ISTITUTO NAZIONALE DI FISICA NUCLEARE

Sezione di Torino

INFN/TC-00/08
30 Maggio 2000

SERVIZIO DI ACCESSO DIAL-UP

Stefano Lusso[1]

[1)]*INFN-Sezione di Torino, Via P. Giuria 1, I-10125 Torino, Italy*

Abstract

Questo documento riporta la procedura utilizzata per la realizzazione di un servizio di accesso dial-up.

Il servizio dial-up consente all'utente il collegamento alla rete di istituto tramite linea telefonica. Il servizio è costituito essenzialmente da quattro componenti: una linea telefonica, un modem, un server di accesso ed un server di autenticazione. Le configurazioni possono variare a seconda delle esigenze e della disponibilità hardware.

Nel documento si analizza la configurazione di un router Cisco e l'installazione di un server di autenticazione (XTACACS) e la sua configurazione su di un server UNIX. Sono riportate inoltre alcune soluzioni adottate per la gestione degli utenti.

Published by ***SIS–Pubblicazioni***
Laboratori Nazionali di Frascati

1 INTRODUZIONE

La necessità di accedere alla rete di istituto dall'esterno ha reso necessario l'attivazione di un servizio di accesso dial-up con protocollo PPP (Point to Point Protocol). Sempre di più si ha l'esigenza di utilizzare le risorse informatiche dell'istituto senza recarsi sul posto di lavoro. I casi sono molteplici: l'accesso alla posta elettronica, il controllo di programmi di analisi o simulazioni, il trasferimento di documenti ed anche la semplice consultazione di pagine web.

In questo scenario il calcolatore esterno è come se fosse connesso alla LAN dell'istituto con caratteristiche di velocità e sicurezza non raggiungibili con gli Internet Service Provider commerciali.

Questo documento tecnico riporta la procedura seguita nell'implementazione del servizio trattando della configurazione del router di accesso, del server di autenticazione e della gestione degli utenti.

Le configurazione fa uso di un Accesso Primario ISDN (PRI), un router Cisco della serie 3600 (3620) con modem digitali integrati ed un Alpha Server 1000/A con Sistema Operativo Digital UNIX 4.0D per l'autenticazione.

2 CONFIGURAZIONE DEL ROUTER CISCO

Il server di accesso alla rete è rappresentato dal router Cisco. Esso deve avere, oltre all'interfaccia ISDN PRI, almeno una interfaccia ethernet (nel nostro caso FastEthernet) collegata alla LAN dell'istituto. Nel router Cisco è integrata una batteria di modem digitali in grado di supportare lo standard ITU V.90 56K[1] sui quali vengono deviate le chiamate provenienti da linee telefoniche non digitali. Questi modem sono in grado di negoziare la velocità di trasmissione con un qualunque modem convenzionale. La configurazione del router riflette questa doppia funzionalità: l'interfaccia **Group-Async** si riferisce infatti alle connessioni analogiche mentre l'interfaccia **Dialer** è legata alle connessioni ISDN.

Per la configurazione del router occorre necessarimente possedere i privilegi di amministratore (enable password); nel caso si tratti di un router nuovo si sconsiglia la procedura di configurazione automatica in quanto non permette di configurare già da subito parametri importanti ed introduce confusione.

2.1 Configurazione generale del router

Nella tabella 1 è riportata la configurazione dei parametri principali del router Cisco.

[1] Uno standard per la trasmissione di dati su linea telefonica con velocità fino a 56 Kbps introdotto dall'International Telecommunications Union (ITU), un comitato delle Nazioni Unite creato per assicurare interoperabilità tra le varie apparecchiature per telecomunicazioni.

TAB. 1: Parametri principali del router Cisco

```
Current configuration:
!
version 12.0
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname cisco-dialup
!
boot system flash:c3620-i-mz.120-5.T1
enable secret 5 $1$pCz8$oSdBMacirHZVADynF9432.
!
ip subnet-zero
ip domain-name domain.it
ip name-server name.server.ip.address
!
ip audit notify log
ip audit po max-events 100
ip classless
no ip http server
!
logging facility daemon
logging ip.del.syslog.server
line con 0
 transport input none
line aux 0
line vty 0 4
 password 7 13021600794114272569 2123
 login
!
ntp clock-period 17180193
ntp server ip.del.server.ntp
end
```

La lista dei parametri elencati in TAB.1 è il risultato del comando **# write terminal** dato sulla console del router. Il simbolo **#** indica che si devono possedere i privilegi di amministratore per poter dare il comando. Il parametro **version 12.0** indica la versione del sistema operativo detto Internetwork Operating System (IOS). La linea **service timestamps log datetime msec localtime show-timezone** fa in modo che i messaggi di log rechino il timestamp con la data e l'ora (**datetime**) con la precisione del millisecondo (**msec**) relativo alla timezone locale (**localtime**) che viene indicata (**show-timezone**). Abilitando il **service**

password-encryption si ottiene la cifratura delle password quando viene visualizzata la configurazione. Il sistema assume il nome "cisco-dialup" per effetto del comando **hostname cisco-dialup;** il prompt diviene così **cisco-dialup> .**
Il router Cisco può caricare il sistema operativo (IOS) sia da una memoria flash presente a bordo sia da un server tftp. La linea **boot system flash:c3620-i-mz.120-5.T1** specifica che il sistema operativo viene caricato dalla memoria flash e che il file si chiama c3620-i-mz.120-5.T1.

