8
Resolución de Problemas

La forma en que usted establezca la infraestructura de soporte de su red es tan importante como el tipo de equipamiento que utilice. A diferencia de las conexiones cableadas, los problemas con las redes inalámbricas a menudo son invisibles, y pueden requerir más capacidades y más tiempo para diagnosticarlos y remediarlos. La interferencia, el viento y otras obstrucciones físicas pueden causar que una red que estaba en funcionamiento desde hace tiempo falle. Este capítulo detalla una serie de estrategias para ayudarlo a formar un equipo de gente que pueda dar soporte a su red de forma efectiva.

Formando su equipo

Cada pueblo, compañía o familia, tiene algunas personas que están intrigadas por la tecnología. Son aquellos a quienes encontramos empalmando el cable de televisión, reparando un televisor roto o soldando una nueva pieza a una bicicleta. Este tipo de gente se va a interesar por su red y querrá aprender tanto como le sea posible. Aunque estas personas son recursos invalorables, debe evitar impartir todo el conocimiento especializado sobre las redes inalámbricas a una sola persona, porque si su único especialista pierde interés o encuentra un trabajo mejor remunerado en otro lugar, se va a llevar el conocimiento consigo cuando se vaya.

También puede haber muchos adolescentes jóvenes y ambiciosos o adultos jóvenes que se interesan por el tema y tienen tiempo para escuchar, ayudar y aprender acerca de la red. Ellos son de gran ayuda y van a aprender rápidamente, pero el equipo debe enfocar su atención en aquellos que sean los mejores para dar soporte a la red en los meses y años siguientes. Lo más probable es que los adultos jóvenes y los adolescentes se marchen a la universidad o a encontrar empleo, especialmente los ambiciosos, que son a los que les gustaría involucrarse. Estos jóvenes también tienen poca influencia

en la comunidad, donde una persona mayor es probable que tenga más capacidad para tomar decisiones que afecten a la red positivamente. A pesar de que estas personas puedan tener menos tiempo para aprender y parezcan menos interesados, su contribución y educación adecuada acerca del sistema puede ser significativa.

Por lo tanto, una estrategia clave para armar un equipo de soporte es balancear y distribuir el conocimiento entre aquellos que son los más capacitados para darle soporte a la red a largo plazo. Si bien debe involucrar a los jóvenes, no les debe dejar capitalizar el uso o el conocimiento de estos sistemas. Encuentre gente que esté comprometida con la comunidad, que tenga sus raíces en ella, que puedan ser motivados, y enséñeles. Una estrategia complementaria es repartir funciones y obligaciones y documentar toda la metodología y procedimientos. De esta forma la gente puede ser entrenada fácilmente y sustituida con poco esfuerzo.

Por ejemplo, en un proyecto el equipo de entrenamiento seleccionó a un brillante joven recién graduado de la universidad que había vuelto a su pueblo; él estaba muy motivado y aprendió rápidamente. Como aprendió tan rápido, se le enseñó más de lo que se había previsto, y era capaz de lidiar con una variedad de problemas, desde arreglar una computadora a rearmar el cable Ethernet. Desafortunadamente, dos meses después de emprender el proyecto le llegó una oferta para un trabajo en el gobierno y dejó la comunidad. Ni siquiera con la oferta de un salario similar se le pudo retener, ya que la perspectiva de un trabajo estable en el gobierno era más atractiva. Todo el conocimiento de la red y cómo realizar su soporte se fue con él. El equipo de entrenamiento tuvo que volver y comenzar el entrenamiento otra vez. La siguiente estrategia fue dividir funciones y entrenar gente que estuviera establecida de forma permanente en la comunidad: gente que tuviera hijos y casas, y que ya tuvieran trabajo. Llevó el triple de tiempo enseñarles a tres personas hasta que alcanzaron el nivel de entrenamiento del joven universitario, pero la comunidad retuvo ese conocimiento por mucho más tiempo.

