

CONFIGURARE UN CISCO 837 PER IL COLLEGAMENTO AD INTERNET



AUTORE: MASSIMO RABBI
DATA: 29/08/2006



Note introduttive

In questa guida vedremo come configurare un router Cisco modello 837 per il collegamento ad Internet, nella fattispecie Alice Adsl 4mbit.

Per il collegamento fisico tra router e pc utilizziamo il cavo console (colore blu).

Ho riportato anche i prompt del router in modo che possiate di volta in volta capire se ci troviamo in modalità configurazione globale o in una sotto-modalità ad esempio di configurazione delle varie interfacce.

Per uscire da una modalità di configurazione è sufficiente digitare `exit` per passare a quella immediatamente più generica.

Partenza!

Accediamo alla modalità privilegiata:

```
Router>en
```

Accediamo alla modalità di configurazione globale:

```
Router#conf t
```

Assegnamo l'hostname al router:

```
Router(config)#hostname max837
```

Disabilito i servizi inutili

Disabilito il protocollo CDP (Cisco Discovery Protocol) che è tipicamente abilitato di default, per farlo ho due possibilità:

- disabilitarlo in maniera globale dalla *global configuration mode*: `no cdp run`
- disabilitarlo per singola interfaccia: `no cdp enable`

Nel nostro caso lo facciamo in maniera globale:

```
max837(config)#no cdp run
```

Il comando `boot network` consente di specificare il file di rete (protocolli tftp, mop o rcp) da cui recuperare i comandi di configurazione. Non è necessario quindi:

```
max837(config)#no boot network
```

Disabilitare la ricerca di un file di configurazione da un server di rete (es: un tftp server);

```
max837(config)#no service config
```

Disabilitiamo il source routing. Con il source routing infatti una sorgente può specificare il percorso (tutto o parte) che un pacchetto deve compiere attraverso la rete. Non dovrebbe essere necessario a meno che la rete non lo richieda. Possibile fonte di attacchi. Di norma è disabilitato sui router, per sicurezza diamo il seguente comando:

```
max837(config)#no ip source-route
```

Disabilitiamo il servizio di finger. Il comando `finger` (specifiche RFC 742) consente di vedere informazioni sugli utenti loggati sul device di rete.

NOTA: il comando `no service finger` è stato sostituito dal comando `no ip finger`. Per compatibilità è molto probabile siano presenti entrambi.

Diamo il seguente comando:

```
max837(config)#no ip finger
```

Disabilitare il servizio di identificazione IP. Questo per impedire ad un sistema connesso sulla rete di rilevare che il router è un dispositivo Cisco e determinarne modello e versione software.

NOTA: nel mio 837 IOS 12.3 non è presente il comando. Verificare che sul vostro dispositivo sia presente.

Il comando è:

```
max837(config)#no ip identd
```

Disabilitare il packet assembler/disassembler, utilizzato per connessioni X.25.

Il comando da dare è:

```
max837(config)#no service pad
```

Disabilitare i tcp e udp small servers. Si tratta di una sorta di daemons che possono essere fatti girare sul router ed essere utilizzati specie per scopi di diagnostica.

A partire dalla versione 11.3 dell'IOS sono disabilitati di default.

In ogni caso i comandi sono:

```
max837(config)#no service tcp-small-servers
```

```
max837(config)#no service udp-small-servers
```

Disabilitiamo il bootp. Nella maggior parte dei casi non dovrebbe essere necessario quindi:

```
max837(config)#no ip bootp server
```

Disabilitiamo anche il servizio snmp. Ricordiamo che il protocollo snmp fornisce funzionalità per recuperare e inoltrare dati sulle prestazioni e sui processi della rete. Può essere usato per il monitoraggio dei router, ma anche per la modifica della loro configurazione.

Per il momento non è necessario quindi diamo il seguente comando:

```
max837(config)#no snmp-server
```

Disabilitiamo il servizio tftp in maniera che il router non si comporti da tftp server:

```
max837(config)#no tftp-server
```

Infine disabilitiamo anche il servizio http in modo che il router non si comporti da server http:

```
max837(config)#no ip http server
```

Password e protezione

Attiviamo il servizio per la protezione della password, che altrimenti sarebbero visibili in chiaro nei file di configurazione:

```
max837(config)#service password-encryption
```

Utilizziamo `enable secret` piuttosto che `enable password` per dare una password di enable. Mentre `enable password` usa lo schema di protezione Type-7 che prevede un algoritmo di crittazione Cisco-defined (facilmente decifrabile), `enable secret` usa lo schema di protezione Type-5 che prevede un salvataggio delle password molto più forte mediante MD5:

```
max837(config)#enable secret <miapasswordsegreta>
```

Risoluzione dei nomi

Capita spesso che si digiti qualche comando errato, ecco allora partire il classico messaggio:

```
Translating "prova"...domain server (255.255.255.255)
```

```
% Unknown command or computer name, or unable to find computer address
```

Quello che avviene in questo caso è che il router interpreta erroneamente il comando `prova` come il tentativo di effettuare una connessione telnet verso l'host di nome `prova`. Ovvero digitare `prova` per il router in questo caso equivale a scrivere `telnet prova`: gli errori che si ottengono sono speculari.

