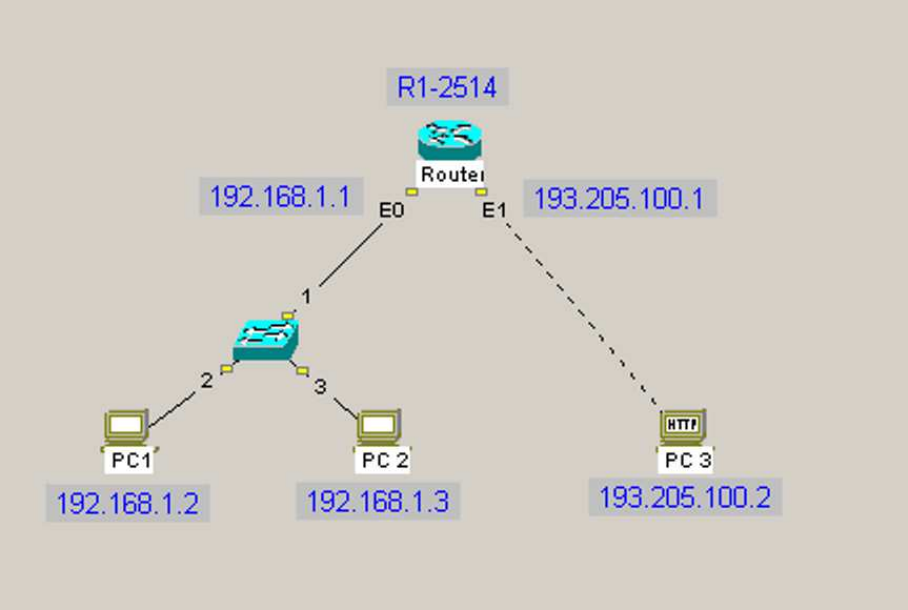
ESERCIZIO N. 1 – ACL BASE



Obiettivo:

Come primo obiettivo, tramite delle ACL sul Router , consentiamo ai soli pacchetti provenienti dal PC 1 l' uscita verso la rete 193.205.100.0/24.

Come secondo obiettivo, vogliamo, in un secondo tempo, consentire, stante l'ACL precedente, l'accesso al server WEB sulla macchina PC 3, da tutti gli host.
Si noti che lasciando solo la prima ACL tutti i pacchetti che non provengono dal PC 1 vengono filtrati in quanto di default il router blocca i pacchetti che non soddisfano alcuna regola di tipo permit. Aggiungendo quindi una seconda regola di permit, i pacchetti che la soddisfano, anche se esclusi dalla prima ACL, possono passare.

Le ACL

Le Access Control List (o, per brevità, ACL) sono liste di istruzioni che controllano ogni singolo pacchetto di ogni flusso di dati per diverse ragioni, molto importante ne è quindi l'ordine in cui sono inserite.

Quando un pacchetto passa per una ACL, la lista viene scorsa istruzione per istruzione (riga per riga), dall'alto al basso, in cerca di una regola che combaci con il pacchetto interessato.

Quando il match è positivo, viene effettuata l'azione relativa alla regola e lo scorrimento della lista termina.

Le ACL possono assumere due ruoli all'interno di una configurazione:

- **1. Identificare una categoria di dati secondo parametri precisi, all'interno di un istruzione.**
- **2. Identificare e filtrare il traffico indesiderato, quando applicate ad un'interfaccia.**

Ogni ACL è marcata da un numero che è comune a tutta la lista di istruzioni. Il numero è arbitrario

ACL Standard

Le ACL standard vengono identificate da un numero tra 1 e 99. Comprendono una parte descrittiva e una decisionale. Vengono normalmente impiegate per un filtering Basilare.

La sintassi è: *access-list [1-99] [decisione] [ip sorgente]*

ACL Estese

Le ACL estese sono la seconda generazione e sono identificate dai numeri da 100 a 199. I blocchi della sintassi sono i medesimi, ma le possibilità sono molto più potenti. E' possibile descrivere regole modo molto più dettagliate.

La sintassi è: access-list [100-199] [decisione] [protocollo] [indirizzo sorgente] [porta sorgente] [indirizzo destinazione] [porta destinazione] [tipo messaggio]

In ambedue i casi le decisioni ammesse sono permit o deny.

Esistono altri range per altri tipi di ACL che però non tratteremo qui, chi è interessato può cercare sulla documentazione Cisco.

