que agregaría la salida a Internet, la infraestructura de red de área local y los servicios. Por otro lado la Universidad de Málaga se encargaría de montar la infraestructura de red local: cableado de fibra y de cobre, conmutadores de diversa índole, ordenadores personales para la sala de terminales o Tablet PC para los ponentes.

El tema de audiovisuales merece mención aparte. El Centro de Tecnologías de la Imagen de la Universidad de Málaga se encargó de la equipación de salas y plenario así como de la definición de servicios multimedia, todo ello en colaboración con el personal de RedIRIS especializado en esta área. Los servidores de streaming también se instalaron de manera coordinada ya que uno estaba ubicado en la Universidad de Málaga y el otro en RedIRIS.

El montaje del evento se realizó en una facultad y la electrónica de red y servicios se instaló en la sede de los servicios informáticos de la Universidad

El despliegue y pruebas de toda esta infraestructura ha supuesto un proceso que comenzó el verano del pasado año. Desde entonces se ha estado trabajando en ello, desde reuniones de coordinación, visitas de replanteo, gestión de compras y préstamos, hasta instalación de cableado y equipos, y configuración y puesta en producción de los mismos, con el objetivo de tener todo listo para los grupos de trabajo de RedIRIS, que tuvieron lugar a finales de abril. De esta manera, se realizaba una prueba real del montaje un mes antes del evento con el objetivo de verificar el correcto funcionamiento y disponer de tiempo para depurar los fallos y ultimar configuraciones.

2. Infraestructura de red externa

Para asegurar que el evento dispondría de la capacidad necesaria, se contrataron dos enlaces Gigabit Ethernet, provisionados sobre rutas diversificadas y que conectarían la infraestructura del TNC con el nodo de RedIRIS en Sevilla. Se decidió contratar la conexión así, en lugar de un único enlace protegido, para que la implementación de la protección la hiciese RedIRIS en lugar de la operadora y disponer así de más garantía ante un fallo en el circuito. Para facilitar la gestión y no desaprovechar los recursos, los enlaces se utilizaron de manera agregada y así el evento dispuso de 2Gbps de salida.

El montaje tenía la particularidad de que el evento se realizaba en una facultad mientras que la

electrónica de red y servicios se instalaron en la sede de los servicios informáticos de la Universidad. Se decidió así por disponer esta última de salas técnicas adecuadas que garantizaban las condiciones medioambientales y la restricción de acceso. Por tanto los dos circuitos GE terminaban en este edificio, y la conexión entre ambos se realizó mediante dos fibras propias de la Universidad.

Esto suponía una restricción, no podía haber continuidad de una misma VLAN configurada entre ambos edificios y a la vez tener como gateway al router de salida, ambas condiciones eran excluyentes; pero en realidad no surgió la necesidad de tener que configurar algo así, con lo que para simplificar, se activaron VLANs distintas en cada edificio.

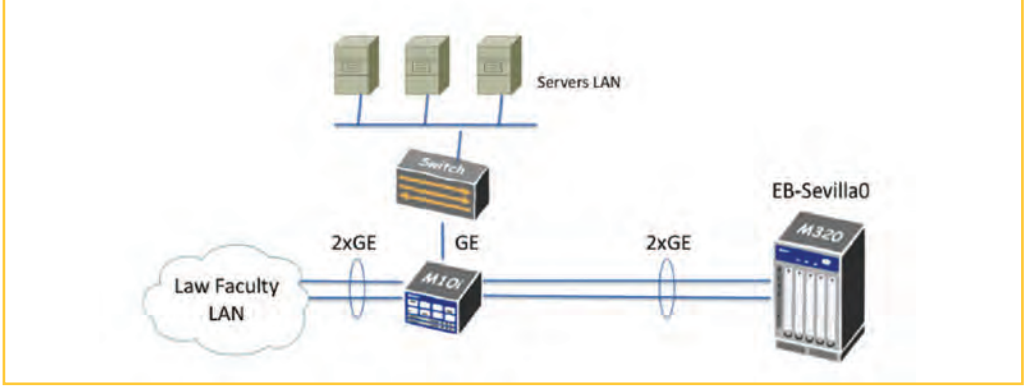
Como electrónica de red se eligió un router Juniper M10i, debido a las necesidades de puertos y por compatibilidad plena con el resto de equipos del backbone. Se equipó con 2 puertos GE-SX (conexión con Sevilla), 2 puertos GE-LX (conexión con la Facultad de Derecho), una tarjeta Tunnel PIC, que se encargaría de encapsular el tráfico multicast, y una tarjeta de cuatro puertos GE con sobresuscripción con un SFP de cobre para conectar los servidores.

La conexión de los circuitos se realizó mediantes dos fibras propias de la Universidad

Otro router equipado de la misma manera estuvo disponible durante el evento como backup del primero por si surgía algún problema. Se optó por tenerlo configurado para que el cambio fuera rápido en caso de necesitarlo; y apagado, para evitar problemas de picos de tensión que pudieran dañar el equipo.

Para conectar los puertos de servicio y gestión de los servidores se instalaron dos switches Juniper EX4200-24T configurados en stack y conectados al router M10i.

GRÁFICO 1



3. Recursos

Se definieron hasta diecinueve VLANs, uno para cada tipo de usuario que acudió al evento (asistentes, ponentes, personal de stands, de servidores, de gestión...)

Se realizó un análisis inicial y se encontraron distintos tipos de usuarios del evento: asistentes, ponentes, personal de stands, personal de demos, de servidores, de gestión... por lo que se decidió definir una VLAN por cada tipo. Más adelante, teniendo en cuenta la configuración de la red wireless y la programación de las demostraciones, se definieron más VLANs para este tipo de usuarios: cuatro VLANs para la red wireless, seis para las demostraciones, seis para servicios y gestión y tres para otro tipo de usuarios. En total diecinueve VLANs ocupadas (se había reservado un rango de veinte).

