Soluzione dei problemi

20

ninux.org

Contents

1 Soluzione dei problemi

L'organizzazione di una struttura di supporto alla rete diventa importante a seconda del tipo di apparecchiature utilizzate. Diversamente dalle connessioni su cavo, nelle reti wireless i problemi sono spesso invisibili e possono richiedere molto tempo e conoscenze in più per essere analizzati e risolti. Interferenze, vento e nuovi ostacoli fisici possono guastare una rete che ha funzionato per molto tempo. In questo capitolo dettaglieremo una serie di strategie utili per creare un team che possa supportare efficentemente la rete.

1.1 Formare un team

In ogni villaggio, famiglia o compagnia c'è qualcuno che ha interesse verso la tecnologia. Ci sono quelli che crimpano i cavi dell'antenna, cambiano il cavo della televisione o saldano un pezzo alla bicicletta. Queste persone saranno interessate alla rete e vorranno imparare quanto più possibile al riguardo. Anche se queste persone saranno risorse inestimabili, bisognerà evitare di impartire tutta la conoscenza specifica ad una sola persona. Se l'unico specialista perde interesse o trova un altro lavoro porterà la conoscenza via con se.

Ci sono anche molti giovani ambiziosi, teenager o adulti, che saranno interessati avendo anche il tempo di ascoltare, imparare e dare un aiuto con la rete. Saranno sicuramente di aiuto e impareranno velocemente ma il team del progetto deve porre l'attenzione su coloro che potranno supportare la rete per i prossimi mesi ed anni. I giovani possono spostarsi per l'università o trovare un lavoro, specialmente i più ambiziosi che tendono a farsi coinvolgere. Spesso i ragazzi hanno una piccola influenza sulla comunità mentre invece una persona più grande sarà probabilmente più capace di prendere decisioni che impatteranno positivamente la rete nel suo complesso. Anche se magari hanno meno tempo a disposizione per imparare e sembrano meno interessati, coinvolgere e formare persone più grandi può risultare fondamentale.

Quindi, una strategia chiave per formare un team di supporto, consiste nel bilanciare e distrubire la conoscenza su coloro che possono supportare la rete nel lungo termine. Bisogna coinvolgere i giovani, ma evitare di fargli accumulare l'uso e la conoscenza di questi sistemi. Bisogna trovare le persone che sono impegnate nella comunità, che vi siano radicate, che possano essere motivate ed insegnare a loro. Una strategia complementare è quella di suddividere in comparti le funzioni e i compiti e documentare tutte le metodologie e le procedure. In questo modo sarà più facile addestrare le persone, ed in caso sostituirle con un piccolo sforzo.

Per fare un esempio, una volta in un sito di progetto, il team di training ha selezionato un brillante neolaureato che era tornato nel suo villaggio. Questi era molto motivato ed ha imparato in fretta, per questo gli è stato insegnato più di quanto previsto, tanto che è diventato capace di affrontare una grande varietà di problemi, dal riparare un PC al sistemare i cavi Ethernet. Sfortunatamente, due mesi dopo il lancio del progetto, gli è stato offerto un impiego pubblico ed ha lasciato la comunità. Anche l'offerta di una paga migliore non è bastata a trattenerlo dato che la prospettiva di stabilità che l'impiego pubblico gli offriva era troppo appetibile. Tutta la conoscenza sulla rete e sul come supportarla è sparita con lui. Il team di training è dovuto tornare e ricominciare daccapo. La strategia successiva è stata di suddividere le funzioni e formare le persone che erano radicate permanentemente nella comunità: le persone con casa e figli, e con un lavoro stabile. Questo ha richiesto tre volte il tempo necessario a formare il neolaureato, ma in questo modo questa formazione potrà rimanere al servizio della comunità per molto più tempo.

Anche se questo ci può far pensare che dovremmo scegliere personalmente chi coinvolgere, non è necessariamente questo l'approccio migliore. Spesso è meglio cercare un'organizzazione locale che possa fare da partner o un manager locale, e lavorare con loro per trovare il giusto team tecnico. Valori, storia, politiche locali e molti altri fattori saranno importanti per loro, anche se rimarranno completamente incomprensibili per le persone che non fanno parte di quella comunità. L'approccio migliore è di guidare i partner locali, fornirgli i criteri, assicurarsi che li abbiano compresi ed impostare chiari limiti e confini. Questi limiti dovrebbero comprendere regole riguardo patrocinio, nepotismo e favoritismo, anche se queste regole devono aver considerazione della situazione locale. Potrebbe risultare impossibile stabilire che non è possibile assumere

parenti, potrebbe esser meglio fornire un sistema di controlli ed equilibri. Se a candidarsi è un parente, dovrebbero esserci criteri chiari ed una seconda autorità che decida riguardo la candidatura. Allo stesso tempo è importante che il partner locale non veda messa in discussione la sua capacità dagli organizzatori del progetto, compromettendo così la propria capacità di amministrazione. Saranno i più indicati a giudicare chi può lavorare meglio con loro stessi. Se vengono formati bene per questo processo, allora tutti i nostri requisiti dovrebbero esser soddisfatti.