SOLUZIONE:

CONFIGURIAMO IL ROUTER R1:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

Configuriamo l'interfaccia Ethernet 0

```
Router(config)#interface Ethernet 0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
```

Configuriamo l'interfaccia Ethernet 1

```
Router(config-if)#interface Ethernet 1
Router(config-if)#ip address 193.205.100.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

Impostiamo l'ACL

```
Router(config)#access-list 101 permit ip host 192.168.1.2 any
```

Applichiamo l'ACL all'interfaccia Ethernet 1

```
Router(config-if)#interface Ethernet 1
Router(config-if)#ip access-group 101 out
Router(config-if)#exit
```

In questo modo i pacchetti in uscita sull'interfaccia Ethernet 1 verranno analizzati secondo l'ACL 101.

Configuriamo ora gli indirizzi ip dei PC e del Server http

Proviamo a pingare il server http dal PC 1

```
C:>ping 193.205.100.2

Pinging 193.205.100.2 with 32 bytes of data:

Reply from 193.205.100.2 on Eth, time<10ms TTL=127
Reply from 193.205.100.2 on Eth, time<10ms TTL=127
Reply from 193.205.100.2 on Eth, time<10ms TTL=127
Reply from 193.205.100.2 on Eth, time<10ms TTL=127
```

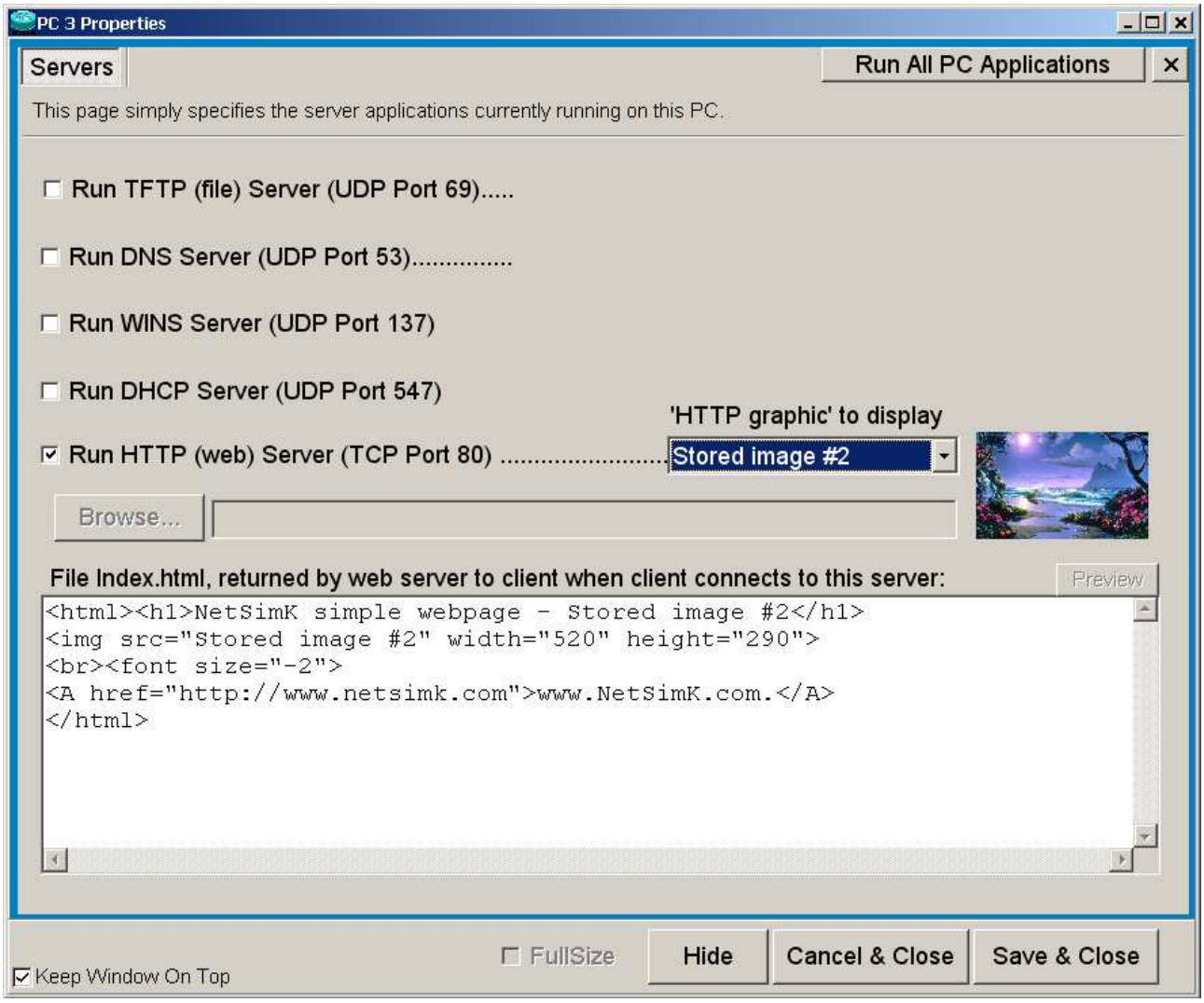
Proviamo a pingare il server http dal PC 2

```
C:>ping 193.205.100.2

Pinging 193.205.100.2 with 32 bytes of data:

Ping request timed out.
Ping request timed out.
Ping request timed out.
Ping request timed out.
```

Come su può vedere tutti pacchetti non provenienti dal PC 1 vengono filtrati.

Ora vogliamo accedere al server tramite un browser dal PC 1

Impostiamo l'http server sul PC3:
apriamo il PC 3 e lanciamo server application

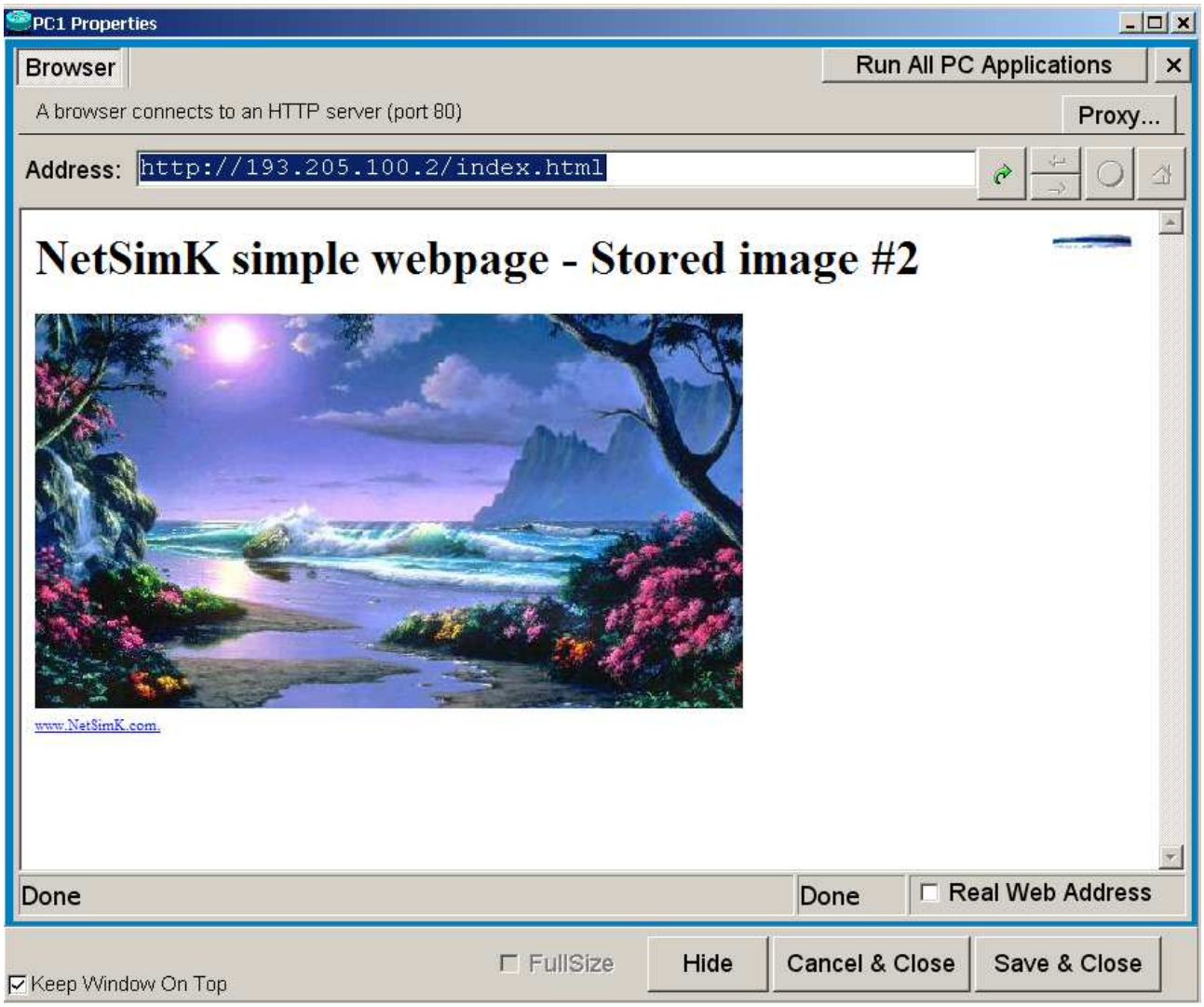


Controlliamo che sia abilitato l'http server e scegliamo "Stored image #2" in http graphic to display

Andiamo sul PC1 e lanciamo Internet Explorer

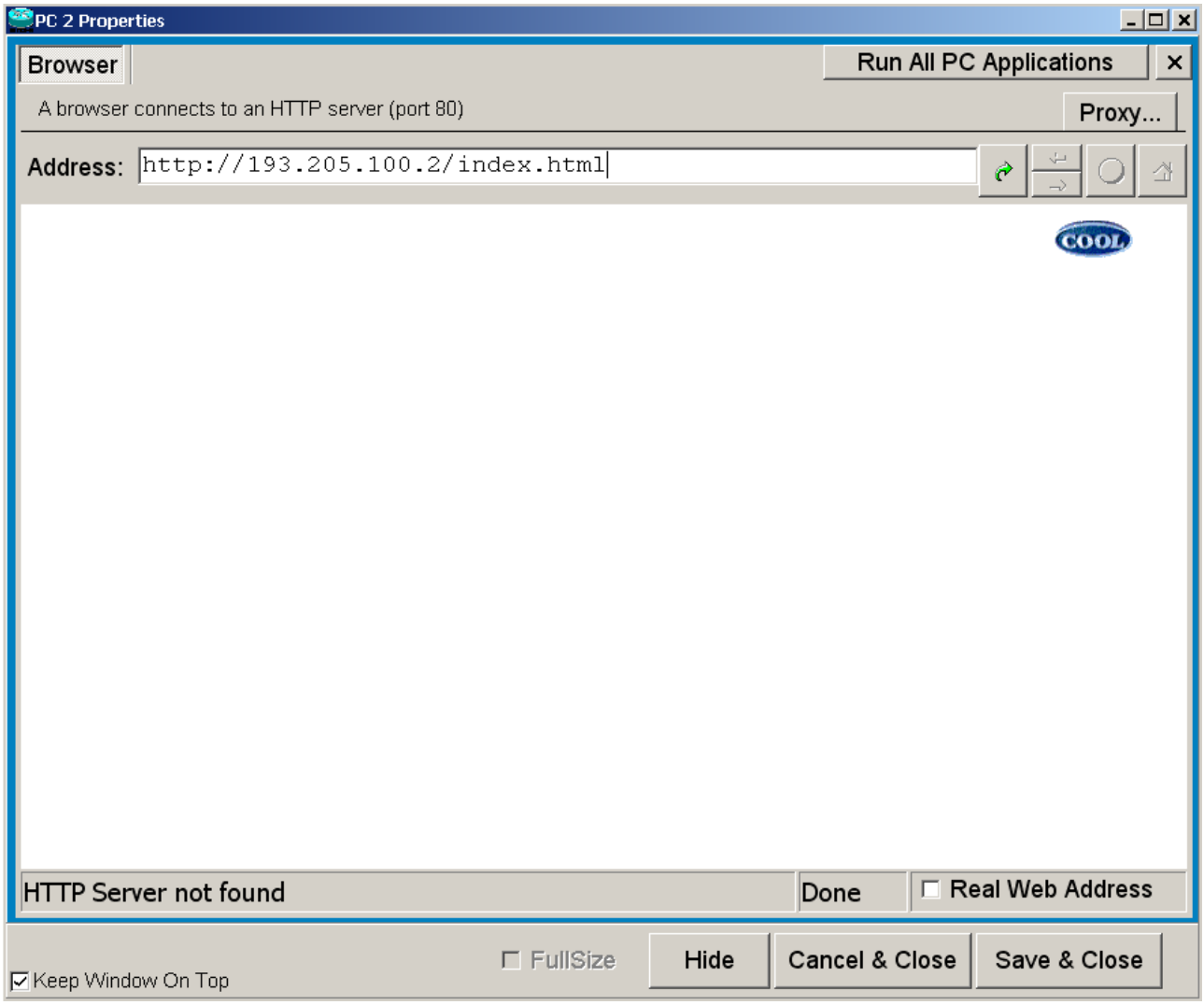