Con esto queremos sugerirle que seleccionar por usted mismo a quien se va a involucrar en el proyecto a menudo no es el mejor enfoque. En general es mejor encontrar una organización local o un administrador local, y trabajar con ellos para encontrar el equipo técnico adecuado. Los valores, la historia, las políticas locales y muchos otros factores pueden ser importantes para ellos, mientras que pueden ser completamente incomprensibles para gente que no es de esa comunidad. El mejor enfoque es entrenar a su socio local para darle cierto criterio (asegurándose de que lo comprenden) y para marcar límites firmes. Dichos límites deben incluir reglas acerca del favoritismo y clientelismo, aunque éstas deben considerar la situación local. Probablemente sea imposible decir que usted no puede contratar familiares, pero deben existir inspecciones y balances. Si tenemos un candidato que sea un

familiar, debe haber un criterio claro, y una segunda autoridad que decida sobre su candidatura. También es importante que el socio local tenga esa autoridad y que no sea influido por los organizadores del proyecto, porque de otro modo se compromete su habilidad gerencial. Los socios locales deben ser capaces de determinar quién va a ser la mejor persona para trabajar con ellos. Si son bien instruidos sobre este proceso, entonces los requerimientos de personal serán cumplidos a cabalidad.

La resolución de problemas y el soporte técnico son como el arte abstracto. La primera vez que usted ve una pintura abstracta puede que le parezca un conjunto de pinceladas al azar. Luego de reflexionar en la composición durante un tiempo, puede que comience a apreciar la obra como un conjunto, y la coherencia "*invisible*" se vuelva real. La mirada de un neófito a una red inalámbrica puede identificar antenas, cables y computadoras, pero le puede tomar bastante tiempo apreciar el objetivo de la red "*invisible*". En áreas rurales, es posible que la gente de la localidad deba hacer una inmensa evolución en su comprensión antes de que pueda apreciar una red invisible que fue instalada en su pueblo. Por lo tanto se necesita una introducción paulatina que les haga más fácil aceptar y apropiarse de la tecnología. El mejor método es fomentar el involucramiento de la comunidad. Una vez que los participantes han sido seleccionados y se han comprometido con el proyecto, involúcrelos tanto como sea posible. Déjelos "manejar". Entrégueles la pinza crimpeadora o el teclado y muéstreles cómo hacer el trabajo. Aunque usted no tenga tiempo para explicar cada detalle, y a sabiendas de que haciéndolo de esta manera va a tomar mucho más tiempo, ellos necesitan involucrarse físicamente y ver no sólo lo que ha sido hecho, sino también cuánto trabajo se ha hecho.

El método científico se enseña prácticamente en todas las escuelas occidentales. Mucha gente lo aprende durante sus clases de ciencia en la secundaria. Para decirlo simplemente, se toma un conjunto de variables, luego se eliminan lentamente dichas variables a través de pruebas binarias hasta quedarse con una o pocas posibilidades. Con esas posibilidades en mente, se completa el experimento. Luego se prueba si el experimento produce algo similar al resultado esperado, de lo contrario se calcula nuevamente el resultado esperado y se intenta de nuevo. Al campesino típico se le pudo haber explicado este concepto, pero probablemente no haya tenido la oportunidad de aplicarlo para resolver problemas complejos. Aunque estén familiarizados con el método científico, es probable que no hayan pensado en aplicarlo para resolver problemas reales.

Este método es muy efectivo a pesar de que puede llegar a consumir mucho tiempo. Se puede acelerar haciendo suposiciones lógicas. Por ejemplo, si un punto de acceso que venía funcionando hace mucho, deja de hacerlo repentinamente luego de una tormenta, se puede sospechar que hay un problema con el abastecimiento eléctrico y por lo tanto obviar la mayor parte

del procedimiento. Las personas que han sido adiestradas para dar soporte deben aprender como resolver los problemas utilizando este método, ya que va a haber momentos en los que el problema no es ni conocido ni evidente. Se pueden hacer simples árboles de decisión, o diagramas de flujo, e intentar eliminar las variables para aislar el problema. Por supuesto, esos cuadros no deben ser seguidos ciegamente.

A menudo es más sencillo enseñar este método utilizando primero un problema no tecnológico. Digamos, haga que su estudiante desarrolle un procedimiento de resolución para un problema sencillo y familiar, como por ejemplo, un televisor a batería. Para empezar, sabotee el aparato: póngale una batería sin carga, desconecte la antena e inserte un fusible roto. Pruebe al estudiante, dejándole en claro que cada problema muestra síntomas específicos, e indíquele la manera de proceder. Una vez que haya reparado el televisor, hágalo aplicar este procedimiento a un problema más complicado. En una red, usted puede cambiar una dirección IP, cambiar o dañar cables, utilizar el ESSID equivocado u orientar la antena en la dirección equivocada. Es importante que ellos desarrollen una metodología y un procedimiento para resolver estos problemas.