La password privilegiata (enable password) è necessaria per compiere qualunque operazione che modifica la configurazione del router. Con il comando **enable secret 5 1pCz8$oSdBMacirHZVADynF9432.** si definisce la password cifrata secondo un algoritmo proprietario Cisco. Al momento attuale l'unico tipo di cifratura possibile è 5.

L'istruzione **ip domain-name domain.it** assegna al router un nome di dominio IP di default. Esso completerà i nomi degli host usando questo domino (domain.it). Per la risoluzione dei nomi il router si rivolgerà al nameserver specificato dal comando **ip name-server name.server.ip.address.**

Il router è in grado di inviare delle segnalazioni ad un calcolatore sul quale è stato attivato un syslog daemon (**ip audit notify log**). Nel nostro caso il massimo numero di eventi immagazzinati nella memoria del router è lasciato al valore di default (**ip audit po max-events 100)**. Utilizzando il syslog daemon di un calcolatore è possibile definire la *facility* ovvero la categoria sotto la quale raccogliere i messaggi inviati dal router. Le linee **logging facility daemon** e **logging ip.del.syslog.server** significano quindi che al server ip.del.syslog.server verranno inviati tutti i messaggi che questo classificherà con la *facility* daemon.

Per utilizzare al meglio il range di indirizzi IP di cui si dispone si usa sia dividere un network in più sottoreti sia aggregare più network contigui per formare una supernet. Con il comando **ip classless** si forza il sistema operativo ad inoltrare i pacchetti destinati ad una sottorete di un network di cui non si hanno informazioni di routing specifiche verso il percorso di default per la supernet che contiene la sottorete.

Sul router Cisco è possibile attivare un server che consente la sua configurazione per mezzo del protocollo http. Poiché, per ragioni di sicurezza, è bene disattivare tutti i servizi non necessari e questo servizio non risulta necessario viene disabilitato dal comando **no ip http server.**

Il sistema operativo dei router Cisco (IOS) associa alle porte fisiche o virtuali di accesso un particolare tipo di linea di connessione[1]. Gli oggetti Cisco (router o access server) possono avere quattro tipi di linee: console (**con**), auxiliaria (**aux**), asincrona (**tty**) e terminale virtuale (**vty**). La loro presenza e numerazione dipende dal modello di router. La porta di console (**line con 0**) è configurata in modo da non permettere di selezionare nessun protocollo (**transport input none**). In questo modo la porta risulta inutilizzabile per qualsiasi collegamento che non sia il terminale di console. La porta ausiliaria (**aux 0**) può essere utlizzata come porta di connessione di back-up dall'esterno per esempio attraverso un modem. Nel nostro caso non viene utilizzata. Risultano invece configurati 5 terminali virtuali

(**vty 0 4**) per connessioni remote, per esempio via telnet. La password di accesso è cifrata e consente l'accesso al livello di privilegio 7 (**password 7 13021600794114272569212 3).** I livelli di privilegio sono 16 e vanno da 0 a 15 che corrisponde al livello enable. Il livello 7 consente di visualizzare lo stato delle interfacce e gli utenti collegati ma non permette di cambiare la configurazione.

2.2 Configurazione delle interfacce ISDN

Nella tabella 2 sono riportati i parametri del router Cisco che si riferiscono alle interfacce ISDN.

L'accesso primario ISDN (PRI) comprende in Europa l'insieme di 30 canali B (Bearer) ciascuno operante a 64Kbps più 1 canale D anch'esso a 64Kbps utilizzato per la segnalazione. La connessione del router al flusso primario ISDN avviene tramite un interfaccia denominata controller E1 nel caso europeo (T1 negli Stati Uniti). Al canale D, invece, ci si riferisce specificando l'interfaccia serial0:15. L'interfaccia dialer è una interfaccia logica che raggruppa le interfacce fisiche. Essa è collegata ai singoli canali B e conserva le configurazioni per il canale D.

Nel nostro caso, trovandoci in Europa, il controller non può che essere un **controller E1 0/0** (0/0 indica la posizione fisica dell'interfaccia nel router). Il comando **pri-group timeslots 1-31** specifica un singolo range di valori da 1 a 31 per la distribuzione dei timeslot della linea E1 collegata. La configurazione dei timeslot deve concordare con quella degli switch nella centrale telefonica. Questa varia a seconda dell'area geografica. Ci sono ben tre tipi di switch nell'area nordamericana, uno per il Giappone ed uno per l'Europa. Lo **switch-type primary-net5**, che è lo switch ISDN PRI europeo, utilizza il sistema di segnalazione Euro-ISDN E-DSS1ed è conforme alle norme ETSI.