En cuanto a direccionamiento, aparte de utilizar algunos rangos privados para la gestión de los

equipos, se reservaron dos prefijos IPv4: un /21 para la red wireless que se dividió en cuatro prefijos /23 (uno por VLAN) y un prefijo /22 para servicios, demos y otros usuarios, que se fue fraccionando en función de las necesidades de los usuarios de cada VLAN.

Se activó también IPv6 en la red wireless utilizando cuatro rangos /64 (uno por cada VLAN) que se configuraron directamente en el router. Éste era el que anunciaba las direcciones a los equipos de usuario, debiendo tener éstos el protocolo IPv6 activado en el interfaz correspondiente para que la configuración se hiciera de manera automática.

4. Infraestructura de red interna

Toda la infraestructura de red destinada a la TNC 2009 era independiente de la red de producción de la Universidad de Málaga

Para la infraestructura de red cableada se pensó en un modelo en estrella, con un conmutador principal en la sala de control al que conectaran todos los demás conmutadores ubicados en cada sala o dependencia. De modo paralelo, todo el equipamiento de cada una de estas ubicaciones se conectaría mediante cableado UTP categoría 5 al conmutador correspondiente.

Adicionalmente, el conmutador principal se conectaba al enrutador de salida a RedIRIS situado en el CPD de la Universidad de Málaga, mediante una doble fibra óptica monomodo, diversificada sobre la infraestructura de red ya existente en la universidad.

Es conveniente destacar que toda la infraestructura de red destinada a la TNC2009 era completamente independiente de la red de producción de la Universidad de Málaga.

Todos los conmutadores utilizados fueron de la marca Cisco, siendo el principal un Catalyst 3750 con 12 puertos giga SFP (WS-3750G-12S-S) y el resto Catalyst 3650G con 48 puertos 10/100/1000 y 4 uplinks giga SFP, con PoE (WS-3650G-48PS-S). Se disponía de una segunda unidad del Catalyst 3750 y de 2 unidades adicionales de Catalyst 3650G para backups.

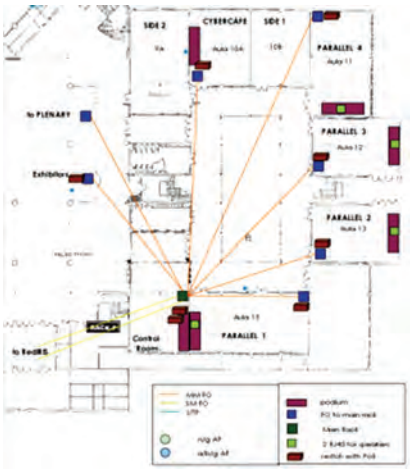
Durante el mes de febrero de 2009 se abordaron todos los trabajos de instalaciones de fibras ópticas y de cableado UTP interior. Desde la sala de control se tendieron fibras multimodo de 4 hilos a cada una de las salas paralelas, al cybercafé, al plenario y al hall de expositores.

Desde la sala de control se tendieron fibras multimodo de cuatro hilos a cada una de las salas paralelas, el cybercafé, el plenario y el hall de exposiciones

Adicionalmente, se instaló un número variable de cables UTP en cada una de las localizaciones, con el fin de proporcionar conectividad a todos los APs y a un par de puntos de ponentes. El resto de cableado UTP para los ordenadores del cybercafé y los expositores se dejó pendiente hasta que se definieran las ubicaciones definitivas de los equipos.

Para la monitorización de toda la infraestructura de red, incluidos los equipamientos inalámbricos, se instaló un servidor Cacti versión 0.8.7d, obteniendo estadísticas, entre otros, de tráfico en cada enlace de cada conmutador, del número de clientes asociados a la red inalámbrica, de modo global y por cada AP, etcétera.

GRÁFICO 2. ESQUEMA DE LA INFRAESTRUCTURA



4.1. Despliegue de red inalámbrica

El diseño de la red WiFi se basó en el uso de un controlador de red inalámbrica y de puntos de acceso ligeros, utilizando tanto tecnología 802.11a/g/b como 802.11n.

Para ello se contó con un controlador WLC Cisco 4400 Wireless Controller (AIR-WLC4404-100-k9), 25 Cisco Aironet 1130AG (AIR-LAP1131AG-E-k9) y 17 Cisco Aironet 1252AG (AIR-LAP1252AG-E-k9) con soporte de tecnología 802.11n. Adicionalmente, se disponía de un segundo controlador WLC y de varios APs de backup. Con respecto al WLC, se decidió mantener el de backup configurado y apagado, en lugar de optar por tener ambos activos.

Dado el alto porcentaje de dispositivos inalámbricos a soportar por cada asistente (entre 1,5 y 1,7 según los espacios) que se requería desde Terena, y la gran afluencia esperada (485 asistentes), se decidió utilizar una alta densidad de puntos de acceso tanto en las salas paralelas como en el auditorio, a fin de garantizar una distribución adecuada de clientes por AP y, por tanto, unas prestaciones de red más que suficientes.

Debido al alto porcentaje de dispositivos inalámbricos se decidió utilizar una alta densidad de puntos de acceso tanto en las salas paralelas como en el auditorio

Por ello, y tras realizar pruebas iniciales de despliegue en el propio edificio del Servicio Central de Informática, se decidió instalar 6 APs por cada una de las salas paralelas, y hasta 15 en el auditorio, junto con un AP para el resto de zonas: hall, cibercafé y sala de control.