Técnicas adecuadas para la resolución de problemas

Ninguna metodología de resolución de problemas puede cubrir por completo todos aquellos con los que se va a encontrar cuando trabaja con redes inalámbricas, pero a menudo los problemas caen dentro de uno de los pocos errores comunes. Aquí hay algunos simples puntos a tener en mente que pueden hacer que su esfuerzo para resolver el problema vaya en la dirección correcta.

- **No entre en pánico.** Si usted está arreglando un sistema, significa que el mismo estaba funcionando, con seguridad muy recientemente. Antes de sobresaltarse y hacer cambios impulsivamente, analice la escena y determine exactamente lo que está roto. Si tiene un registro histórico o estadísticas de funcionamiento, mucho mejor. Asegúrese de recolectar la información en primer lugar para poder tomar una decisión bien informada antes de hacer cambios.
- **¿Está conectado?** Este paso a menudo es pasado por alto hasta que muchas otras posibilidades son exploradas. Los enchufes pueden desconectarse muy fácilmente, ya sea accidental o intencionalmente. ¿El cable está conectado a una buena fuente de energía? ¿El otro extremo está conectado a su equipo? ¿La luz de energía está encendida? Esto puede sonar algo tonto, pero usted se verá aún más tonto si pierde mucho tiempo en probar la línea de alimentación de la antena sólo para compro-

bar que el AP estuvo desenchufado todo ese tiempo. Confíe en nosotros, esto sucede más a menudo de lo que la mayoría de nosotros queremos admitir.

- **¿Cuál fue la última cosa que cambiamos?** Si usted es la única persona con acceso a sistema, ¿cuál fue el último cambio que hizo? Si otros tienen acceso a él, ¿cuál fue el último cambio que hicieron y cuándo? ¿Cuándo fue el último momento en el que el sistema funcionó? A menudo los cambios tienen consecuencias imprevistas que pueden no ser notadas inmediatamente. Deshaga ese cambio y vea el efecto que tiene en el problema.
- **Haga una copia de seguridad.** Esto se debe hacer antes de que usted detecte problemas y le servirá después. Si va a hacer una actualización compleja de software al sistema, tener una copia de seguridad significa que puede restaurarlo rápidamente a la configuración previa y comenzar de nuevo. Cuando resolvemos problemas muy complejos, tener una configuración que "más o menos funciona" puede ser mucho mejor que tener una que no funciona para nada (y que no puede restaurar fácilmente desde la memoria).
- **El bueno conocido.** Esta idea se aplica tanto al equipamiento como a los programas. Un ***bueno conocido*** es cualquier componente que se pueda reemplazar en un sistema complejo para verificar que sus contrapartes están en buenas condiciones de funcionamiento. Por ejemplo, puede llevar junto con sus herramientas, un cable Ethernet previamente probado. Si sospecha que hay problemas con el cable que está en la instalación, sencillamente puede intercambiar el cable sospechoso con el bueno conocido y ver si las cosas mejoran. Esto es mucho más rápido y menos propenso a los errores que rearmar un cable, y le dice inmediatamente si el cambio solucionó el problema. De la misma forma usted puede tener una batería de repuesto, un cable de antena, o un CD-ROM con una buena configuración conocida para el sistema. Cuando solucionamos problemas complicados, guardar su trabajo en un punto dado nos permite retornar a un estado bueno conocido, aún si el problema no se ha solucionado por completo.
- **Cambie una variable por vez.** Cuando estamos bajo presión para poner un sistema de nuevo en línea, tendemos a actuar impulsivamente y cambiar muchas variables al mismo tiempo. Si lo hace, y sus cambios arreglan el problema, entonces no va a comprender exactamente qué fue lo que ocasionó el problema en primer lugar. Peor aún, sus cambios pueden solucionar el problema original, pero al mismo tiempo generar consecuencias imprevistas que pueden dañar otras partes del sistema. Si cambia sus variables una a la vez, puede entender con precisión qué fue lo que se dañó en primera instancia, y ser capaz de ver los efectos directos de los cambios que va haciendo.

- **No lo dañe.** Si no comprende en su totalidad cómo funciona un sistema, no dude en llamar a un experto. Si no está seguro de si un cambio en particular va a dañar otras partes del sistema, entonces encuentre a alguien con más experiencia, o busque una forma de probar su cambio sin hacer daño. Poner una moneda en lugar de un fusible puede resolver el problema inmediato, pero también puede incendiar el edificio.