Analizziamo ora i parametri relativi alle interfacce fisiche (**interface Serial0/0:15**) del controller ISDN. Per utilizzare il minor numero possibile di indirizzi IP non si attribuisce nessun indirizzo all'interfaccia (**no ip address**). A partire dalla versione 12.0 del sistema operativo (IOS) è possibile interdire tutti i broadcast IP con il comando **no ip directed-broadcast**. Questo comando risulta molto utile perché consente di evitare di inoltrare pacchetti IP in broadcast la cui risposta può portare al collasso la rete[1]. Il meccanismo del Weighted Fair Queueing (WFQ) permette di definire priorità nelle code dei pacchetti in entrata su di una interfaccia. In questo modo quando si supera una certa soglia i pacchetti cominciano ad essere eliminati. Nel nostro caso il meccanismo non è abilitato (**no fair-queue**).

[1] Tristemente famosi sono gli attacchi *smurf* dove l'invio di un pacchetto ICMP (ping) in broadcast produce una risposta amplificata verso l'indirizzo IP di partenza.

TAB. 2: Parametri relativi alle connessioni ISDN del router Cisco

```
!
isdn switch-type primary-net5
!
controller E1 0/0
 pri-group timeslots 1-31
 description Accesso ISDN primario (# telefono)
!
interface Serial0/0:15
 description D channel interface (E1 ==> serial0:15)
 no ip address
 no ip directed-broadcast
 encapsulation ppp
 ip tcp header-compression passive
 dialer rotary-group 1
 isdn switch-type primary-net5
 isdn incoming-voice modem
 no fair-queue
!
interface Dialer1
 description Parent Interface for the 2 ISDN D channels
 ip unnumbered FastEthernet0/0
 no ip directed-broadcast
 encapsulation ppp
 ip tcp header-compression passive
 dialer in-band
 dialer idle-timeout 300
 dialer-group 1
 peer default ip address pool ISDN-nomepool
 no fair-queue
 ppp authentication pap
 ppp use-tacacs
 ppp multilink
```

Per permettere alle chiamate di tipo *voce* su ISDN, cioè quelle effettuate da modem analogici convenzionali, è necessario inserire il comando **isdn incoming-voice modem**.

Con **encapsulation ppp** si definisce il tipo di incapsulamento per l'interfaccia seriale a Point-to-Point Protocol (PPP).

Per aumentare la banda disponibile è possibile utilizzare la compressione dell'header TCP utilizzando l'algoritmo di Van Jacobson[2]. L'aumento della banda dipende fortemente dal tipo di traffico effettuato sulla linea. Con **ip tcp header-compression passive** questa

opzione è abilitata.

L'interfaccia Serial0/0:15 viene collegata logicamente all'interfaccia Dialer1 dal comando **dialer rotary-group 1**.

Dopo le interfacce fisiche viene l'interfaccia logica (**interface Dialer1)** alla quale sono attribuita le configurazioni globali per i canali D ISDN. Anche l'interfaccia Dialer1 non ha indirizzo ip proprio, assume quello dell'interfaccia FastEthernet0/0 (**ip unnumbered FastEthernet0/0**). L'indirizzo IP del peer, cioè del sistema che si connette all'interfaccia, viene assegnato in modo dinamico attingendolo da un insieme di indirizzi denominato pool (**ISDN-nomepool**) e definito nella configurazione.

Il comando **dialer in-band** specifica che è supportato il *dial-on-demand routing* (DDR). Questo significa che la comunicazione è stata iniziata dall'utente remoto e consente al sistema operativo di disconnettere la linea dopo un certo periodo di inattività (idle time) perchè possa essere riutilizzata. Il periodo di 300 secondi (5 minuti) è ragionevole (**dialer idle-timeout 300**).

Specificando il **dialer-group 1** si fa riferimento ad una dialer-list 1 che è legata ad una Access Control List (ACL). In questo modo si possono abilitare dei filtri per eliminare protocolli indesiderati.

L'autenticazione viene effettuata mediante il Password Authentication Protocol (PAP)[3] ed è abilitata sull'interfaccia **Dialer1** dal comando **ppp authentication pap**. Al sistema remoto vengono quindi richiesti uno username ed una password da validare tramite un server TACACS (**ppp use-tacacs**).

Per consentire l'aggregazione di più canali ISDN è necessario abilitare il **ppp multilink.**

2.2 Configurazione delle interfacce analogiche

Dopo aver trattato delle connessioni ISDN occorre analizzare le configurazioni relative alle connessioni su linea analogica. Nella tabella 3 sono elencati i parametri relativi alle connessioni su modem.