La soluzione dei problemi ed il supporto in ambito tecnologico sono un'arte astratta. La prima volta che vediamo un a pittura astratta ci appare come una serie di schizzi di vernice casuali. Dopo aver riflettuto sulla composizione per un pò di tempo, iniziamo ad apprezzare il lavoro nel suo complesso e la sua "invisibile" coerenza ci appare più chiara. Il neofita in una rete wireless può vedere le antenne, i cavi e i computer, ma può richiedergli un pò di tempo per capire che si tratta di una rete "invisibile". Nelle aree rurali, può spesso accadere che le persone debbano fare uno grosso sforzo di comprensione per apprezzare la rete invisibile che gli viene semplicemente piazzata nel villaggio. Per questo è necessario un'approccio graduale per avvicinare più facilmente le persone al supporto dei sistemi tecnologici. Il miglior metodo è il coinvolgimento. Una volta che sono stati scelti i partecipanti e si sono impegnati nel progetto bisogna coinvolgerli il più possibile. Lasciarli "guidare". Dar loro la crimpatrice o la tastiera e mostrargli come fare il lavoro. Anche se non c'è tempo per spiegare ogni dettaglio, anche se richiedesse più tempo, devono essere fisicamente coinvolti, non solo vedere il risultato di quel che è stato fatto ma anche quanto e che lavoro è stato eseguito.

Il metodo scientifico è insegnato in tutte le scuole occidentali. Molte persone lo imparano sin dal momento in cui arrivano alle lezioni di scienza alle scuole superiori. Prendere una serie di variabili, quindi lentamente eliminare le variabili tramite test binari fino a rimanere con una o poche possibilità. Con queste possibilità in mente, si completa l'esperimento. Dopodichè si testa per vedere se l'esperimento fornisce risultati simili a quanto atteso. In caso negativo si ricalcolano i risultati attesi e si prova ancora. Il contadino tipico potrebbe esser stato introdotto al concetto, ma probabilmente non avrà la possibilità di risolvere problemi complessi. Anche se ha familiarità con il metodo scientifico, potrebbe non pensare di applicarlo ai problemi reali.

Questo metodo è molto efficiente, anche se lungo. Può essere velocizzato facendo assunzioni logiche. Ad esempio, se un access point che funziona da tempo a volte smette di funzionare dopo un temporale, si può sospettare di problemi legati all'alimentatore e saltare così la maggior parte della procedura di risoluzione dei problemi. Alle persone incaricate di supportare la tecnologia dovrebbe venir insegnato a risolvere i problemi con questo metodo dato che ci saranno occasioni in cui il problema non sarà nè noto nè evidente. Un semplice albero delle decisioni o un diagramma di flusso che testi queste variabili può essere stilato per eliminare le variabili ed isolare il problema. Ovviamente il diagramma non dovrebbe essere seguito ciecamente.

Spesso è più semplice insegnare questo metodo usando dapprima un problema non tecnologico. Far sviluppare ai propri studenti una procedura di risoluzione dei probemi su qualcosa di semplice e familiare, ad esempio, una televisione alimentata a batterie. Iniziare sabotando la televisione dando loro una batteria non carica. Disconnettendo l'antenna. Inserendo un fusibile guasto. Testare gli studenti, spiegando bene che ogni problema mostrerà sintomi specifici e indirizzarli verso il modo in cui procedere. Una volta che hanno riparato il televisore, facciamoli applicare questa procedura ad un problema più complicato. In una rete possiamo cambiare un indirizzo IP, scambiare o rompere i cavi, usare l'SSID sbagliato o orientare l'antenna nella direzione sbagliata. E' importante che gli studenti sviluppino una metodologia e delle procedure per risolvere questi problemi.

1.2 La tecnica corretta per la risoluzione dei problemi

Nessuna metodologia di risoluzione può coprire completamente tutti i problemi che si incontrano quando si lavora con le reti wireless. Ma, spesso, i problemi si riducono ad uno degli errori più comuni. Qui vengono elencati pochi semplici punti da tenere a mente per far lavorare nella giusta direzione i propri sforzi per la soluzione dei problemi.