In questo caso il router non riesce a trovare una corrispondenza per l'ipotetico hostname `prova` né in memoria (i mapping di questo tipo possono essere creati con il comando `ip host <hostname> <address>`) né attraverso una risoluzione dei nomi.

Per disabilitare questa scocciatura possiamo usare il comando:

```
max837(config)#no ip domain lookup
```

Quello che succede è che viene disabilitato l'accesso al server dns e per questo il router non tenta di convertire comandi mal digitati in indirizzi ip.

Quello che otterremo nel caso digitassimo nuovamente `prova` è quanto segue:

```
Translating "prova"
```

```
% Unknown command or computer name, or unable to find computer address
```

In particolare non si perdono secondi nell'attesa di un'inutile risoluzione dns.

Il consiglio è tuttavia di impostare dei server dns e di prestare più attenzione a quanto viene digitato in console!

Nella fattispecie aggiungiamo i server dns ns1.tin.it e ns2.tin.it:

```
max837(config)#ip name-server 212.216.172.62
```

```
max837(config)#ip name-server 212.216.172.162
```

Configurazione delle interfacce

Passaggio successivo è configurare le interfacce di cui dispone il router.

Partiamo in questo caso prima di tutto dall'Ethernet0 che permette tra l'altro di gestire il traffico da e verso la nostra lan.

Il primo comando da dare è:

```
max837(config)#interface Ethernet0
```

e consente di entrare nella modalità di configurazione dell'interfaccia specificata.

Diamo una descrizione alla nostra interfaccia:

```
max837(config-if)#description HOME LAN
```

Settiamo un indirizzo ip e una subnet mask valide:

```
max837(config-if)#ip address 192.168.1.2 255.255.255.0
```

Indichiamo ora che i client che stanno sulla nostra lan 192.168.1.0 useranno il nat per uscire sulla WAN:

```
max837(config-if)#ip nat inside
```

Impostiamo la coda di output dell'interfaccia:

```
max837(config-if)#hold-queue 100 out
```

Nel nostro caso andiamo a configurare una ADSL casalinga (no ip statico) di Telecom, la Alice 4mbit per intenderci, sfruttando il protocollo PPPoA.

Quello che dovremo fare sarà quindi andare a configurare le interfacce Atm0 e Dialer0.

Vediamo come, prima di tutto entrando in modalità configurazione della Dialer0:

```
max837(config)#interface dialer0
```

Al solito una descrizione:

```
max837(config-if)#description CONNESSIONE ADSL ALICE 4MBIT
```

Poiché come abbiamo detto l'ip ce lo fornirà direttamente Telecom, utilizziamo l'apposito comando per specificare il caso di ip dinamico:

```
max837(config-if)#ip address negotiated
```

Impostiamo il tipo di encapsulation PPP:

```
max837(config-if)#encapsulation ppp
```

Affinchè l'interfaccia possa essere messa in contatto con la WAN che fa parte delle rete pubblica del provider:

```
max837(config-if)#ip nat outside
```

Specifichiamo un solo dialer pool, quello della nostra connessione appunto:

```
max837(config-if)#dialer pool 1
```

Impostiamo ora username e password di accesso: nel caso di Alice è possibile specificare alice:alice, altrimenti specificate quelli comunicati dal vostro ISP.

Come protocollo di autenticazione selezioniamo chap.

```
max837(config-if)#ppp chap hostname alice
```

```
max837(config-if)#ppp chap password alice
```

Definiamo anche il caso di tipologia di autenticazione pap.

```
max837(config-if)#ppp pap sent-username alice password alice
```

Configuriamo ora l'interfaccia fisica atm0, entrando per prima cosa in modalità configurazione:

```
max837(config)#interface atm0
```

Descrizione per l'interfaccia:

```
max837(config-if)#description ADSL INTERFACCIA ATM
```

Configuriamo correttamente il circuito PVC (Permanent Virtual Connection) utilizzando la coppia VPI/VCI che serve per indirizzare il flusso ATM, andrà bene 8/35 che è quella utilizzata da quasi tutti i provider italiani:

```
max837(config-if)#pvc 8/35
```

Configuriamo ora il tipo di encapsulation per i pacchetti dati che viaggiano con protocollo PPP, ricordiamo infatti che stiamo utilizzando PPP over ATM:

```
max837(config-if-atm-vc)#encapsulation aal5mux ppp dialer
```

Associamo ora all'interfaccia fisica il profilo dialer corretto, quello che avevamo definito sopra in fase di configurazione della Dialer0:

```
max837(config-if-atm-vc)#dialer pool-member 1
```

Altri settaggi

Abilitiamo il NAT per i client della nostra rete.