El auditorio presentó algunas problemáticas para la instalación de los APs. En primer lugar, la enorme altura de su techo hacía imposible suspender del mismo los APs (solución adoptada en las salas paralelas) que tuvieron que colocarse en las paredes. Además se trata de un recinto forrado en madera, que obligaba a un tendido provisional reciclable y estéticamente transparente bastante complejo.

4.2. Configuración de red inalámbrica

Se decidió que la red inalámbrica de la conferencia ofreciera 2 SSIDs diferenciados, uno para eduroam y un segundo TNC2009 como alternativa para usuarios no eduroam.

El SSID eduroam se configuró con soporte tanto de WPA como WPA2, con encriptación TKIP y AES respectivamente, mientras que el SSID TNC2009 estaba abierto, dando acceso a la red mediante un portal cautivo soportado en el propio WLC, que obligaba a autenticar a los usuarios en base a las credenciales recibidas en su paquete de asistente.

La red inalámbrica de la conferencia ofrecía dos SSIDs, uno para eduroam y otro como alternativa para usuarios no eduroam

En todos los casos se ofreció direccionamiento IP público, estando el servicio de DHCP implementado sobre el propio controlador y se configuraron los APs y el WLC con capacidad de soporte IPv6, de modo que permitieran dicho tipo de tráfico, realizándose los anuncios de prefijos IPv6 para autoconfiguración en el enrutador Juniper.

Inicialmente se pensó que la mayor parte de los asistentes utilizarían el SSID eduroam, y dado el alto número de dispositivos a soportar por asistente, se tomó la decisión de utilizar una característica del controlador de la inalámbrica, que permite separar en grupos distintos los puntos de acceso y distribuir el tráfico de los clientes en distintas VLANs.

Mediante este agrupamiento, y a pesar de que todos los usuarios siempre ven un indicador de SSID único, se les separa en distintas VLANs, de modo que es posible limitar el efecto de un gran número de dispositivos en la misma VLAN. Dependiendo de a qué AP esté conectado un cliente, el WLC encaminará su tráfico por alguna de las 2 VLANs que dedicamos a cada uno de los 2 SSIDs visibles por el usuario.

En realidad, el reencaminar el tráfico de cada cliente por una VLAN u otra no depende exclusivamente del AP al que conecta, pues el controlador tiene en cuenta la validez de la dirección IP obtenida por DHCP, y mientras la IP no caduque, y para minimizar impactos en el usuario, mueve su tráfico a la VLAN que le corresponde a dicha IP, y no a la del AP, ignorando el grupo al que pertenece, y evitando la asignación de una IP de rango distinto.

La gran densidad de puntos de acceso inalámbricos nos permitió deshabilitar la funcionalidad que posee el controlador de Aggressive Load Balancing, que intenta redistribuir los clientes entre los APs menos utilizados, eliminando así posibilidades de problemas de asociación en algunos clientes.

Se realizó un estudio preliminar de frecuencias y coberturas en las zonas destinadas a la conferencia y otro a posteriori, tras la instalación de todo el equipamiento inalámbrico. El propio controlador, con los datos proporcionados por los APs, genera un listado de rogues, en su inmensa mayoría pertenecientes a la red inalámbrica de la Universidad de Málaga.

Se realizó un estudio preliminar de frecuencias y coberturas en las zonas destinadas a la conferencia y otro a posteriori, tras la instalación del equipamiento inalámbrico

Para evitar conflictos, se apagaron durante la conferencia todas las radios de los APs de la Universidad en las zonas de uso de la conferencia, y se eliminó del resto de APs próximos el SSID eduroam.

También decidimos dejar fijados los canales de los APs en las bandas de 2.4Ghz y 5Ghz y para ellos confiamos en otra funcionalidad del WLC, Dynamic Channel Assignment, que permite decidir que canal elige cada AP de modo coordinado. Una vez el controlador estableció los canales de los APs, y tras verificar que eran adecuados, realizamos un par de reasignaciones manuales y los dejamos fijados a partir de ese momento. La reasignación de canales en modo automático puede provocar cambios dinámicos de los mismos, que obligatoriamente suponen desconexiones y reasociaciones de los clientes, y que preferíamos evitar.

Con respecto a la potencia de emisión de los APs, dejamos que el WLC utilizara su funcionalidad Tx Power Control(TPC), que permite una regulación automática de la potencia en base a las emisiones e interferencias observadas entre los propios APs, pudiendo en un momento dado, cubrir los huecos de señal dejados por un AP averiado, por ejemplo, lo que nunca nos ocurrió.

4.3. Estadísticas de uso

Respecto a la red inalámbrica, se pudo observar un reparto equitativo entre ambos SSID en prácticamente cada momento. Así, en el momento de mayor número de clientes asociados durante toda la TNC2009, se contaban 168 usuarios de eduroam y 172 del portal, como se puede observar en las gráficas adjuntas.

El tráfico agregado de salida y entrada a Internet no fue muy alto, con medias entre 40 y 50 Mbps, destacando algunos momentos de tráfico más alto correspondientes a las demostraciones de uso de la red

Se observó en diferentes ocasiones (aparte de la monitorización con Cacti) la distribución de clientes inalámbricos entre los distintos APs, principalmente en las sesiones celebradas en el auditorio, y en las sesiones paralelas. En todos los casos se encontró un reparto bastante equilibrado de clientes entre los APs, con una carga ligeramente mayor en los equipos situados en el centro de las salas paralelas, posiblemente debido a la propia distribución de los asistentes. Como anécdota, el único AP (un Cisco Aironet 1252AG) situado en la zona de expositores (y del café...) llegó a soportar simultáneamente hasta 61 clientes... sin despeinarse.