Es poco probable que la gente que diseñó su red esté disponible veinticuatro horas al día para resolver los problemas cuando aparecen. Aunque su equipo de soporte sea muy capaz de resolver problemas, puede que no sea lo suficientemente competente como para configurar un enrutador desde cero o poner el conector a un cable LMR-400. A menudo es mucho más eficiente tener varios componentes de respaldo a mano, y entrenar a su equipo para reemplazar por completo la pieza rota. Esto puede significar tener un punto de acceso o un enrutador preconfigurado, guardados en un gabinete cerrado, claramente etiquetado y almacenado junto con los cables de respaldo y las fuentes de alimentación. Su equipo puede cambiar el elemento que funciona mal y enviarlo a un experto para que lo repare o coordinar para que se envíe otro equipo de respaldo. Mantener los respaldos seguros y reemplazarlos cuando los usamos puede ahorrarnos mucho tiempo a todos.

Problemas comunes de las redes

A menudo los problemas de conectividad provienen de la rotura de componentes, un clima adverso o simplemente un problema de configuración. Una vez que su red esté conectada a Internet o abierta al público en general, van a aparecer una gran cantidad de amenazas provenientes de los mismos usuarios. Esas amenazas pueden estar en un rango desde las benignas hasta las indiscutiblemente malévolas, pero todas van a tener impacto en su red si no está configurada correctamente. Esta sección se enfoca en algunos problemas comunes encontrados una vez que su red es utilizada por seres humanos reales.

Sitios web alojados localmente

Si una universidad aloja su sitio web localmente, los visitantes del sitio desde fuera del campus y del resto del mundo van a competir con los trabajadores de la universidad por el ancho de banda. Esto incluye el acceso automatizado desde los motores de búsqueda que periódicamente ***escanean*** su sitio por completo. Una solución para este problema es dividir el DNS y reflejar el sitio. La universidad refleja una copia de sus sitios web en un servidor que puede ser una compañía de almacenamiento web europea, y utiliza el DNS dividido para direccionar a todos los usuarios de fuera de la universidad hacia el sitio reflejado, mientras que los usuarios de la universidad acceden al

mismo sitio pero a nivel local. Los detalles sobre cómo configurar esto se proveen en el capítulo tres.

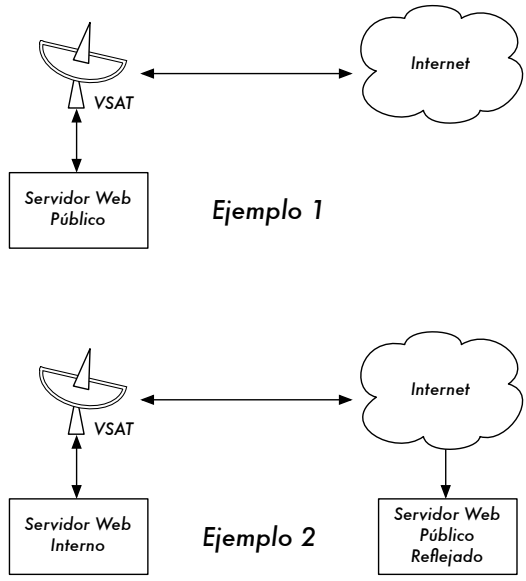

Figura 8.1: En el ejemplo 1, todo el tráfico del sitio web que viene desde Internet debe atravesar el VSAT. En el ejemplo 2, el sitio web público es alojado en un servicio europeo rápido, mientras que en el servidor interno se mantiene una copia para tener un acceso local muy rápido. Esto mejora la conexión del VSAT y reduce los tiempos de carga para los usuarios del sitio web.

Proxis abiertos

Un servidor proxy debe ser configurado para aceptar solamente conexiones desde la red de la universidad, no desde el resto de Internet. Esto se debe a que gente de todos lados se va a conectar y utilizar los proxis abiertos por una variedad de razones, como por ejemplo evitar pagar por ancho de banda internacional. La forma de configurarlo depende del servidor proxy que usted use. Por ejemplo, puede especificar el rango de direcciones IP para la red del campus en su archivo **`squid.conf`** de manera que esta sea la única red que puede utilizar Squid. Alternativamente, si su servidor proxy está detrás del límite de un cortafuego, puede configurar el cortafuego para que le permita solamente a los servidores internos que se conecten al puerto proxy.

Servidores de retransmisión abiertos

Un servidor de correo electrónico configurado incorrectamente puede ser encontrado por gente inescrupulosa, y usado como un servidor de retransmisión para enviar grandes cantidades de mensajes y de correo no deseado.