Creiamo innanzitutto una access-list che mi permetta di effettuare su di essi la traslazione:

```
max837(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

Infine configuriamo il NAT vero e proprio andando ad agganciare l'access-list prima creata:

```
max837(config)#ip nat inside source list 1 interface dialer0 overload
```

Impostiamo l'interfaccia dialer0 come default gateway:

```
max837(config)#ip route 0.0.0.0 0.0.0.0 dialer0
```

Nel caso volessimo pubblicare su internet un server web, un server ftp o anche semplicemente aprire le porte in maniera da ottenere id alto con emule possiamo farlo nel seguente modo:

```
ip nat inside source static <protocollo> <ip_macchina_lan>  
<porta_macchina_interna> interface Dialer0 <porta_esterna_pubblicata>
```

In un caso reale, ad esempio volendo dare la possibilità di raggiungere un host interno mediante desktop remoto, diamo il seguente comando:

```
max837(config)#ip nat inside source static tcp 192.168.1.79 3389 interface  
Dialer0 3389
```

Abilitiamo ora la possibilità di configurare il router via telnet.

Prima di tutto è bene sapere che i collegamenti via telnet vengono indicati con VTY.

Per vedere tutte le vie di accesso (Tty) al router digitiamo:

```
max837#show line
```

Ecco l'output sul mio 837:

```
myrouter#show line
  Tty Typ Tx/Rx A Modem Roty Acc0 AccI Uses Noise Overruns Int
*  0 CTY  -  -  -  -  -  -  0  0  0/0  -
  1 AUX  0/0  -  -  -  -  -  0  0  0/0  -
  2 VTY  -  -  -  -  -  -  2  0  0/0  -
  3 VTY  -  -  -  -  -  -  0  0  0/0  -
  4 VTY  -  -  -  -  -  -  0  0  0/0  -
  5 VTY  -  -  -  -  -  -  0  0  0/0  -
  6 VTY  -  -  -  -  -  -  0  0  0/0  -
```

In questo caso l'asterisco vicino a CTY indica che c'è un collegamento attraverso la porta console. Come si può notare ci sono 5 possibili slot VTY e infatti tipicamente in configurazione vengono riferiti come `line vty 0 4`.

Vediamo quindi di configurare l'accesso via telnet proteggendolo con password:

```
max837(config)#line vty 0 4
```

```
max837(config-line)#password <miapasswordsegreta>
```

```
max837(config-line)#login
```

Se invece vogliamo creare una autenticazione che sfrutti la combinazione username/password procediamo come segue.

Prima di tutto creiamo gli appositi utenti dalla modalità di configurazione globale:

```
max837(config)#username <username1> password <password1>
```

```
max837(config)#username <username2> password <password2>
```

Ora configuriamo l'autenticazione dal "database locale":

```
max837(config)#line vty 0 4
```

```
max837(config-line)#login local
```

Il consiglio è quello di agganciare al login da telnet anche una access-list che specifichi quali ip possono fare login da remoto.

Scegliamo per esempio di consentire il login solo agli ip su rete 192.168.1.0/24:

```
max837(config)#access-list 2 permit 192.168.1.0 0.0.0.255 log
```

```
max837(config)#access-list 2 deny any log
```

Dalla modalità di configurazione line vty, digitare:

```
max837(config-line)#access-class 2 in
```

In maniera simile a quanto già fatto per il telnet qui sopra è possibile proteggere anche la porta console: al posto di `line vty 0 4`, usate `line con 0`.

Conclusioni

Questo documento è stato realizzato prima di tutto per scopo personale, visto che ho dovuto affrontare la configurazione del Cisco 837 proprio in questi giorni.

Queste pagine sono un collage di tante informazioni trovate su internet, in particolare dal sito Cisco e da configurazioni preesistenti, rielaborate con alcune osservazioni personali.

Quello che consiglio di fare è di leggere la guida di Giuseppe Paternò che tratta del tuning e dell'hardening dei router cisco. Troverete sicuramente altre interessanti informazioni.

Per qualsiasi tipo di informazione, suggerimento, segnalazione di errori e imprecisioni, feedback e quant'altro potete contattarmi usando i riferimenti presenti su uno dei seguenti siti:

- <http://www.brainweb.it>
- <http://www.techtown.it>
- <http://www.secornetwork.net>

Riferimenti e Sitografia.

Documentazione e tutorials di vario tipo:

<http://www.cisco.com>

http://gpaterno.free.fr/publications/Sicurezza_router_cisco.pdf

MIRROR:

<http://www.techtown.it/home/detail.asp?iData=2006&iCat=364&iChannel=2&nChannel=Articoli>

<http://netgroup.polito.it/NetLibrary/cisco/ConfigBase/>

Esempi di configurazioni:

http://www.ngi.it/f5/guide/cisco_837.asp

<http://www.altohiway.com/cgi-bin/knowledge/86.html>

http://www.ilpuntotecnicoeadsl.com/index.php/azione_cisco827.html

<http://www.assint.org/content/view/19/44/>