Por tecnologías, se conectaron aproximadamente un 50% de clientes en 802.11g, y un 25% tanto para 802.11a como 802.11n.

Finalmente, el tráfico agregado de salida y entrada a Internet no fue muy alto, con medias de entre 40 y 50 Mbps, destacando algunos momentos de tráfico más alto correspondientes a las demostraciones de uso de la red que se llevaban a cabo.

GRÁFICO 3. NÚMERO TOTAL DE ASOCIACIONES

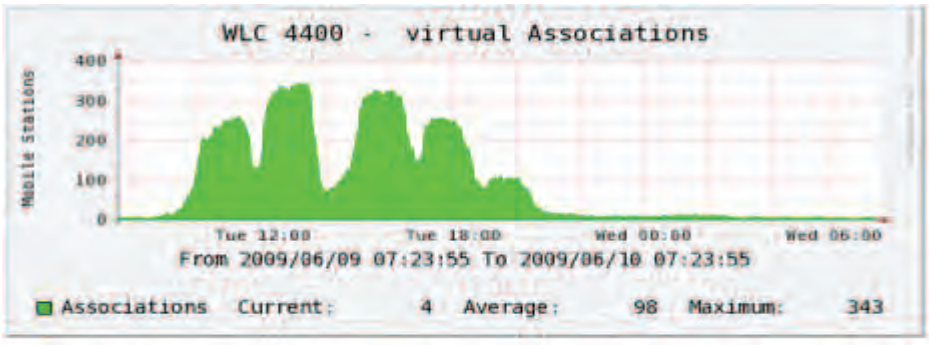
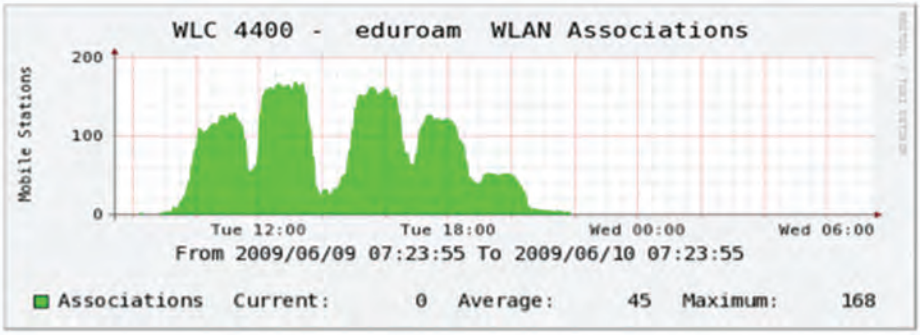
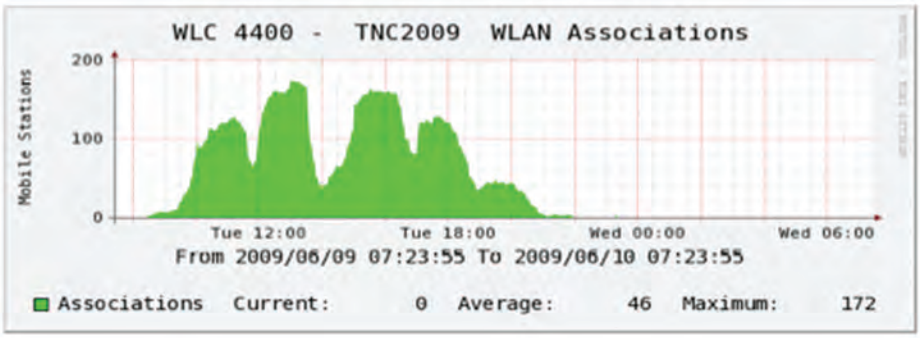


GRÁFICO 4. NÚMERO TOTAL DE ASOCIACIONES POR SSID





Los gráficos muestran el número total de asociaciones conectadas y el tráfico

GRÁFICO 5. TRÁFICO ENLACE 1 ENTRE TNC Y ENRUTADOR DE SALIDA

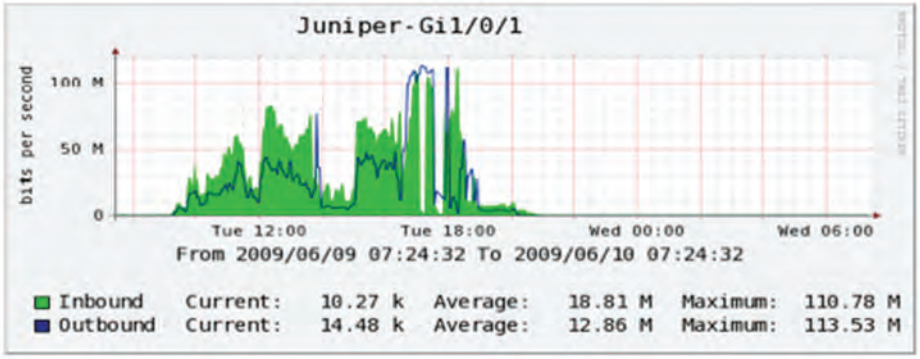
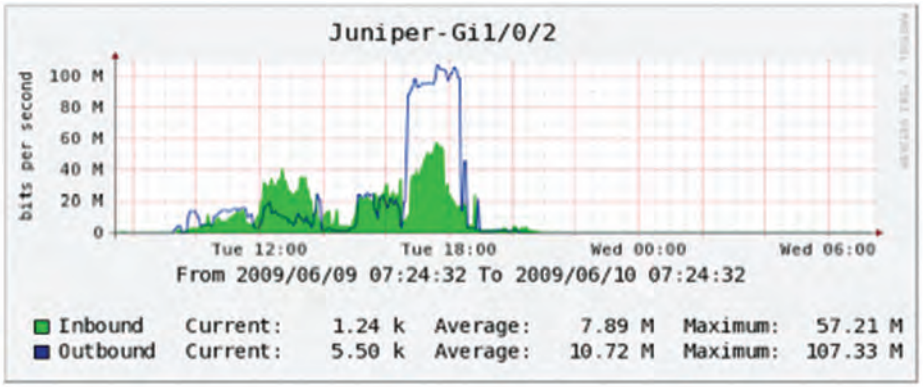