Ellos lo hacen para ocultar la verdadera fuente del correo no deseado y para evitar ser atrapados. Para detectar esta vulnerabilidad, haga la siguiente prueba en su servidor de correo electrónico (o en el servidor SMTP que actúa como servidor de retransmisión en el perímetro de la red del campus). Use ***telnet*** para abrir una conexión al puerto 25 del servidor en cuestión (con algunas versiones Windows de telnet, puede ser necesario escribir '*set local_echo*' antes de que el texto sea visible):

```
telnet mail.uzz.ac.zz 25
```

Si se permite conversación de línea de comando interactiva (como el ejemplo que sigue), el servidor está abierto para retransmitir:

```
MAIL FROM: spammer@waste.com
250 OK - mail from <spammer@waste.com>
RCPT TO: innocent@university.ac.zz
250 OK - rcpt to spammer@waste.com
```

En su lugar, la respuesta después del primer **`MAIL FROM`** debe ser algo así:

```
550 Relaying is prohibited.
```

Una prueba en línea como esta, así como información acerca de este problema, están disponibles en sitios como *http://www.ordb.org/*. Como aquellos que envían correos masivos tienen métodos automatizados para encontrar los servidores de retransmisión abiertos, una institución que no protege sus sistemas de correo es casi seguro que va a ser víctima de abusos. Configurar el servidor de correo para que no sea un relevador abierto consiste en especificar las redes y hosts que están autorizados para transmitir mensajes a través de él en el MTA (por ejemplo, Sendmail, Postfix, Exim, o Exchange). Éste probablemente va a ser el rango de direcciones IP de la red del campus.

Redes entre pares (P2P - peer-to-peer)

El abuso del ancho de banda a través de programas entre pares (P2P) para compartir archivos como Kazaa, Morpheus, WinMX y BearShare se puede prevenir de las siguientes formas:

- **No permita la instalación de nuevos programas en las computadoras del campus.** Para prevenir la instalación de programas como el Kazaa, no debe darse a los usuarios comunes acceso de administrador a las estaciones de trabajo. Muchas instituciones también estandarizan la configuración de sus máquinas, instalando el sistema operativo requerido en una computadora, luego instalan todas las aplicaciones y las configuran de una forma óptima, incluyendo la imposibilidad de que los usuarios instalen nuevas aplicaciones. Una imagen del disco de esta PC se clona a todas

las otras PCs utilizando un programa como Partition Image (vea *http://www.partimage.org/*) o Drive Image Pro (vea *http://www.powerquest.com/*).

Es probable que de vez en cuando los usuarios puedan eludir el control y consigan instalar nuevo software o dañar el que ya tenía instalado la computadora (provocando por ejemplo que esta se "cuelgue" a menudo). Cuando esto pasa, un administrador simplemente puede restablecer la imagen del disco, logrando que el sistema operativo y todo el software en la computadora sean exactamente como se especificó originalmente.

- **Bloquear esos protocolos no es una solución.** Esto pasa porque Kazaa y otros protocolos son lo suficientemente hábiles como para eludir los puertos bloqueados. Por omisión Kazaa utiliza para la conexión inicial el puerto 1214, pero si no está disponible intentará utilizar los puertos 1000 al 4000. Si también están bloqueados, utiliza el puerto 80, haciéndose ver como tráfico de consultas web. Por esta razón los ISPs no lo bloquean, pero sí lo "limitan", utilizando un administrador de ancho de banda (vea el capítulo tres).
- **Si limitar el ancho de banda no es una opción, cambie el diseño de la red.** Si el servidor proxy y los servidores de correo están configurados con dos tarjetas de red (como se describe en el capítulo tres), y esos servidores no están configurados para reenviar ningún paquete, entonces van a bloquear todo el tráfico P2P. También van a bloquear todos los otros tipos de tráfico como Microsoft NetMeeting, SSH, software VPN, y todos los otros servicios no permitidos específicamente por el servidor proxy. En redes con un ancho de banda escaso se puede decidir que la simplicidad de este diseño prepondera sobre las desventajas que tiene. Esta decisión puede ser necesaria, pero no debe tomarse a la ligera. Los administradores no pueden predecir las formas innovadoras en las que los usuarios van a hacer uso de la red. Si bloqueamos preventivamente todos los accesos, también impediremos que los usuarios puedan hacer uso de cualquier servicio (aún los servicios de ancho de banda lento) que su proxy no soporte. Si bien esto puede ser deseable en circunstancias de ancho de banda muy lento, en general nunca debe ser considerada como una buena política de acceso.