Le configurazioni delle interfacce **Dialer1 e Group-Async1** sono sostanzialmente simili. L'interfaccia **Group-Async1** va considerata come una tipica interfaccia asincrona. Per configurare una interfaccia seriale asincrona su di un device è necessario settare l'interfaccia in modo tale che possa inviare pacchetti PPP o SLIP[1] (Serial Line Internet Protocol). L'interfaccia può essere configurata in modalità di rete interattiva o dedicata (**async mode interactive**). Nel caso in cui sia dedicata, l'interfaccia risulta automaticamente configurata per connessioni PPP o SLIP. L'utente non ha la possibilità di accedere ad un livello di EXEC da dove, per esempio, iniziare una connessione in modalità carattere. Con l'istruzione **group-range 33 62** si associano le singole interfacce asincrone dello stesso device ad un singolo gruppo. Questa struttura permette di configurare contemporaneamente tutti i membri del gruppo con un unico comando. La numerazione delle interfacce deriva dalla loro posizione all'interno del device.

---

[1] I protocolli PPP e SLIP definiscono lo standard per la tramissione di pacchetti IP su di una linea seriale standard asincrona EIA-232.

TAB. 3: Parametri relativi alle connessioni su modem del router Cisco

```
Interface Group-Async1
 Description Parent Interface for the Async Interface
 ip unnumbered FastEthernet0/0
 no ip directed-broadcast
 encapsulation ppp
 ip tcp header-compression passive
 dialer in-band
 dialer idle-timeout 300
 dialer-group 1
 async mode interactive
 peer default ip address pool ISDN-nomepool
 no fair-queue
 ppp authentication pap
 ppp use-tacacs
 group-range 33 62
!
line 33 62
 autoselect ppp
 login tacacs
 modem Dialin
 transport input all
 stopbits 1
 flowcontrol hardware
!
```

A ciascuna interfaccia asincrona corrisponde una linea di un terminale fisico. Le configurazioni sono così assegnate globalmente alle **line 33 62**. La configurazione **autoselect ppp** fa in modo che il sistema operativo inizi una sessione PPP sulla linea quando questa viene acceduta. Il controllo della password viene attivato dalla presenza del comando **login**. Con l'opzione **tacacs** il controllo della password non è locale ma demandato ad un server TACACS. Il modem collegato all'interfaccia è un grado di accettare solamente chiamate in ingresso (**modem Dialin**) e tutti i protocolli di connessione sono permessi (**transport input all**). Il numero di bit di stop trasmessi per ogni byte è fissato a 1 (**stopbits 1**). Il controllo del flusso dei dati tra il dispositivo seriale (in questo caso il modem) ed il router può avvenire sia a livello software (Ctrl-S e Ctrl-Q) sia a livello hardware. Nel caso di **flowcontrol hardware** il controllo viene specificato nei manuali forniti con il router.

Fino ad ora non si è ancora trattato dell'indirizzamento IP del router. Nella scrittura del

presente documento si è preferito utilizzare indirizzi IP privati[1] per non coinvolgere indirizzi IP ufficiali, che appartengono ad una organizzazione e sono visibili su Internet. La rete di classe B 172.16.0.0 rappresenta quindi la classe di indirizzi IP utilizzata per gli esempi e non è instradata. Sarà cura di chi implementerà questo servizio procurarsi un range di indirizzi IP ufficiali da utilizzare. Per tenere conto della futura espansione del servizio (utilizzando per esempio un router con due accessi ISDN PRI e due moduli di 30 modem digitali ciascuno) si è scelto di riservare una sottorete con 62 indirizzi (172.16.141.192/26) della rete di classe B per gli indirizzi da assegnare dinamicamente agli host che si collegano al router. Gli indirizzi utilizzati sul router Cisco sono riassunti nella tabella 4. L'interfaccia **FastEthernet0/0** che collega il router alla LAN di istituto ha un indirizzo primario della rete 172.16.119/24 che è quella degli host presenti sulla LAN più un indirizzo secondario dell'altra rete. Il pool di indirizzi da attribuire agli host remoti va da 172.16.141.193 a 172.16.141.223.

TAB. 4: Parametri relativi agli indirizzi IP del router Cisco

```
Interface FastEthernet0/0
 ip address 172.16.141.254 255.255.255.192 secondary
 ip address 172.16.119.220 255.255.255.0
 no ip directed-broadcast
 speed auto
 full-duplex
!
ip local pool ISDN-nomepool 172.16.141.193 172.16.141.223
!
```

2.4 ROUTING

2.4.1 Routing statico

La configurazione più semplice per una realtà non troppo complessa è il routing statico. Su ogni router dell'Autonomous System gli instradamenti sono configurati manualmente. Nella tabella 5 è riportato il comando sul router che instrada tutti i pacchetti verso il gateway di default che ha indirizzo IP 172.16.119.254.

Analogamente sul default gateway sarà necessario definire una route statica per gli indirizzi del router utilizzato per il dial-up.