GRÁFICO 6. TRÁFICO ENLACE 2 ENTRE TNC Y ENRUTADOR DE SALIDA



La red inalámbrica era incompatible con los clientes con Windows Vista e Internet Explorer 7 y la implementación del portal cautivo WLC

4.4. Problemas descubiertos

Con respecto a la red inalámbrica, podemos mencionar un par de aspectos que merece la pena destacar:

- En primer lugar, y a pesar de que se había aprovechado la celebración de los Grupos de Trabajo de RedIRIS en abril para probar el despliegue realizado, y se había vuelto a probar 2 semanas antes de la TNC, descubrimos una incompatibilidad de los clientes con Windows Vista e Internet Explorer 7 y la implementación del portal cautivo del WLC.

  Tales clientes nunca recibían la página de autenticación del portal, lo que no ocurría si se usaba otro navegador como Firefox u Opera, o incluso Internet Explorer 8 en la misma máquina. Como no habíamos detectado antes este problema, lo achacamos a alguna incompatibilidad causada por alguna actualización reciente, y al no descubrir la forma de solventarlo, decidimos dejar el ssid TNC2009 como una red completamente abierta, que no necesitaba autenticación por parte del usuario, a partir del segundo día de conferencia.

Para la infraestrucura de servicios se optó por una arquitectura de sistemas virtualizados, en la que cada servicio fue montado sobre una máquina virtual diferente

- El segundo problema que detectamos estaba relacionado con el direccionamiento IPv6 y el cambio de VLANs provocado por el uso de agrupamiento de APs en el controlador de la red inalámbrica. Ocurría a veces que los clientes obtenían 2 prefijos de direccionamiento IPv6 y utilizaban uno de ellos, que no era válido en la VLAN definitiva en la que acababan siendo colocados.

  El motivo era un cierto retraso, en momentos de uso elevado, por parte del controlador en decidir la VLAN final que correspondía al usuario, lo que daba tiempo al cliente a recibir el anuncio de un primer prefijo, junto con el definitivo. Esto provocaba falta de conectividad hasta que el cliente invalidaba el primer prefijo al dejar de oír los anuncios del enrutador correspondiente y comenzaba a utilizar el segundo y correcto para su VLAN.

5. Infraestructuras de servicios

Para la infraestructura que soportase los servicios desplegados durante la TNC2009 se optó por una arquitectura de sistemas virtualizados, en la que cada servicio (o grupo de servicios relacionados) fue montado sobre una máquina virtual diferente. Utilizar tecnologías de virtualización para la

prestación de servicios permitió dotar al sistema de flexibilidad y tolerancia a fallos, haciendo posible la migración de máquinas virtuales si la carga de las físicas que las albergaban excedía determinado límite o en caso de caída de las mismas.

La arquitectura de virtualización diseñada estaba basada en un cluster VMware ESX y la infraestructura física que lo sustentó fueron 5 máquinas SunFire X4150 con dos procesadores Quad-Core Intel Xeon a 2.83GHz, 8GB de memoria RAM y fuente de alimentación redundante.

A pesar de disponer de suficiente espacio de almacenamiento local en cada máquina, con el fin de dotar al cluster de un almacenamiento altamente fiable (redundancia en discos duros y capacidad de realizar snapshots) se decidió utilizar una solución NAS de Network Appliance, concretamente el sistema NetApp 3020, exportando todos los datos a las máquinas físicas por NFS. Por otro lado, contar con un almacenamiento remoto centralizado era requisito para posibilitar la migración de máquinas virtuales entre máquinas físicas.

La arquitectura de virtualización diseñada estaba basada en un cluster VMware ESX y la infraestructura física que lo sustentó fueron 5 máquinas SunFire X4150

Cada una de las máquinas físicas tenía conectado un interfaz de red para la gestión y operación intrínseca del cluster VMware y otro interfaz para la conexión con el sistema de almacenamiento. Así mismo, también disponía de tantos interfaces conectados y asociados a una VLAN determinada, como VLAN's a los que las máquinas virtuales albergadas estaban conectadas. Para realizar la conexión de estos interfaces, se utilizaron dos conmutadores Juniper EX4200-24T configurados a modo de stack.

La gestión del cluster VMware requería una máquina con sistema operativo Windows con la herramienta VMware Infrastructure Client instalada. Para ello se reutilizó un servidor HP Proliant DL320 con procesador Intel Pentium 4 a 3.4GHz y 1GB de memoria RAM. Dado que se trataba de una máquina antigua y sin componentes redundantes, se montó otra máquina idéntica paralela, con todo el software necesario para la gestión del cluster VMware replicado.

Adicionalmente a la gestión del cluster VMware, para la gestión física de los elementos que lo conformaban, así como la del enrutador de salida a RedIRIS ubicado en el CPD de la UMA, se tomaron las siguientes medidas:

- Conexión de los interfaces de gestión (ELOM) de los servidores SunFire X4150.