Disabilitiamo il proxy, cliccando sul tasto proxy e togliendo il segno di spunta alla voce Use a Proxy Server.

Digitiamo nella barra degli indirizzi il seguente indirizzo: **http://193.205.100.2/**



Vediamo che riusciamo tranquillamente ad accedere al web server.

Proviamo ora la stessa cosa dal PC2



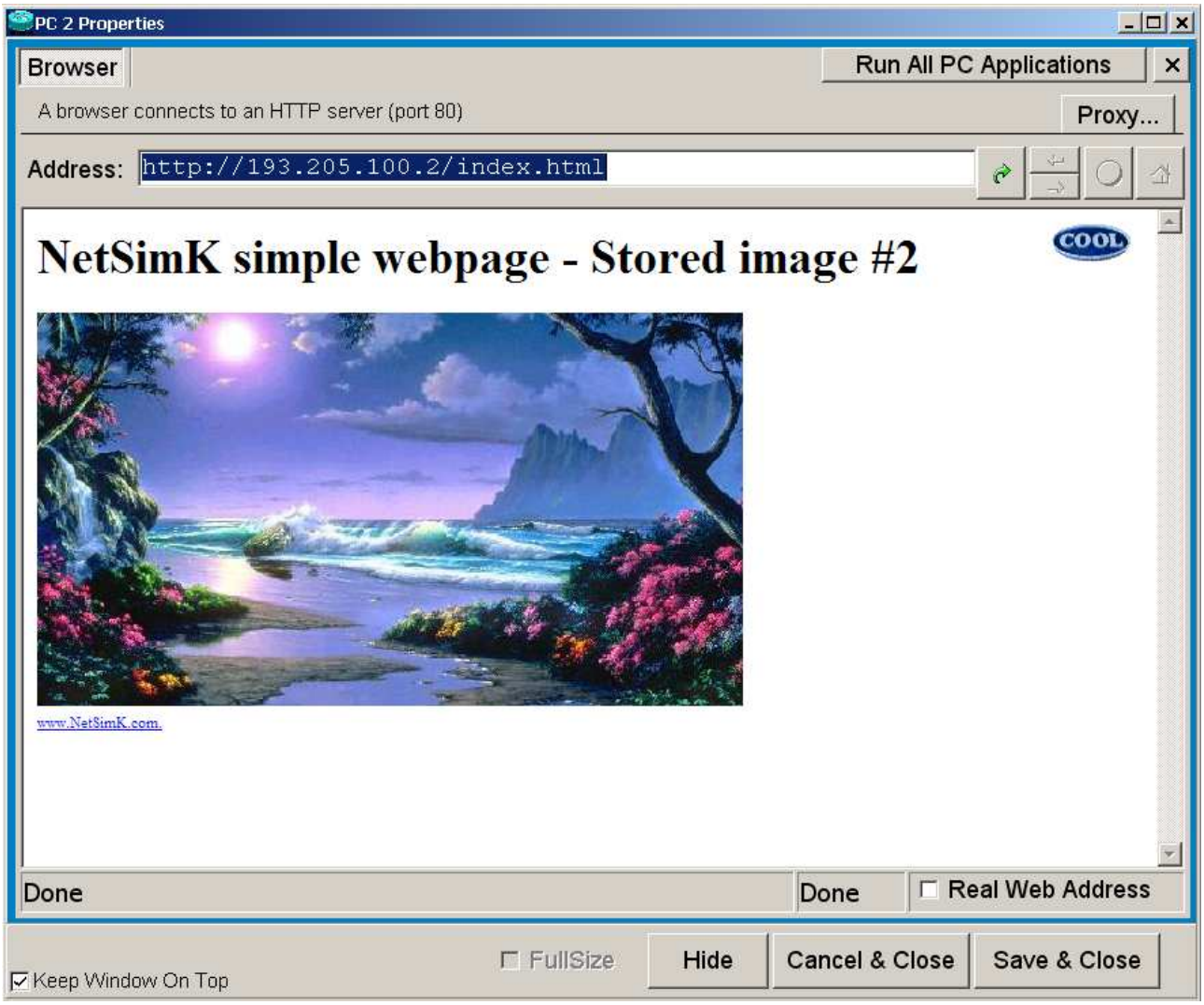
E vediamo che non riusciamo ad accedere a causa dell'ACL impostata prima.

Impostiamo ora un ACL che permetta al traffico http da qualsiasi host di passare

Andiamo su R1 e impostiamo la seguente ACL

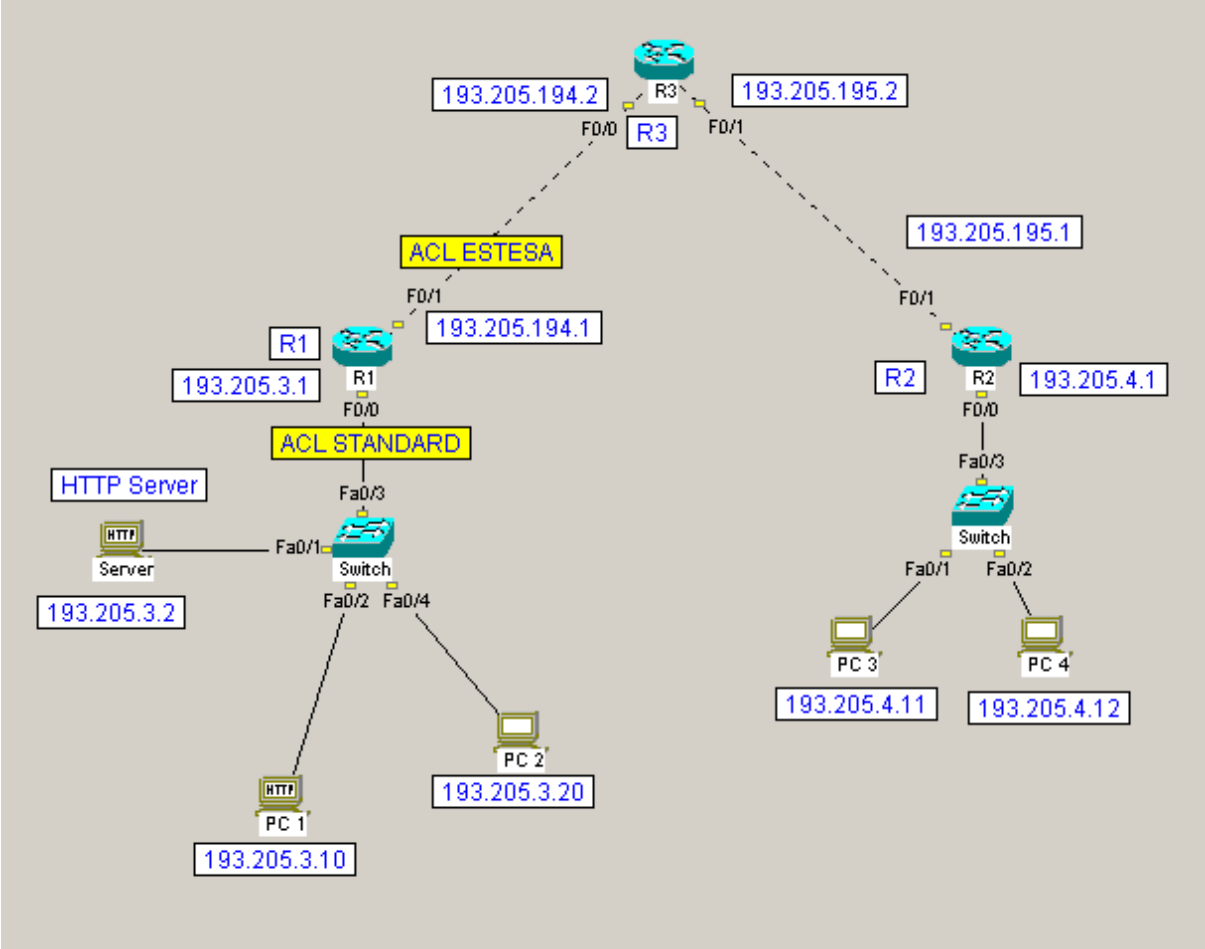
```
Router(config)#access-list 101 permit tcp any host 193.205.100.2 eq www
```

Ora riproviamo dal PC2



E vediamo che la pagina si carica correttamente

ESERCIZIO N. 2 – ACL STANDARD E ESTESE



Utilizzare come router il Cisco 2620 e come switch un 2950 24+2 Switch.
Ricordarsi di usare cavi incrociati nei link fra i router

Obiettivo:

Si vuole negare al PC4 qualsiasi accesso alla rete 193.205.3.0 e allo stesso tempo negare al PC3 l'accesso via http all' host PC1 dove è presente un server Web

SOLUZIONE

R1:

Colleghiamo un pc a R1 con un cavo console e apriamo Hyperterm

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

Impostiamo il nome del Router