Programas que se instalan a sí mismos (desde Internet)

Existen programas que se instalan a sí mismos y luego utilizan ancho de banda –por ejemplo el denominado Bonzi-Buddy, el Microsoft Network, y otros tipos de "gusanos". Algunos programas son espías, y permanecen enviando información sobre los hábitos de búsqueda (y de consumo) de un usuario hacia una compañía en algún lugar de Internet. Estos programas se previenen, hasta cierto punto, educando a los usuarios y cerrando las PCs para evitar el acceso como administrador a los usuarios normales. En otros

casos, tenemos soluciones de software para encontrar y remover estos programas problemáticos, como Spychecker (*http://www.spychecker.com/*), Ad-Aware (*http://www.lavasoft.de/*), o xp-antispy (*http://www.xp-antispy.de/*).

Actualizaciones de Windows

Los últimos sistemas operativos de Microsoft Windows suponen que una computadora con una conexión LAN tiene un buen enlace a Internet, y descarga automáticamente parches de seguridad, correctores de fallas y mejoradores, desde el sitio web de Microsoft. Esto puede consumir grandes cantidades de ancho de banda en un enlace a Internet costoso. Los dos posibles enfoques a este problema son:

- **Deshabilitar las actualizaciones de Windows en todas las estaciones de trabajo.** Las actualizaciones de seguridad son muy importantes para los servidores, pero que las estaciones de trabajo en una red privada protegida como la red de un campus las necesiten, es algo debatible.
- **Instalar un Servidor de Actualización de Software.** Este es un programa gratuito de Microsoft que le permite descargar todas las actualizaciones de Microsoft durante la noche al servidor local y luego distribuirlas desde allí a las estaciones de trabajo cliente. De esta forma las actualizaciones de Windows utilizarán el ancho de banda del enlace a Internet durante el día. Desafortunadamente, para que esto funcione, todos los PCs cliente deben ser configurados para utilizar el Servidor de Actualización de Software. Si usted tiene un servidor DNS flexible, también puede configurarlo para que responda todas las solicitudes al sitio web *windowsupdate.microsoft.com*, y lo redireccione hacia su servidor de actualización. Esta es una buena opción sólo para redes muy grandes, pero puede ahorrar una incalculable cantidad de ancho de banda de Internet.

Bloquear el sitio de actualizaciones de Windows en el servidor proxy no es una buena solución porque el servicio de actualización de Windows (Actualización Automática) va a continuar intentando más agresivamente, y si todas las estaciones de trabajo lo hacen, se produce una pesada carga en el servidor proxy. El extracto de abajo es del registro del proxy (registro de acceso Squid) donde esto fue hecho bloqueando los archivos de gabinete Microsoft (.cab).

La mayoría del registro Squid lucía así:

```
2003.4.2 13:24:17 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
  *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:18 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:18 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab HEAD 0
2003.4.2 13:24:19 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:19 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:20 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:21 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:21 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:21 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab HEAD 0
```

Si bien esto puede ser tolerable cuando tenemos unos pocos PC cliente, el problema crece significativamente cuantos más nodos se agregan a la red. En lugar de forzar al servidor proxy a procesar solicitudes que siempre van a fallar, tiene más sentido redireccionar los clientes del Software de Actualización a un servidor local de actualización.

Programas que suponen un enlace de gran ancho de banda

Además de las actualizaciones de Windows, muchos otros programas y servicios dan por sentado que el ancho de banda no es un problema, y por lo tanto lo consumen por razones que el usuario no puede predecir. Por ejemplo, los paquetes anti-virus (como el Norton AntiVirus) se actualizan a sí mismos directamente desde Internet, automática y periódicamente. Sería mejor si esas actualizaciones se distribuyeran desde el servidor local.

Otros programas como el reproductor de video RealNetworks, descarga actualizaciones y publicidad automáticamente, así como envía información sobre los hábitos de uso a un sitio en Internet. Pequeñas aplicaciones (conocidas como *applets*) aparentemente inocuas (como Konfabulator y miniaplicaciones que crean accesos directos desde el escritorio del usuario, conocidas como *Dashboard widgets*) sondean continuamente los servidores de Internet buscando información actualizada. Esta información puede requerir poco ancho de banda (como las actualizaciones del estado del tiempo o de noticias), o mucho ancho de banda (como las cámaras web). Estas aplicaciones deben ser limitadas o bloqueadas por completo.