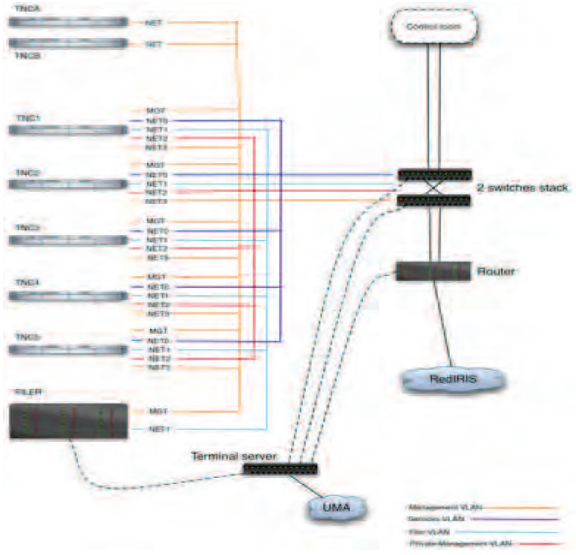
- Conexión de los puertos de consola de los conmutadores utilizados para la interconexión de los servidores anteriores y del enrutador de salida, utilizando para ello un servidor de consolas Cyclades TS-800.

Para no perder el acceso al servidor de consolas en caso de caída de red, el interfaz de red del servidor de consolas se conectó a la red de gestión de la UMA permitiendo un acceso fuera de banda a los equipos

Para no perder el acceso al servidor de consolas en caso de caída de alguno de los equipos de red, y en consecuencia, el acceso a la consola del equipo que permitiera solucionar el problema que hubiese motivado tal caída, el interfaz de red del servidor de consolas se conectó a la red de gestión de la UMA permitiendo, en este sentido, un acceso fuera de banda a los equipos.

La siguiente figura ilustra la infraestructura de servicios desplegada. Los equipos nombrados como TNC1 a TNC5 hacen referencia a los servidores SunFire X4150, los equipos nombrados como TNCA y TNCB hacen referencia a los servidores HP Proliant DL 320 y el FILER al sistema de almacenamiento NetApp 3020.

GRÁFICO 7



6. Servicios implementados

La figura ilustra la infraestructura de servicios desplegada para la ocasión

La distribución de máquinas virtuales, y servicios vinculados a las mismas, en máquinas físicas del cluster fue la siguiente:

- TNC1:
  - dns1.tnc2009.rediris.es
    - DNS: servidor principal
  - radsecproxy1.tnc2009.rediris.es
    - eduroam: servidor radiator principal
    - eduroam en los autobuses: servidor radsecproxy principal

- TNC2:
  - dns2.tnc2009.rediris.es
    - DNS: servidor secundario
  - radsecproxy1.tnc2009.rediris.es
    - eduroam: servidor radiador secundario
    - eduroam en los autobuses: servidor radsecproxy secundario

- TNC3
  - radguest.tnc2009.rediris.es
    - Autenticación wifi invitados: servidor radiador

- TNC4:
  - catci.tnc2009.rediris.es
    - Gráficas de red: servidor cacti
    - Gráficas eduroam: rgraph
  - nagios.tnc2009.rediris.es
    - Monitorización de equipos y servicios: servidor nagios

- TNC5:
  - db.tnc2009.rediris.es
    - Bases de datos: servidor MySQL
  - syslog.tnc2009.rediris.es
    - Recolección de logs: servidor syslog-ng

6.1. Servicio de DNS

Para configurar la resolución de nombres de los equipos implicados en el evento se creó el dominio tnc2009.rediris.es, el cuál fue delegado en dos servidores de los instalados en Málaga: dns1.tnc2009.rediris.es y dns2.tnc2009.rediris.es. Además se delegó también en sun.rediris.es y chico.rediris.es, servidores ubicados en una red distinta, para que el dominio se siguiera sirviendo en caso de fallo de servicio o de acceso a los primeros.

Dado que la mayor parte de los usuarios serían clientes conectados a través de una red wireless en la que un servidor dhcp les serviría los datos de configuración, se decidió generar mediante scripts las zonas relativas a la red wireless; y ya también, por comodidad, las relativas a la red de stands, de demos y de sala de terminales. Así, por defecto, cualquier máquina conectada a una de esas redes tendría resolución directa e inversa, con el formato nºhost-nºred-red_id.tnc2009.rediris.es.

Para configurar los nombres de los equipos implicados en el evento se creó el dominio tnc2009.rediris.es

Por otro lado, se configuró la resolución de nombres de los servicios y otras máquinas relevantes como es habitual en cualquier red. El caso del servidor de streaming fue particular, y es que, en realidad se montaron dos servidores, uno ubicado en la Universidad de Málaga y otro ubicado en RedIRIS, y se quería que hubiera un único nombre y que sirviera la información uno u otro en función de la procedencia de la petición. Para ello, se hizo una configuración en horizonte partido, consistente en la creación de vistas con listas de acceso asociadas de manera que en función de la dirección IP origen, se sirve una zona u otra. En este caso particular se tenían dos ficheros de zona para tnc2009.rediris.es, iguales, excepto para el nombre stream.tnc2009.rediris.es, ya que uno asociaba este nombre a una IP del rango reservado para el evento, y otro a una IP perteneciente al rango de servicios centrales de RedIRIS.

6.2. Servicio de soporte a la red inalámbrica

De cara a dar soporte a la autenticación en el SSID eduroam se apostó por utilizar dos servidores RADIUS para tener redundancia

6.2.1. EDUROAM

De cara a dar soporte a la autenticación en el SSID eduroam desplegado en la red inalámbrica de la conferencia, se apostó por utilizar dos servidores RADIUS para tener redundancia, con el controlador de la red inalámbrica como cliente. Estos recibirían las peticiones de los usuarios de eduroam (todos eran usuarios en roaming, incluso los propios de Málaga), y las encaminarían hacia la jerarquía de eduroam.