```
Router(config)#hostname R1
```

Configuriamo l'interfaccia Fastethernet 0/0

```
R1-2620(config)#interface F0/0
R1-2620(config-if)#ip address 193.205.3.1 255.255.255.0
R1-2620(config-if)#no shutdown
%LDXX - Line protocol on Interface FastEthernet0/0, changed state to up
R1-2620(config-if)#exit
R1-2620(config)#exit
```

Configuriamo l'interfaccia Fastethernet 0/1

```
R1-2620(config)#interface F0/1
R1-2620(config-if)#ip address 193.205.194.1 255.255.255.0
R1-2620(config-if)#no shutdown
R1-2620(config-if)#exit
R1-2620(config)#exit
```

Impostiamo il RIP

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1-2620(config)#router rip
R1-2620(config-router)#network 193.205.3.0
R1-2620(config-router)#network 193.205.194.0
R1-2620(config-router)#exit
```

R3:

Colleghiamo un pc a R3 con un cavo console e apriamo Hyperterm

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

Impostiamo il nome del Router

```
Router(config)#hostname R3
```

Configuriamo l'interfaccia Fastethernet 0/0

```
R3(config)#interface F0/0
R3(config-if)#ip address 193.205.194.2
                                       ^ Error or incomplete command
R3(config-if)#ip address 193.205.194.2 255.255.255.0
R3(config-if)#no shutdown
%LDXX - Line protocol on Interface FastEthernet0/0, changed state to up
R3(config-if)#nexit
```

Configuriamo l'interfaccia Fastethernet 0/1

```
R3(config)#interface F0/1
R3(config-if)#ip address 193.205.195.2 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
```

Impostiamo il RIP

```
R3(config)#router rip
R3(config-router)#network 193.205.194.0
R3(config-router)#network 193.205.195.0
R3(config-router)#exit
```

R2:

Colleghiamo un pc a R2 con un cavo console e apriamo Hyperterm

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

Impostiamo il nome del Router

```
Router(config)#hostname R2
```

Configuriamo l'interfaccia Fastethernet 0/0

```
R2(config)#interface F0/0
R2(config-if)#ip address 193.205.4.1 255.255.255.0
R2(config-if)#no shutdown
%LDXX - Line protocol on Interface FastEthernet0/0, changed state to up
R2(config-if)#exit
R2(config)#exit
```

Configuriamo l'interfaccia Fastethernet 0/1

```
R2(config)#interface f0/1
R2(config-if)#ip address 193.205.195.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#
%LDXX - Line protocol on Interface FastEthernet0/1, changed state to up
R2(config-if)#exit
```