TAB. 5: Configurazione del routing statico del router Cisco

```
!
ip route 0.0.0.0 0.0.0.0 172.16.119.254
!
```

[1] Secondo il RFC1597 "Address Allocation for Private Networks" gli indirizzi di classe B da 172.16.0.0 a 172.31.255.255 sono riservati per le reti private e non sono instradati.

2.4.2 Routing con OSPF

Nel caso di realtà complesse è necessario l'utilizzo di un protocollo di routing dinamico all'interno dell'Autonomous System. Per esperienza diretta si consiglia l'uso di Open Shortest Path First (OSPF)[4], un protocollo dinamico basato sui Link State che utilizza un algoritmo[1] per calcolare il percorso più breve per far giungere a destinazione i pacchetti. La configurazione di OSPF del router è riportata in tabella 6.

TAB. 6: Configurazione del routing con OSPF del router Cisco

```
!
router ospf 220
 network 172.16.119.0 0.0.0.255 area 6
 network 172.16.141.192 0.0.0.63 area 6
!
```

In questo caso è sufficiente abilitare il processo OSPF (**router ospf 220**) che ha come identificativo il numero 220. Vanno quindi inserite le linee con le informazioni sulle reti di cui il router possiede informazioni che verrano distribuite in broadcast a tutti i router OSPF della stessa area.

3 AUTENTICAZIONE CON XTACACS

Per gestire agevolmente un numero elevato di accessi al router Cisco non è pensabile la creazione di utenti locali sul router stesso. È necessario utilizzare un server di autenticazione esterno. I router Cisco permettono l'autenticazione attraverso vari protocolli[5] quali TACACS, XTACACS, TACACS+, RADIUS e Kerberos. Il protocollo XTACACS (eXtended Terminal Access Controller Access Control System) viene descritto nell'RFC 1492[6]. Cisco consiglia l'uso dei protocolli TACACS+ e RADIUS che essendo più recenti assicurano un accounting maggiormente dettagliato e soddisfano requisiti standard relativamente alla sicurezza dal momento che la comunicazione client-server per la validazione della password è crittata. Nella realizzazione del servizio di accesso dial-up si è scelto XTACACS in quanto, nonostante la sua semplicità di configurazione, consente di controllare gli accessi su più router differenti utilizzando un unico server con più file di password.

Il protocollo XTACACS utilizza la porta UDP 49 per lo scambio di pacchetti IP. Il dialogo client/server è una sequenza di richiesta (client) / risposta (server) in cui la risposta contiene semplicemente due valori: accettato (1) o rifiutato (2).

L'utilizzo del protocollo UDP fa sì che XTACACS si presti poco per un utilizzo su rete geografica. Questo non rappresenta un problema in quanto in genere il server di autenticazione è collocato sulla stessa LAN su cui è presente il router. La cattura delle password che, come detto in precedenza, viaggiano in chiaro tra router e server XTACACS da

[1] L'algoritmo di Dijkstra permette di trovare il tragitto più breve tra due punti. Questo algoritmo si utilizza anche per la costruzione di vie di comunicazione e per le rotte aeree.

parte di eventuali processi di sniffer presenti sulla rete può essere evitata utilizzando uno switch ethernet per connettere tra di loro server di autenticazione e router.

3.1 Installazione del server XTACACS

La prima operazione da compiere per installare il server XTACACS è procurarsi il codice sorgente[1]. Anche se ne esistono versioni precompilate, la possibilità di disporre del codice sorgente consente di configurare alcuni parametri per ottimizzare l'eseguibile. La distribuzione si trova in formato compresso (**.gz**). Dopo aver scompattato il file di archivio con il comando **gunzip xtacacsd-4.1.2.tar.gz** si procede al ripristino dell'intera distribuzione con **tar –xf xtacacsd-4.1.2.tar**. Andando nella directory creata dal processo di ripristino dell'archivio, è necessario editare il **Makefile** per modificarlo secondo le necessità. Nel nostro caso, per esempio, il sistema operativo è Digital UNIX quindi bisogna definire **OS=DECOSF1**.

Quindi si procede alla compilazione vera e propria con il comando **make**.

Se la compilazione è stata eseguita con successo, si procede con la creazione di un albero di directory che contiene tutti i file di interesse del server. Nel nostro caso si è utilizzata la directory **/usr/local/xtacacs**. Nella sottodirectory **/usr/local/xtacacs/bin** vanno copiati gli eseguibili **taclast, taupd, xpasswd e Getpw**. Il server vero e proprio (**xtacaxd**) lo si può copiare nella directory **/usr/sbin** dove stanno tutti gli altri daemon. Il file di configurazione (**xtacacsd-conf**) va copiato nella directory **/etc**.