- **Non andare in panico.** Se si risolvendo i problemi di un sistema, significa che il sistema ha lavorato una volta, probabilmente molto di recente. Prima di iniziare a fare modifiche bisogna analizzare la scena e stabilire esattamente cosa s'è rotto. Se si hanno a disposizione log storici o statistiche da cui partire sarà meglio. Bisogna assicurarsi primadituttо di raccogliere tutte le informazioni in modo da poter prendere decisioni informate prima di fare modifiche.
- **E' connesso?** Questo passo viene spesso sorvolato fino a quando molte altre strade sono percorse. I connettori possono essere accidentalmente (o intenzionalmente) disconnessi molto faclimente. Il cavo è connesso ad una buona sorgente di corrente? L'altro capo è connesso al dispositivo? La spia di accensione è accesa? Può sembrare sciocco ma ci sentiremmo ancora più sciocchi dopo aver speso un sacco di tempo a controllare la linea di alimentazione di un'antenna per poi scoprire che l'AP era sconnesso dall'inizio. Accade molto più spesso di quanto saremmo disposti ad ammettere.
- **Cos'è l'ultima cosa che è cambiata?** Se si è l'unici ad avere accesso al sistema, qual'è l'ultima modifica che abbiamo effettuato? Se vi hanno accesso anche altri, qual'è l'ultima modifica che hanno fatto e quando? Quand'è stata l'ultima volta che il sistema ha funzionato? Spesso le modifiche al sistema hanno conseguenze non intenzionali che possono non essere notate immediatamente. Si può annullare le ultime modifiche e vedere che effetto hanno sul problema.
- **Fare un backup.** Questo si applica prima di aver notato un problema, ma anche dopo. Se si effettua un complesso cambio di software in un sistema, avere un backup significa che sarà possibile ripristinare velocemente le vecchie impostazioni e ricominciare. Quando si analizzano problemi molto complessi, avere una configurazione che "più o meno" funziona può essere molto meglio di avere un pasticcio che non funziona affatto (e che non si può facilmente ripristinare).
-  **Quello buono** . Quest'idea è applicabile all'hardware così come al software. Un ***quello buono*** è un componente che si può sostituire in un sistema complesso per verificare che la sua controparte è in buone condizioni di funzionamento. Ad esempio ci si può portare un cavo Ethernet testato nella nostra cassetta degli attrezzi. Se si sospettano problemi con un cavo sul campo, potremmo facilmente sostituire il cavo sospetto con quello buono e vedere se le cose migliorano. E' più semplice e meno a rischio di errori che crimpare di nuovo un cavo, e ci dice immediatamente se la sostituzione risolve il problema. Allo stesso modo, ci si può portare anche una batteria di backup, un cavo antenna o un CD-ROM con una configurazione valida per il sistema. Quando si risolvono problemi complicati, salvare il lavoro ad un certo punto ci permette di tornare ad una situazione stabile anche se il problema non è ancora del tutto risolto.
- **Cambiare una variabile alla volta.** Quando si è sotto pressione per ripristinare un sistema guasto, si è tentati di saltare in avanti e cambiare molte variabili con una volta. Se si fa questo, e le modifiche sembrano risolvere il problema, non saremo mai in grado di capire esattamente cos'ha causato il problema inizialmente. O, ancor peggio, le modifiche potrebbero risolvere il problema originario e portare a conseguenze inaspettate che guastino altre parti del sistema. Modificando le variabili una alla volta, è possibile capire con precisione cos'è andato storto all'inizio e vedere gli effetti diretti delle modifiche effettuate.
- **Non fare danni.** Se non si è capito appieno come funziona un sistema, non bisogna temere di chiamare un esperto. Se non si è sicuri se una particolare modifica danneggi un'altra parte del sistema, allora bisogna trovare qualcuno con più esperienza o escogitare un modo per testare le modifiche senza fare danni. Mettere un penny al posto di un fusibile può risolvere il problema nell'immediato, ma può anche far bruciare il palazzo.

Non è plausibile che le persone che progettano la rete restino a telefono 24 ore al giorno per risolvere i problemi quando arrivano. Il team di troubleshooting deve avere buone capacità di soluzione dei problemi ma potrebbe non essere competente abbastanza per configurare un router da zero o crimpare un pezzo di LMR-400. E' spesso molto più efficiente avere una serie di componenti di backup a portata di mano e addestrare il team a sostituire l'intera parte guasta. Questo può significare avere un access point o un router preconfigurati e chiusi in un armadietto, chiaramente etichettati e con i cavi e gli alimentatori di backup. Il team può sostituire il componente guasto e spedirlo ad un esperto per la riparazione, o fare in modo di farsi spedire un'altro componente di backup. Mantenendo al sicuro le componenti di backup e rimpiazzandole quando vengono usate si può far risparmiare un sacco di tempo a tutti.