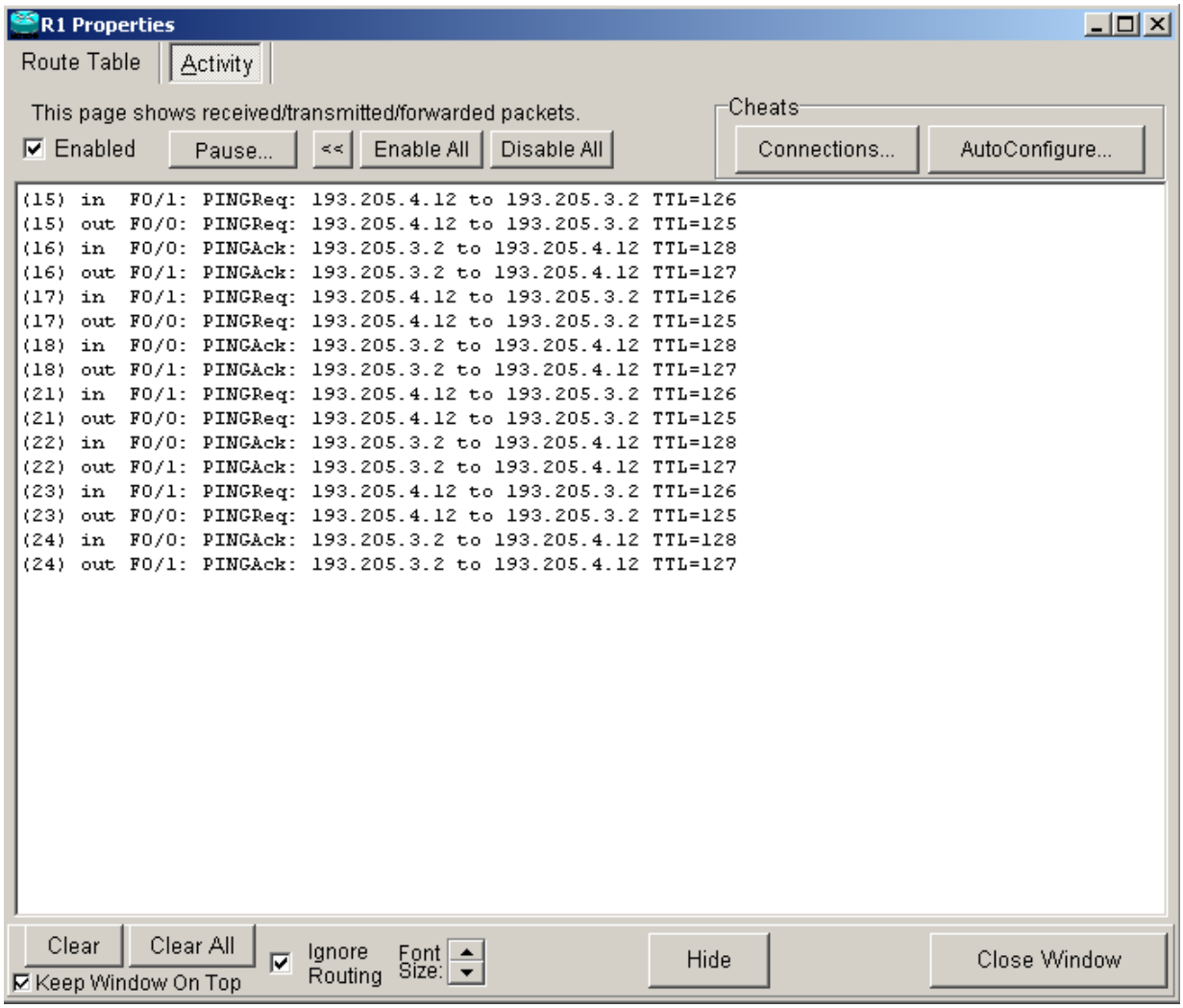
Impostiamo il RIP

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router rip
R2(config-router)#network 193.205.4.0
R2(config-router)#network 193.205.195.0
R2(config-router)#exit
```

IMPOSTIAMO ORA LE ACL RICHIESTE

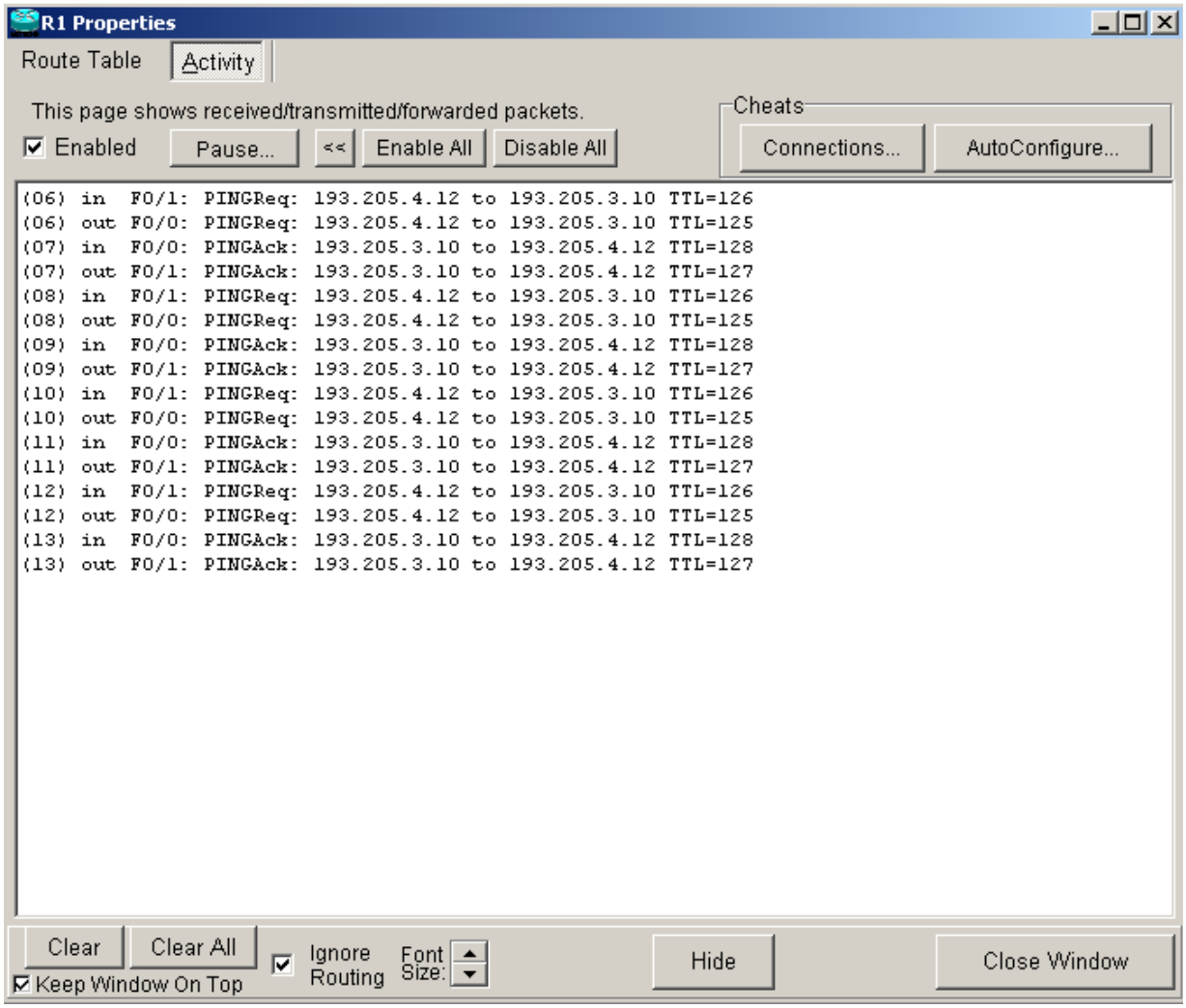
Aprimamo la finestra delle prorietà di R1 e attiviamo la visualizzazione delle Activity, poi pinghiamo dal PC 4 il server HTTP

```
C:>ping 193.205.3.2

Pinging 193.205.3.2 with 32 bytes of data:

Reply from 193.205.3.2 on Eth, time<10ms TTL=125
Reply from 193.205.3.2 on Eth, time<10ms TTL=125
Reply from 193.205.3.2 on Eth, time<10ms TTL=125