Il server XTACACS è costituito da un daemon che non è sempre attivo. Esso viene attivato di volta in volta dal server **inetd** come avviene per alcuni servizi principali (telnet, ftp, finger…). Pertanto è necessario introdurre la seguente linea nel file /etc/inetd.conf:

tacacs dgram udp wait root /usr/sbin/xtacacsd xtacacsd –c /etc/xtacacsd-conf

che istruisce il server inetd sul fatto che tacacs sia un servizio che utilizza datagrammi **udp**, ha le priorità di **root**, si trova in **/usr/sbin/xtacacsd** ed il suo file di configurazione sta in /**etc/xtacacsd-conf**. In più va inserita nel file **/etc/services** una linea per il servizio tacacs:

tacacs 49/udp

in cui si specifica quale sia il servizio associato alla porta **49 UDP**.

Il server XTACACS utilizza per i file di log il server syslog presente sullo stesso calcolatore. La facility di default è la local6.debug. Occorre quindi specificare il file di log in **/etc/syslog**.conf con la seguente linea:

local6.debug /var/adm/syslog.dated/xtacacs.log

con i caratteri tab al posto degli spazi, che specifica il file di log su di un calcolatore con sistema operativo Digital UNIX.

Perché le modifiche alla configurazione del server abbiano effetto occorre che sia il server inetd sia quello syslog rileggano i loro file di configurazione. Questo si ottiene inviando un segnale di hangup nel modo seguente:

kill –HUP PID-del-server-inetd

kill –HUP PID-del-server-syslog

---

[1] La versione utilizzata proviene dalla seguente URL: http://www.netplex-tech.com/software/xtacacs/download/xtacaxd-4.1.2.tar.gz.

3.2 Configurazione del server XTACACS

Una volta che il server XTACACS è correttamente installato si può passare alla sua configurazione modificando il file /etc/xtacacsd-conf di cui è ripotato un estratto in tabella 7.

TAB. 7: Esempio di file di configurazione /etc/xtacacsd-conf

```
## xtacacs config file. Use with xtacacsd v2.x
#
WTMP    /var/xtacacs/wtmp
UTMP    /var/xtacacs/utmp
#
PASSWD  /usr/local/xtacacs/passwd/tac-passwd-1
PASSWD  /usr/local/xtacacs/passwd/tac-passwd-2
#
USER    all    HOST    all    all    numlogin      5
#
# - gruppo 50
GROUP   50     HOST cisco1.domain.it     MASK 0.0.0.0    all     permit
GROUP   50     HOST cisco2.domain.it     MASK 0.0.0.0    all     deny
#
# - gruppo 60
GROUP   60     HOST cisco2.domain.it     MASK 0.0.0.0    all     permit
GROUP   60     HOST cisco1.domain.it     MASK 0.0.0.0    all     deny
#
```

In una situazione complessa può accadere di avere più gruppi di utenti divisi in più file di password[1]. Anche i router da gestire possono essere molteplici. Nell'esempio descritto l'utente appartenente al gruppo 50 può collegarsi solamente utilizzando il router cisco1.domain.it mentre chi appartiene al gruppo 60 ha accesso solamente al router cisco2.domain.it. Questa configurazione può sembrare complessa ma riflette l'esigenza sempre più diffusa di limitare i servizi a seconda delle strutture di afferenza degli utenti cercando nel contempo di limitare il numero di server da installare.

Il sever XTACACS, in modo analogo ai calcolatori con sistema operativo UNIX, tiene traccia delle connessioni degli utenti. Nel file di configurazione **WTMP** definisce il file di log dove vengono registrati tutti gli accessi e con **UTMP** si indica il file di log dove sono indicati gli utenti collegati in quel momento. Quest'ultimo file viene controllato prima di concedere l'accesso ad un utente per verificare che non sia stato raggiunto il massimo numero di connessioni permesse. Nel nostro caso la linea **USER all HOST all all numlogin 5** stabilisce che cinque è il massimo numero di collegamenti contemporaneei che un utente può effettuare.

---

[1] La versione 4.1.2 di xtacacsd consente fino a cinque file di password.

I file con le password stanno nella directory **/usr/local/xtacacs/passwd** come indicato dall'istruzione **PASSWD**.

La linea **GROUP 50 HOST cisco1.domain.it MASK 0.0.0.0 all permit** fa sì che gli utenti del gruppo 50 possano collegarsi dall'host cisco1.domain.it mentre è loro impedito l'accesso da cisco2.domain.it (**GROUP 50 HOST cisco2.domain.it MASK 0.0.0.0 all deny**).

3.3 Utilizzo del server XTACACS

A questo punto il server XTACACS è installato e perfettamente funzionante. Il passo successivo consiste nel configurare il router Cisco affinché lo utilizzi. Nella tabella 8 sono riportati i parametri relativi all'utilizzo del server tacacs sul router.