1.3 Problemi di rete comuni

Spesso i problemi di connettività sono causati da componenti guaste, maltempo o semplicemente cattive configurazioni. Una volta che la nostra rete è connessa ad Internet o aperta al pubblico, una considerevole serie di minacce arriveranno dagli stessi utenti della rete. Queste minacce spaziano dal benigno al totalmente maligno ma avranno tutte impatto sulla rete se non è correttamente configurata. Questa sezione riguarda alcuni problemi comunemente riscontrabili una volta che la rete venga usata dalla razza umana attuale.

1.3.1 Siti ospitati localmente

Se un'università ospita il suo sito web localmente, i visistatori del sito all'esterno del campus e nel resto del mondo si contenderanno la banda Internet con lo staff dell'università. A questi si aggiungono gli accessi automatici degli ***spider*** dei motori di ricerca che periodicamente scansioneranno l'intero sito. Una soluzione a questo problema è di usare uno split DNS ed un mirror. L'università replicherà una copia del suo sito su di un server, diciamo, di una compagnia di hosting Europea, ed utilizzerà uno split DNS per redirigere tutti gli utenti esterni alla rete universitaria verso il sito mirror, mentre gli utenti interni alla rete universitaria accederanno allo stesso sito localmente. I dettagli su come effettuare questa configurazione sono forniti nel capitolo tre.