Además del controlador de red inalámbrica, también tenían como clientes RADIUS una instancia de radsecproxy. Dicho proxy escuchaba peticiones RadSec de cualquier dirección, pero sólo encaminaba aquellas que coincidían con certificados válidos generados para dotar de eduroam a los autobuses. En un apartado posterior abordaremos este despliegue

Como novedad con respecto a pasadas conferencias, se decidió utilizar para este encaminamiento RadSec (actualmente en estado de draft dentro del proceso de estandarización del IETF), en lugar de una conexión "sólo-RADIUS", teniendo para ello la bendición y el apoyo tanto del comité organizador del evento, como de eduroam Europa, desde donde se está apoyando dicho protocolo para ser usado en eduroam. La implementación usada de RadSec fue la de Radiator, actuando los servidores de la conferencia como clientes RadSec que conectaban directamente con la raíz de la jerarquía europea, los servidores ETLR1 y ETLR2 (servidores primario y secundario en la jerarquía de

eduroam en Europa), que además de RADIUS tienen habilitado el protocolo RadSec. En el gráfico 8 viene reflejada cómo se configuró esta conexión.

Aparte de la ganancia obvia de realizarse una conexión más directa, usar RadSec nos ha permitido comprobar que el protocolo es ya lo suficientemente maduro como para poder ser usado a gran escala. El gráfico 8 muestra la configuración usada en la conferencia.

6.2.2. AUTENTICACIÓN Wi-Fi DE INVITADOS

Para identificar a los usuarios invitados se utilizó un servidor RADIUS con Radiator, con una base de datos local que contenía las contraseñas de dichos usuarios. Dicho servidor era completamente independiente de la infraestructura RADIUS/RadSec para eduroam.

La configuración de este servidor se muestra también en el gráfico 8.

Usar RadSec nos ha permitido comprobar que el protocolo es ya lo suficientemente maduro como para poder ser usado a gran escala

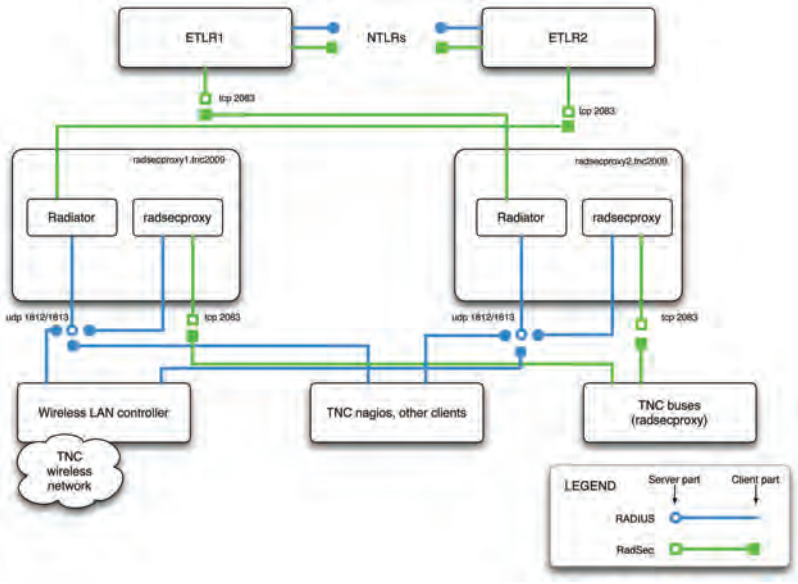
Los invitados se identificaban a través de un portal cautivo servido por el propio controlador de red inalámbrica, usando las contraseñas distribuidas a los asistentes en los kits de bienvenida. Estas contraseñas se generaron aleatoriamente, una por asistente.

6.2.3. EDUROAM EN LOS AUTOBUSES

Los autobuses de la Empresa Municipal de Transportes de Málaga, cubriendo la línea que conecta el centro de Málaga con el Campus de Teatinos donde se encuentra la Facultad de Derecho, tenían ya instalados un modem 3G con capacidad wireless, sin embargo la red inalámbrica no podía utilizarse directamente para eduroam. Los modems contaban también con una salida Ethernet, con lo cual se

Los asistentes al TNC pudieron utilizar internet en los autobuses mediante conexión Wi-Fi con eduroam

GRÁFICO 8. ESQUEMA DE CONEXIÓN DE LOS SERVIDORES RADIUS/RADSEC



instalaron puntos de acceso en los que se configuró eduroam, y un proxy RadSec (radsecproxy), conectado a los servidores proxy de eduroam para la conferencia. Esta configuración puede observarse también en el gráfico 8.

Una ventaja adicional de RadSec, estriba en que puede usarse sin conocer las direcciones que tendrán los clientes. En el caso de los autobuses, las direcciones pertenecían a un pool dinámico del operador de telefonía que conectaba el autobús a Internet vía el modem 3G. Configurando un certificado distinto en el radsecproxy instalado en los puntos de acceso de cada autobús, podíamos admitir en el otro extremo sólo aquellas conexiones cuyos certificados fueran válidos.

Podría haberse configurado también Radiator como servidor RadSec, pero queríamos probar también la implementación de radsecproxy a fondo, y al mismo tiempo sacar estadísticas individuales de las conexiones desde los autobuses. Por este motivo, en cada máquina el radsecproxy conectaba como cliente de Radiator.

6.2.4 DATOS SOBRE LAS AUTENTICACIONES REALIZADAS

La siguiente tabla recoge las autenticaciones válidas realizadas cada día para eduroam y los autobuses, así como los totales.