Las últimas versiones de Windows y Mac OS X tienen un servicio de sincronización horaria. Este mantiene el reloj de la computadora en la hora exacta conectándose a dos servidores de sincronización en Internet. Para eso es

mejor instalar un servidor local de hora y distribuir la hora exacta desde allí, en lugar de ocupar el enlace de Internet con esas solicitudes.

Tráfico de Windows en el enlace a Internet

Las computadoras que tienen el sistema operativo Windows se comunican entre ellas usando ***Network Basic Input/Output System - NetBIOS*** (es una interfaz de programación que permite a las aplicaciones instaladas en computadores diferentes dentro de una red local comunicarse) y ***Server Message Block - SMB*** (un protocolo para compartir archivos, impresoras, puertos y otros servicios y dispositivos entre computadores). Estos protocolos operan sobre TCP/IP y otros protocolos de transporte. SMB es un protocolo que realiza ***elecciones*** para determinar cuál computadora va a ser el ***buscador maestro***. El buscador maestro es una computadora que mantiene una lista de todas las computadoras, recursos compartidos e impresoras que usted puede ver en el ***Entorno de Red.*** La información sobre recursos compartidos también es transmitida a intervalos regulares.

El protocolo SMB fue diseñado para redes LAN y causa problemas cuando la computadora con Windows está conectada a Internet. A menos que el tráfico SMB sea filtrado, se esparcirá por el enlace a Internet, desperdiciando el ancho de banda de la organización. Para prevenirlo se pueden tomar los siguientes pasos:

- Bloquear el tráfico SMB/NetBIOS saliente en el enrutador perimetral o en el cortafuego. Este tráfico consume ancho de banda, y peor aún, presenta un riesgo de seguridad. Muchos "gusanos" en Internet y herramientas de penetración buscan activamente SMB abiertos, y explotan dichas conexiones para ganar ulterior acceso a su red.
- **Instale ZoneAlarm en todas las estaciones de trabajo (no en el servidor).** Una versión gratuita se puede encontrar en *http://www.zonelabs.com/*. Este programa le permite al usuario determinar cuáles aplicaciones pueden hacer conexiones a Internet y cuáles no. Por ejemplo, Internet Explorer necesita conectarse a Internet, pero el Explorador de Windows no. ZoneAlarm puede bloquear el Explorador de Windows para que no lo haga.
- **Reduzca los recursos compartidos de la red.** Idealmente, sólo el servidor de archivos debería tener recursos compartidos. Puede utilizar una herramienta como SoftPerfect Network Scanner (disponible en *http://www.softperfect.com/*) para identificar fácilmente todos los recursos compartidos en su red.

Gusanos y virus

Los gusanos y los virus pueden generar una gran cantidad de tráfico. Por ejemplo el gusano W32/Opaserv aún prevalece, a pesar de que es muy viejo. Se esparce a través de los recursos compartidos de Windows y es detectado por otras personas en Internet porque intenta esparcirse aún más. Por esta razón es esencial que haya una protección anti-virus instalada en todas las PCs. Más esencial aún es la educación de los usuarios en cuanto a no ejecutar archivos adjuntos, así como no dar respuesta a correos no deseados. De hecho debería haber una política de que ni las estaciones de trabajo, ni el servidor, puedan correr servicios que no están utilizándose. Una computadora no debería tener recursos compartidos a menos que fuera un servidor de archivos; y un servidor no debería correr servicios innecesarios. Por ejemplo, los servidores Windows y Unix generalmente corren un servicio de servidor web por omisión. Éste debería deshabilitarse si dicho servidor tiene una función diferente; cuantos menos servicios corra una computadora, menos posibilidades tiene de ser atacada.

Lazos de reenvío de correo electrónico

Ocasionalmente, un error cometido por un único usuario puede llegar a causar un problema serio. Por ejemplo, un usuario cuya cuenta universitaria está configurada para reenviar todo el correo a su cuenta personal en Yahoo. El usuario se va de vacaciones, y todos los correos que le fueron enviados se siguen reenviando a su cuenta en Yahoo la cual puede crecer sólo hasta 2 MB. Cuando la cuenta de Yahoo se llene, va a comenzar a rebotar los correos para la cuenta de la universidad, la cual inmediatamente los va a reenviar a la cuenta de Yahoo. Un lazo de correo electrónico se forma cuando se envían y re-envían cientos de miles de correos, generando un tráfico masivo y congestionando los servidores de correo.