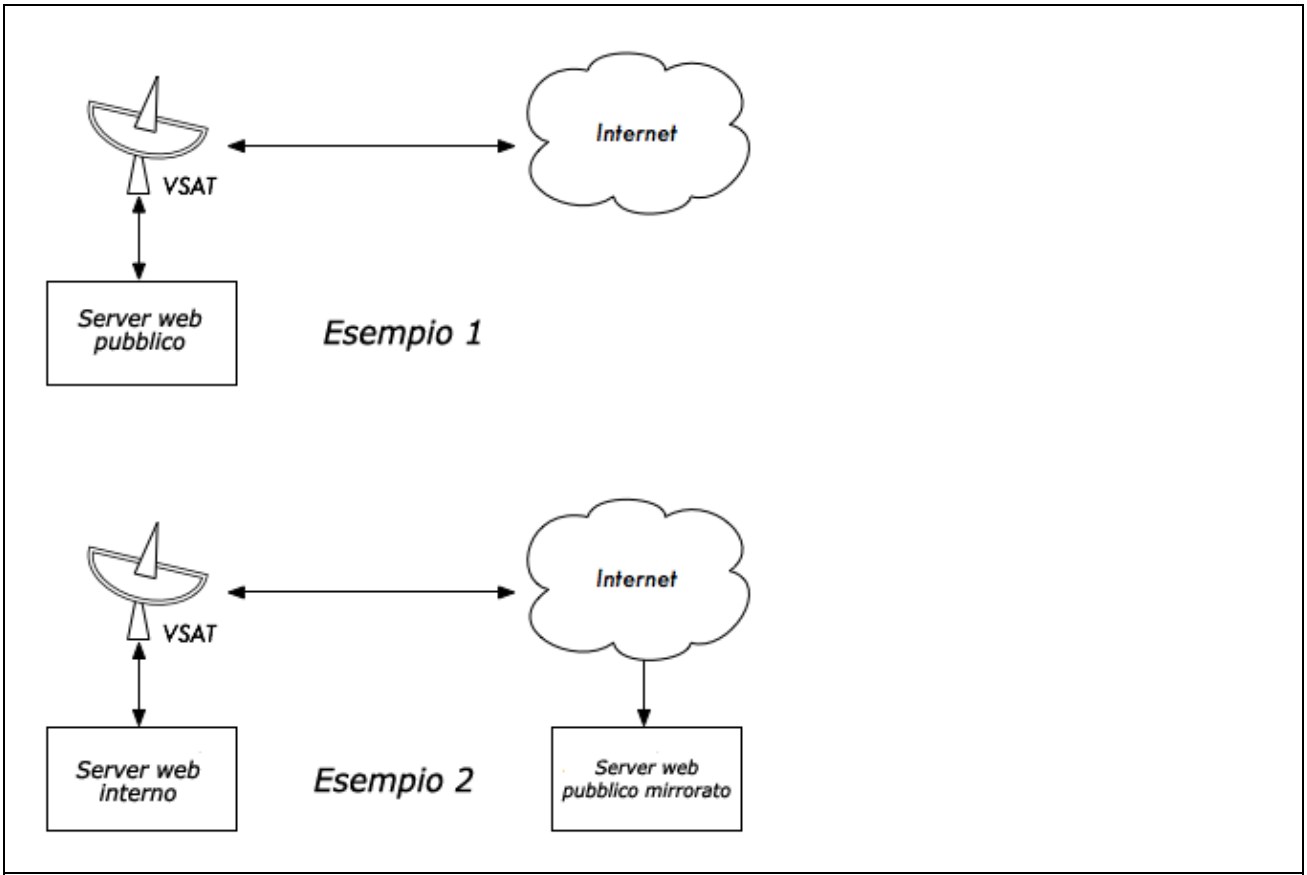

Figura 8.1: Nell'Esempio 1, tutto il traffico del sito web che proviene da Internet deve attraversare il VSAT. Nell'Esempio 2 il sito web pubblico è ospitato su un servizio Europeo e viene mantenuata una copia su di un server interno per accessi locali molto veloci. Questa configurazione migliora la connessione VSAT e riduce i tempi di caricamento per gli utenti del sito web.

1.3.2 Proxy aperti

Un server proxy dovrebbe esser configurato per accettare solo connessioni provenienti dalla rete dell'università, non dal resto di Internet. Questo per evitare che altre persone vi si connettano ed utilizzino il proxy aperto per una serie di scopi come l'evitare di pagare collegamenti internazionali. Il modo di

configurarlo dipende dal tipo di proxy server che si utilizza. Ad esempio è possibile specificare il range di indirizzi IP utilizzati nella rete del campus. ⚠ LA FRASE è INCOMPLETA NELLA VERSIONE ORIGINALE! ⚠

1.3.3 /!\ Host a ritrasmissione aperta (Open relay hosts) /!\

Un server mail mal configurato sarà scovato dalle persone senza scrupoli di Internet e usato come macchina di ritrasmissione per ⚠ email di massa ⚠ e spam. Lo fanno per nascondere la vera sorgente dello spam ed evitare di essere scoperti. Per trovare host che inoltrano apertamente (open relay host n.d.t.) i test seguenti dovrebbero essere eseguiti sul vostro mail server (o sul server SMTP che lavora come relay host sul perimetro della rete del campus). Usare ***telnet*** per aprire una connessione alla porta 25 del server in questione (con alcune versioni di Windows telnet potrà esser necessario digitare 'set local_echo' per rendere visibile il testo):

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

Quindi, se è possibile aprire una sessione da linea di comando (come nell'esempio che segue), il server è un host open relay:

```
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 ¶
```

In caso contrario, la risposta al primo MAIL FROM dovrebbe essere qualcosa del tipo:

```
550 Relaying is prohibited.
```

All'indirizzo http://www.ordb.org/ è disponibile anche un tester online. Il sito contiene anche informazioni su questa problematica. Dal momento che le i ⚠ bulk emailers ⚠ hanno sistemi automatizzati per trovare questi host open relay, un'organizzazione che non protegge il proprio sistema email ha quasi la certezza che il proprio server venga trovato ed abusato. Configurare un server mail per non essere un open relay host consiste nello specificare le reti e gli host che sono autorizzati ad inoltrare le email tramite il suo MTA (Sendmail, Postfix, Exim, o Exchange). Tipicamente si specifica il range di indirizzi della rete del campus.

1.3.4 Peer-to-peer networking

L'abuso di banda dei programmi di scambio file su peer-to-peer (P2P) come Kazaa, Morpheus, WinMX e BearShare può essere prevenuto nei modi seguenti:

- **Rendere impossibile installare programmi nuovi sui computer del campus.** Evitando di dare accessi amministrativi ad utenti normali delle workstation e PC, è possibile evitare l'installazione di programmi come Kazaa. Molte istituzioni standardizzano una configurazione tipo installando il sistema operativo e tutte le applicazioni necessarie su di un PC, e configuranole in modo ottimale. Il PC viene configurato anche in modo da impedire agli utenti di installare nuove applicazioni. L'immagine del disco di questo PC viene poi clonata verso tutti gli altri PC usando programmi come Partition Image (vedi http://www.partimage.org/) o Drive Image Pro (vedi http://www.powerquest.com/).
- **Bloccare questi protocolli non è una soluzione.** Kazaa ed altri protocolli sono bravi abbastanza da attraversare porte bloccate. Kazaa utilizza normalmente la porta 1214 per la connessione iniziale ma

se questa non è disponibile proverà ad usare le porte dalla 1000 alla 4000. Se anche queste sono bloccate, usa la porta 80, rendendosi simile al traffico web. Per questa ragione gli ISP non lo bloccano ma lo "moderano", usando dei prodotti di bandwidth-manager (vedi capitolo tre).