La tabla muestra las autenticaciones válidas realizadas cada día para eduroam y los autobuses

GRÁFICO 9

		Lunes	Martes	Miércoles	Jueves	TOTAL
eduroam Proxy 1	Congreso	208	2001	1422	727	**4358**
	Buses	45	230	55	154	**484**
eduroam Proxy 2	Congreso	729	505	1860	1874	**4968**
	Buses	40	0	2	64	**106**
eduroam TOTAL	**Congreso**	**937**	**2506**	**3282**	**2601**	**9326**
	Buses	**85**	**230**	**57**	**218**	**590**

7. Servicios de sala

Durante los meses previos al evento se realizaron visitas conjuntas entre UMA y RedIRIS para estudiar la adecuación de los espacios a las necesidades de un evento de estas características.

Durante los meses previos al evento se realizaron visitas conjuntas entre la UMA y RedIRIS para estudiar la adecuación de los espacios a las necesidades del evento

Los espacios disponibles eran 4 aulas con capacidad aproximada para 120 personas y un gran salón de actos en el que se desarrollarían las conferencias plenarias con capacidad para unas 700 personas. Las aulas estaban equipadas con proyección y micrófonos para megafonía.

Después del estudio previo se llegó a la conclusión de que la proyección podría ser utilizada aunque en el caso de dos de las salas, que eran estrechas y alargadas debía complementarse con dos pantallas planas en un lateral de la sala que servirían de apoyo a las personas sentadas más atrás.

La microfonía y megafonía no era la más adecuada por lo se decidió sustituir por otros sistemas más adecuados a las necesidades.

Además, como apoyo a la grabación y streaming que se haría de cada una de las sesiones se encontró necesario iluminar adecuadamente la zona del ponente ya que la luz fluorescente que había en las

aulas más la luz natural que entraba por la ventana, no era las más adecuadas. Por ello se cerraron las ventanas más cercanas al lugar de ponencia, se apagaron fluorescentes en zona delantera y se iluminó con focos desde el techo a la zona de ubicación del ponente.

El salón de actos contaba con todos los servicios habituales de proyección, iluminación del escenario, microfonía y megafonía

Por otro lado, la pared de detrás del ponente estaba ocupada por pizarras por lo que se decidió realizar un panel que taparía completamente esa zona con la imagen de la conferencia y de los sponsors, mediante un área de proyección.

El salón de actos contaba con todos los servicios habituales de proyección, iluminación del escenario, microfonía y megafonía. Se decidió sustituir únicamente el proyector que había en la sala de 4.500 lúmenes ANSI por otro de 9.000 lúmenes ANSI.

Uno de los requisitos que debía tener cada sala era la existencia de tomas de electricidad para cada asiento

Uno de los requisitos que deberían ser cumplidos en los 5 espacios en los que habría sesiones era la existencia de tomas de electricidad para cada asiento. Esto se llevo cabo con instalaciones que quedaron en la Universidad para otros eventos.

Adicionalmente a los espacios dedicados a sesiones de la conferencia se definió un espacio en el hall de entrada para demos en el cual se habilitó el siguiente equipamiento:

- Microfonía y megafonía
- Pantalla plana con pie
- Equipo de videoconferencia
- Proyector
- Tomas eléctricas
- Tomas de red Ethernet

8. Servicios multimedia

Se determinó que cada una de las aulas contaría con 3 fuentes de vídeo: 2 cámaras y el ordenador del ponente. El salón de actos contaría con 3 cámaras más el ordenador del ponente. En cada una de las salas habría un equipo de realización que se encargaría de la operación de las cámaras, sonido, realización y gestión del codificador.

Cada sala tendría un Macbook con el software Wirecast que permite realizar y codificar la señal. La entrada al Macbook de las señales de vídeo se realiza por firewire desde un hub firewire. En éste se encuentran conectadas las dos cámaras. En Wirecast aparece un previo de la señal de las dos cámaras y el ordenador del ponente. Para el envío de la señal del PC del ponente se instaló en éste un componente que envía la pantalla mediante red Ethernet.

Se instalaron dos servidores de streaming basados en el software Wowza Media Server, uno situado en el CPD de UMA y otro en el nodo nacional que RedIRIS tiene en las instalaciones de Telvent en Alcobendas (Madrid). Con la implementación de un horizonte partido en el servicio de DNS, la dirección *stream.tnc2009.rediris.es* se resolvió con la IP del servidor local de la UMA para los clientes situados en la UMA mientras que desde fuera se resolvía con la IP del servidor situado en RedIRIS.

El servidor fue preconfigurado con los códigos que se correspondían a cada una de las sesiones del programa de forma que la publicación en la página web que haría Terena fuera independiente del manejo de los servidores de streaming. Adicionalmente los servidores de streaming no deberían ser configurados una vez iniciado el evento. Para ello los codificadores eran iniciados para enviar sus flujos a cada uno de los puntos de entrada previamente definidos. Cuando finalizaba la sesión el vídeo quedaba almacenado de forma que la misma entrada que servía para ver el directo servía como VoD. Posteriormente, durante las sesiones sucesivas, se editaban estos videos para quitar del inicio las partes sobrantes. Cada vez que se hacía esta edición había un script que replicaba este contenido en los dos servidores.

Vicente Giles
vicente.giles@uma.es
Servicio Central de Informática
Universidad de Málaga

Maribel Cosín
maribel.cosin@rediris.es
Área de red

Enrique de Andrés
enrique.deandres@rediris.es
Área de middleware

José Manuel Macías
jmanuel.macias@rediris.es
Área de middleware

José María Fontanillo
jmaria.fontanillo@rediris.es
Área de middleware
Red.es / RedIRIS

En cuanto al servicio multimedia se determinó que las aulas de las sesiones contaría con 3 fuentes de vídeo, 2 cámaras y el ordenador del ponente

Se instalaron dos servidores de streaming basados en el software Wowza Media Server, uno situado en el UMA y otro en el nodo nacional de RedIRIS