Existen opciones dentro de los servidores de correo que son capaces de reconocer los lazos. Estas opciones deben activarse por omisión. Los administradores también deben tener cuidado de no apagarlas por error. Debe también evitar instalar un sistema de re-envío SMTP que modifique los encabezados de los correos de tal forma que el servidor de correo no pueda reconocer el lazo que se ha formado.

Descargas pesadas

Un usuario puede iniciar varias descargas simultáneas, o descargar grandes archivos tales como 650MB de imágenes, acaparando la mayor parte del ancho de banda. La solución a este tipo de problemas está en el entrenamiento, hacer descargas diferidas, y monitoreo (incluyendo monitoreo en tiempo real, como se subrayó en el capítulo seis). La descarga diferida se puede implementar al menos de dos formas:

En la Universidad de Moratuwa, se implementó un sistema utilizando el direccionamiento URL. A los usuarios que acceden a direcciones **ftp://** se les ofrece un directorio donde cada archivo listado tiene dos enlaces: uno para la descarga normal, y otro para la descarga diferida. Si se selecciona la descarga diferida, el archivo especificado se pone en cola para descargarlo más tarde, y al usuario se le notifica por correo electrónico cuando la descarga está completa. El sistema mantiene una memoria intermedia (*cache*) de archivos descargados recientemente, y cuando los mismos se solicitan de nuevo, los recupera inmediatamente. La cola de descarga se ordena según el tamaño del archivo, por lo tanto los archivos pequeños se descargan primero. Como una parte del ancho de banda se dedica para este sistema aún en las horas pico, los usuarios que solicitan archivos pequeños pueden recibirlos en minutos, algunas veces hasta más rápido que una descarga en línea.

Otro enfoque puede ser crear una interfaz web donde los usuarios ingresan el URL del archivo que quieren descargar. El mismo se descarga durante la noche utilizando una tarea programada (o ***cron job*** por su nombre en inglés). Este sistema funciona solamente para usuarios que no sean impacientes, y que estén familiarizados con los tamaños de archivos que pueden ser problemáticos para descargarlos durante las horas de trabajo.

Envío de archivos pesados

Cuando los usuarios necesitan transferir archivos grandes a colaboradores en cualquier lugar en Internet, se les debe enseñar cómo programar la subida (*upload*) del archivo. En Windows, subir archivos a un servidor FTP remoto se puede hacer utilizando un guión (*script*) FTP, que es un archivo de texto con comandos FTP similares a los siguientes (guardado como **`c:\ftpscript.txt`**):

```
open ftp.ed.ac.uk
gventer
mysecretword
delete data.zip
binary
put data.zip
quit
```

Para ejecutarlo, escriba esto desde la línea de comando:

```
ftp -s:c:\ftpscript.txt
```

En computadoras con Windows NT, 2000 y XP, el comando puede guardarse en un archivo como **`transfer.cmd`**, y ser programado para correr en la noche utilizando las Tareas Programadas (Inicio ➜ Configuración ➜ Panel

de Control ➜ Tareas Programadas). En Unix, se puede hacer lo mismo utilizando las opciones ***at*** o ***cron***.

Usuarios enviándose archivos unos a otros

Los usuarios a menudo necesitan enviarse archivos grandes. Si el receptor es local, es un gasto innecesario de ancho de banda enviarlos vía Internet. Para eso se debe crear un recurso compartido en el servidor web local Windows / Samba / Novell, donde un usuario puede colocar archivos grandes para que otros los descarguen.

Como una alternativa se puede escribir una interfaz web para que un servidor web local acepte un archivo pesado y lo coloque en un área de descarga. Después de cargarlo al servidor web, el usuario recibe un URL correspondiente al archivo, que puede transmitir a sus colaboradores locales o internacionales para que accedan al archivo. Esto es lo que ha hecho la Universidad de Bristol con su sistema FLUFF. La universidad ofrece una facilidad para la carga de archivos pesados (FLUFF por su sigla en inglés) disponible en *http://www.bristol.ac.uk/fluff/*. Esos archivos pueden se accedidos por cualquiera al que se le haya dado su ubicación. La ventaja de este enfoque es que los usuarios pueden brindar acceso a sus archivos a usuarios externos, mientras el método de archivos compartidos funciona sólo para los usuarios dentro de la red del campus. Un sistema como este se puede implementar fácilmente como un guión (*script*) CGI utilizando Python y Apache.