- **Se la moderazione non è un'opzione, cambia il layout di rete.** Se il server proxy ed i server email sono configurati con due schede di rete (come descritto nel capitolo tre) e questi server non sono configurati per inoltrare nessun pacchetto, essi bloccheranno tutto il traffico P2P. Bloccheranno anche tutti gli altri tipi di traffico come Microsoft NetMeedting, SSH, programmi di VPN e tutti gli altri servizi non espressamente permessi dal server proxy. In reti con poca banda si può decidere che la semplicità di questa implementazione sia più importante degli svantaggi. Un decisione del genere potrebbe essere necessaria, ma non dovrebbe essere presa facilmente. Gli amministratori di rete semplicemente non possono prevedere che utilizzo innovativo gli utenti faranno di una rete. Bloccando categoricamente gli accessi, impediremo agli utenti di utilizzare ogni servizio (compreso quelli che occupano poca banda) che il proxy non supporta. Anche se questo può essere ideale in circostanze di banda estremamente piccola, non dovrebbe mai esser considerata una regola di accesso in generale.

1.3.5 Programmi che si installano da soli (tramite Internet)

Esistono programmi che si installano da soli automaticamente e poi continuano ad usare banda come, ad esempio, il cosiddetto Bonzi-Buddy, il Microsoft Network ed alcuni tipi di worm. Alcuni di questi programmi sono spyware e continuano ad inviare informazioni sulle abitudini di navigazione dell'utente ad aziende da qualche parte in Internet. Questi programmi sono prevedibili in qualche caso con l'educazion dell'utente e bloccando il PC per prevenire accessi amministrativi per utenti normali. In altri casi, ci sono soluzioni software per trovare e rimuovere questi programmi problematici, come Spychecker (http://www.spychecker.com/), Ad-Aware (http://www.lavasoft.de/), o xp-antispy (http://www.xp-antispy.de/).

1.3.6 Aggiornamenti di Windows

Gli ultimi sistemi operativi Microsoft Windows danno per scontato che un computer con una connessione LAN abbia un buon collegamento ad Internet e automaticamente scaricano patch di sicurezza, bug fix ed aggiornamenti dal sito Web della Microsoft. Questo può consumare la gran parte della banda a disposizione su collegamenti economici a Internet. I due approcci possibili a questo problema sono:

- **Disabilitare Windows updates su tutti i PC e workstation.** Gli aggiornamenti di sicurezza sono molto importanti per i server ma se per le workstation che risiedono in reti private e protette come una rete campus, il loro bisogno è dubbio.
- **Installare un server Software Update.** E' un programma Microsoft gratuito che consente di scaricare tutti gli update dalla Microsoft di notte su di un server locale e da lì distribuirli a tutte le workstation client. In questo modo gli aggiornamenti di Windows non utilizzeranno alcuna banda Internet durante il giorno. Sfortunatamente, tutti i PC client devono essere configurati per usare il server Software Update locale affinchè questo abbia un effetto. Se si hanno a disposizione DNS server flessibili, si può anche configurarli per rispondere alle richieste per windowsupdate.microsoft.com e redirigerle verso il server di aggiornamento locale. Sembra solo un buon rimedio per grandi reti ma può risparmiare una quantità indicibile di banda Internet

Bloccare il sito di aggiornamento di Windows sul proxy server non è una buona soluzione perchè il servizio di aggiornamento di Windows (Aggiornamento Automatico) continua a riprovare sempre più aggressivamente, e se lo fanno tutte le workstation, il proxy server sarà pesantemente caricato. L'estratto seguente proviene dal log del proxy (log accessi di Squid) dove è stato impostato di bloccare i file cabinet di Microsoft (.cab).

Gran parte del log di Squid appare così:

```
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 ¶
```

Anche se questo può essere tollerabile per pochi client, il problema cresce significativamente man manco che gli host si aggiungono alla rete. Invece che forzare un proxy a servire richieste che falliranno sempre, ha molto più senso redirigere i client Software Update verso un server di aggiornamento locale.

1.3.7 Programmi che presuppongono una gran disponibilità di banda

Oltre Windows updates, molti altri programmi e servizi fanno conto che la banda non sia un problema e, per questo, consumano banda per ragioni che l'utente non può prevedere. Ad esempio i pacchetti antivirus (come il Norton antivirus) si aggiorna periodicamente in modo automatico da Internet. Sarebbe meglio che questi aggiornamenti fossero distribuiti da un server locale.