TAB. 8: Configurazione del server XTACACS sul router Cisco

```
!
tacacs-server host xtacacs.server.ip.address
tacacs-server extended
tacacs-server authenticate connections
tacacs-server authenticate slip
!
tacacs-server notify logout
!
```

Il server di autenticazione è definito dal comando **tacacs-server host xtacacs.server.ip.address**. Il server TACACS è di tipo extended (**tacacs-server extended**) e viene interrogato per l'autenticazone quando un utente compie una connessione TCP oppure quando inizia una sessione SLIP/PPP. Il server può anche essere informato quando un utente compie una particolare operazione: con **tacacs-server notify logout**, per esempio, viene trasmesso un messaggio quando un utente si scollega.

4 GESTIONE DEGLI UTENTI

L'ultimo passo nella realizzazione del servizio di accesso dial-up è la creazione degli utenti e la loro gestione.

Gli utenti vengono definiti nei file di password elencati nel file di configurazione **/etc/xtacacsd-conf** (vedi tabella 7). La disposizione dei vari campi all'interno del file di password riflette la versione di UNIX del server ed è diversa da BSD a System V. Nel nostro caso il sistema è Digital UNIX quindi di tipo BSD. Ogni record del file di password si presenta così:

user:passwd:uid:gid:gecos:dir:exp-date

la struttura è quella del file /etc/passwd con al posto della shell di ingresso la data di scadenza (**exp-date**). In questo modo se si vuole che un account abbia scadenza 28 febbraio 2001 il

campo **exp-date** deve essere settato a “Feb 28 2001”. La possibilità di definire una scadenza per gli account risulta particolarmente utile qualora si abbia a che fare con utenti temporanei.

L’utilità di attribuire un gruppo comune a più utenti è stata già descritta. Il campo **gecos** può essere utilizzato per inserire informazioni aggiuntive sull’utente.

La lunghezza della stringa **user** può essere definita maggiore di otto caratteri al momento della compilazione; questo implica una incompatibilità con ogni sistema UNIX-like. Se ne sconsiglia quindi l’uso.

4.1 Aggiunta di utenti nel file di password

Anche se è possibile utilizzare come file di password il file /etc/passwd del calcolatore UNIX su cui è installato il server XTACACS per ottenere una maggiore flessibilità è consigliabile l’uso di un file diverso. Nel nostro caso (vedi tabella 7) i file di password sono nella directory /usr/local/xtacacs/passwd.

La distribuzione del sorgente di xtacacsd contiene tra i tool di supporto (copiati in /usr/local/xtacacs/bin) il programma **xpasswd** che serve appunto per modificare le password.

La soluzione più pratica per la gestione degli utenti e delle password sembra essere la creazione di uno script (shell o perl per esempio) che consenta la manipolazione dei file di password utilizzando il programma xpasswd o direttamente mediante chiamate a funzioni che sono in grado di produrre stringhe crittate (per esempio la funzione crypt di perl).

5 MONITORAGGIO DELL'UTILIZZO

Una volta che il server è attivo il suo corretto funzionamento va controllato periodicamente. Il programma **taclast** (risultato anch’esso della compilazione) è l’analogo del programma last sui sistemi UNIX. Nella tabella 9 è riportato l’output dell’esecuzione del comando taclast sul file di log /var/xtacacs/wtmp.

TAB. 9: uso di taclast sul file wtmp

```
XTACACS-server#  /usr/local/xtacacs/bin/taclast -f /var/xtacacs/wtmp | more
user51    sli36    cisco1   Fri May 19 10:04  online  (00:04) 246
user51    tty36    cisco1   Fri May 19 10:04 - 10:04  (00:00) 0
user62    sli36    cisco2   Fri May 19 09:59  online  (00:09) 592
user62    tty36    cisco2   Fri May 19 09:59 - 09:59  (00:00) 0
user55    sli35    cisco1   Fri May 19 09:43 - 09:56  (00:12) 776
user55    tty35    cisco1   Fri May 19 09:43 - 09:43  (00:00) 0
user68    sli42    cisco2   Fri May 19 09:30  online  (00:38) 2310
user68    tty42    cisco2   Fri May 19 09:30 - 09:30  (00:00) 0
…….
```

Nel momento in cui è stato dato il comando erano presenti 3 utenti collegati: due sul sistema cisco2 ed uno sul sistema cisco1. L’utente user51 ha aperto una connessione sulla linea seriale 36 del server di accesso cisco1 ed è online da 246 secondi (4 minuti). L’utente

user68, che si è collegato alle 09:30, risulta invece online da 2310 secondi. Si può notare come la connessione sulla linea tty, necessaria per attivare il collegamento PPP, sia istantanea e quindi di durata 0 secondi.

Quando si analizza con taclast il file che contiene l'elenco degli utenti collegati in quel momento sul sistema si ottiene il risultato riportato in tabella 10.

TAB. 10: uso di taclast sul file utmp

```
XTACACS-server# /usr/local/xtacacs/bin/taclast -f /var/xtacacs/utmp
user68   sli42   cisco2   Fri May 19 09:30  online  (00:39) 2351
user51   sli36   cisco1   Fri May 19 10:04  online  (00:04) 287
user62   sli36   cisco2   Fri May 19 09:59  online  (00:10) 633
```

I diversi tempi di "online" derivano dal fatto che le due operazioni si sono susseguite dopo qualche decina di secondi.