Altri programmi, come il video player RealNetworks, scaricano automaticamente aggiornamenti e pubblicità, ma fanno anche l'upload delle abitudini d'uso verso un sito su Internet. Applet dall'aspetto innocuo (come Konfabulator e Dashboard widgets) contattano continuamente degli host in Internet per avere informazioni aggiornate. Si può trattare di richieste con una piccola esigenza di banda (come gli aggiornamenti sul tempo o sulle notizie), o di richieste molto più onerose (come le webcam). Potrebbe essere necessario moderare queste applicazioni o bloccarle del tutto.

Le ultime versioni di Windows e Mac OS X hanno anche un servizio di sincronizzazione del tempo. Connettendosi a time server su Internet, il servizio assicura la precisione dell'ora mostrata dall'orologio del computer. E' meglio installare un time server locale e distribuire il segnale orario esatto da lì invece che sprecare la banda verso Internet con queste richieste.

1.3.8 Traffico Windows sul collegamento ad Internet

I computer Windows comunicano tra loro tramite il ***NetBIOS*** e il ***Server Message Block*** (***SMB***). Questi protocolli si lavorano sopra il TCP/IP o altri protocolli di trasporto. Si tratta di un protocollo che usa un processo di ***elezione*** per determinare quale computer sarà il ***master browser***. Il master browser è un computer che mantiene la lista di tutti gli altri computer, condivisioni e stampanti che si possono vedere in ***Risorse di Rete*** o ***Connessioni di Rete***. Le informazioni riguardo le condivisioni disponibili sono anche inviate a tutti (broadcast) ad intervalli regolari.

Il protocollo SMB è pensato per le LAN ed è fonte di problemi nel momento in cui il computer Windows è connesso ad Internet. Se il traffico SMB non è filtrato tenderà a propagarsi attraverso il collegamento ad Internet, sprecando la bandwidth dell'organizzazione. Le seguenti misure possono essere adottati per prevenire questo comportamento:

- **Bloccare il traffico SMB/NetBIOS in uscita sul router o firewall perimetrale.** Questo traffico consumerà la banda Internet e, ancora peggio, espone a potenziali rischi di sicurezza. Molti worm Internet e tool di penetrazione cercano attivamente di trovare condivisioni SMB aperte e di exploitare queste connessioni per avere un accesso alla nostra rete.
- **Installare ZoneAlarm su tutte le workstation (non il server)**. Una versione gratuita la si può trovare all'indirizzo http://www.zonelabs.com/. Questo programma permette all'utente di scegliere quale applicazione può connettersi ad Internet e quale no. Internet Explorer, ad esempio, deve connettersi ad Internet ma Windows Explorer no. ZoneAlarm può impedire a Windows Explorer di farlo.
- **Ridurre le condivisioni di rete.** Teoricamente solo il file server dovrebbe avere delle condivisioni. E' possibile usare programmi come SoftPerfect Network Scanner (http://www.softperfect.com/) per trovare facilmente tutte le condivisioni della nostra rete.

1.3.9 Worms e virus

Worm e virus possono generare una quantità enorme di traffico. Il worm W32/Opaserv, ad esempio, è ancora presente nonostante sia piuttosto vecchio. Si diffonde tramite le condivisioni Windows e viene rilevato dalle altre persone in Internet perchè tenta di diffondersi ancora. Per questo è essenziale che una protezione antivirus sia installata su di ogni PC. Così come è essenziale far capire all'utente i rischi connessi all'esecuzione degli allegati e al rispondere alle email non attese. Bisognerebbe osservare la regola di non tenere alcun servizio non utilizzato su workstation e server. Un PC non dovrebbe avere condivisioni di rete se non fa da file server; un server, a sua volta, non dovrebbe eseguire servizi non necessari. I server Windows e Unix, ad esempio, hanno normalmente attivi i servizi di web server. Questi servizi dovrebbero essere disabilitati qualora i server ricoprano un'altra funzione; meno servizi sono attivi su un computer, meno possibilità di "exploit" ci saranno.

1.3.10 Inoltri ciclici di email

Talvolta i problemi possono essere causati da un singolo utente. Prendiamo ad esempio il caso di un utente il cui account all'università è configurato per inoltrare tutta la posta al suo account su Yahoo. L'utente va in vacanza. Tutte le email speditegli durante la sua assenza vengono ancora inoltrate all'account su Yahoo che è limitato a soli 2 MB. Quando la casella su Yahoo si riempie, inizia a far rimbalzare le email indietro verso l'account dell'università, che immediatamente le re-inoltra indietro verso la casella Yahoo. In questo modo si crea un ciclo di email in grado di inviare centinaia di migliaia di email avanti e indietro, generando un grosso traffico capace di compromettere i mail server.