In tabella 11 è riportato un estratto del file di log. Alle ore 01:48:51 il server XTACACS (con PID = 22554) si chiude dopo 15 minuti di inattività. Alle ore 07:04:07, sollecitato dalla richiesta dell'utente "user53", il server si risveglia. Incomincia quindi a leggere il suo file di configurazione (vedi tabella 7). Il livello di debug è settato a 6. Il massimo numero di login vale 5. Sono presenti configurazioni per il gruppo 50; il file di password è /usr/local/xtacacs/passwd/tac-passwd-1.

L'utente esiste nel file di password e la password corrisponde. Anche il controllo della scadenza dell'account è negativo. A questo punto, poiché anche la configurazione per il gruppo di appartenenza non impedisce il login, si procede con la connessione.

TAB. 11: estratto dal file di log

```
01:48:51 server xtacacsd[22554]: exiting after 15 minutes of inactivity
07:04:07 server xtacacsd[22124]: read_config: debug level set to 6
07:04:07 server xtacacsd[22124]: read_config: user all @ all, REQUEST
                                   all numlogin ARGS = 5
07:04:07 server xtacacsd[22124]: read_config: group 50 @ cisco1, REQUEST
                                   all permit ARGS=
07:04:07 server xtacacsd[22124]: read_config: group 50 @ cisco2, REQUEST
                                   all deny ARGS=
07:04:07 server xtacacsd[22124]: read_config: password file
                                  </usr/local/xtacacs/passwd/tac-passwd-1>
07:04:07 server xtacacsd[22124]: (1) main: request from cisco1 [172.16.119.210]
07:04:07 server xtacacsd[22124]: new_process: Querytype 1 for 'user53'
07:04:07 server xtacacsd[22124]: authent_files: checking user="user53"
07:04:07 server xtacacsd[22124]: search_pwname: Match for user53 found in
                                   /usr/local/xtacacs/passwd/tac-passwd-1
07:04:07 server xtacacsd[22124]: authent_files: Password matched (dAslWhUJgzLGA)
07:04:07 server xtacacsd[22124]:  Checking expiration from pw age field
07:04:07 server xtacacsd[22124]: check_key: User 'user53', matched permission
                                   line 'group 50' req 'all', doing action permit
```

L’osservazione nel dettaglio del file di log consente in taluni casi di individuare le cause di un mancato collegamento. Risulta quindi necessario conservare un file di log con quante più informazioni possibili. Il livello di debug 6 fornisce informazioni sufficienti per la diagnostica e la soluzione dei problemi di connessione.

6 CONSIDERAZIONI GENERALI

L’utilizzo del server di autenticazione XTACACS insieme con un router Cisco dotato di accesso primario ISDN e modem digitali integrati è risultato particolarmente robusto e flessibile nello stesso tempo.

La possibilità di utilizzare la stessa linea nelle due modalità (analogica/ISDN) consente di accontentare tutte le tipologie di utenti: da quello che possiede l’accesso ISDN a quello con un modem magari acquistato da tempo.

Il router Cisco è un oggetto stabile che non necessita di particolari manutenzioni se non per l’aggiornamento del sistema operativo.

Il server XTACACS anche se non offre caratteristiche di sicurezza elevate per quanto riguarda la trasmissione delle password consente un buon livello di configurabilità.
Il sistema descritto offre prestazioni di ottimo livello per quanto riguarda la velocità trasmissiva (fino a 56Kbps su linea analogica oppure 64Kbps su ISDN). La gestione degli utenti non risulta particolarmente laborisa se si utilizzano perl script per la creazione degli account. La linea telefonica ISDN è molto stabile e gestisce le chiamate in modo migliore di alcuni centralini analogici. Controllando periodicamente i file di log, sia quelli del server XTACACS sia quelli del syslog server indicato nel router Cisco, ci si può accorgere del comportamento anomalo del sistema e prendere provvedimenti adeguati.

7 REFERENCES

[1] Cisco IOS Dial Solutions, Cisco Press, ISBN: 1-57870-055-8, 121 (1998).
[2] V. Jacobson, Compressing TCP/IP Headers for Low-Speed Serial Links, Request for Comment: 1144, NWG/LBL, February 1990.
[3] B. Lioyd & W. Simpson, PPP Authentication Protocol, Request for Comments: 1334, NWG/Daydreamer, October 1992.
[4] J. Moy, OSPF Specification Version 1, Request for Comments: 1131, October 1989
[5] Security Configuration Guide - Cisco IOS Release 12.0 - Cisco documentation CD-ROM (November 1999).
[6] C. Finseth, An Access Control Protocol, Sometimes Called TACACS, Request for Comments: 1492, NWG/University of Minnesota, July 1993.