Esistono funzionalità per alcuni programmi di mail server in grado di riconoscere questi cicli o loop. Dovrebbero essere attivi per default. Gli amministratori dovrebbero assicurarsi di non disattivare queste funzionalità per errore, e di evitare di installare SMTP forwarder che modificano l'intestazione (header n.d.t.) delle email con il risultato che il mail server non riesca a riconoscere il loop di email.

1.3.11 Download di file di grandi dimensioni

Un utente può avviare molti download contemporaneamente, o scaricare file di grandi dimensioni come le immagini ISO da 650 MB. In questo modo, un singolo utente può utilizzare la maggior parte della banda. La soluzione a questo tipo di problema si può trovare con il training, download offline e monitoring (compreso il monitoring in tempo reale come spiegato nel capitolo sei). Il download offline può essere implementato in almeno due modi:

- All'Università di Moratuwa, è stato implementato un sistema di redirezione degli URL. Gli utenti che accedono ad URL **ftp://** vedono comparire elenco di directory con due collegamenti per ogni file elecanto: uno per il download normale, e l'altro per il download in tempo differito. Se viene selezionato il link per il download offline, il file selezionato viene accodato per il download in un tempo successivo e l'utente viene notificato tramite email del completamento del download. Il sistema tiene in cache i file scaricati recentemente per metterli a disposizione immediatamente se richiesti di nuovo. La coda di download è ordinata per dimensione dei file. Per questo i file piccoli vengono scaricati per primi. Dato che parte della banda è allocata per questi sistemi anche durante le ore di picco, gli utenti che richiedono file piccoli possono riceverli in pochi minuti, a volte anche più velocemente che scaricandoli direttamente.
- Un altro approccio potrebbe essere di creare un'interfaccia web dove gli utenti inseriscono l'URL del file che vogliono scaricare. Il file viene scaricato di notte con un ***cron job*** o operazione pianificata. Questo sistema funziona però solo con utenti pazienti e che conoscono la dimensione dei file che potrebbe essere problematico scaricare durante la giornata lavorativa.

1.3.12 Inviare file di grandi dimensioni

Quando gli utenti devono spedire file di grandi dimensioni a collaboratori da qualche parte su Internet, dovrebbe venir loro mostrato come schedulare l'upload. In Windows, l'upload ad un server FTP remoto può essere fatto utilizzando uno script FCP che consiste in un file di testo che contiene i comandi FTP, qualcosa di simile all'esempio seguente (salvato come **`c:\ftpscript.txt`**):

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

Per eseguirlo, al prompt dei comandi basta digitare:

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

Su computer con Windows NT, 2000 e XP il comando può essere salvato in un file del tipo **`transfer.cmd`**, e schedulato per essere eseguito di notte utilizzando la funzione Scheduled Tasks - Operazioni Pianificate (Avvio -> Impostazioni -> Pannello di Controllo -> Operazioni Pianificate). In Unix, lo stesso risultato può essere ottenuto utilizzando ***at*** o ***cron***.

1.3.13 Utenti che scambiano file

Gli utenti spesso desiderano scambiarsi file di grandi dimensioni. Se il destinatario è locale, può risultare molto dispendioso, in termini di banda, inviare questi file tramite Internet. Sui server Windows / Samba / Web o Novell dovrebbero esser create delle cartelle condivise dove gli utenti possano mettere file di grandi dimensioni per scambiarli con gli altri utenti.

Altrimenti è possibile scrivere un front-end web che accetti grandi file e li ospiti in un'area di download. Dopo aver fatto l'upload, l'utente riceve un URL che punta al file. A questo punto potrà dare questo URL ai suoi collaboratori locali o internazionali che potranno effettuare il download del file tramite l'URL fornita. Questo è ciò che l'Università di Bristol ha realizzato con il suo sistema FLUFF. L'Università offre strutture per l'upload di grandi file (FLUFF) disponibili tramite http://www.bristol.ac.uk/fluff/. A questi file può accedere chiunque conosca la loro posizione. Il vantaggio di quest'approccio è che gli utenti possono dare agli utenti esterni l'accesso ai loro file, mentre il metodo della condivisione di rete può andar bene solo per gli utenti interni al campus. Un sistema di questo tipo può essere implementato facilmente con uno script CGI utilizzando Python e Apache.