Reply from 193.205.3.2 on Eth, time<10ms TTL=125
```



Puliamo la finestra delle Activity e pinghiamo il PC 1

```
C:>ping 193.205.3.10

Pinging 193.205.3.10 with 32 bytes of data:

Reply from 193.205.3.10 on Eth, time<10ms TTL=125
Reply from 193.205.3.10 on Eth, time<10ms TTL=125
Reply from 193.205.3.10 on Eth, time<10ms TTL=125
Reply from 193.205.3.10 on Eth, time<10ms TTL=125
```

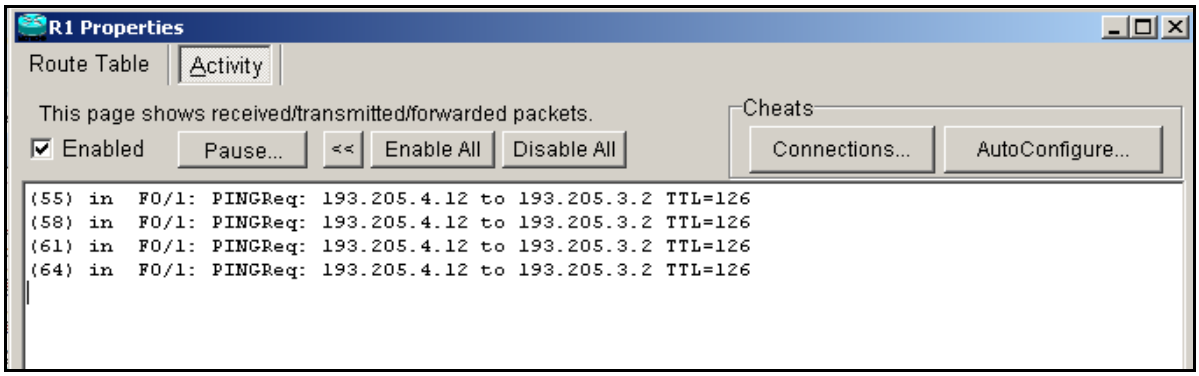


Impostiamo le ACL di tipo standard (1-99) su R1 in modo da negare al PC4 (193.205.4.12) qualsiasi accesso alla rete 193.205.3.0

```
R1-2620(config)#access-list 1 deny host 193.205.4.12
R1-2620(config)#access-list 1 permit any
R1-2620(config)#interface F0/0
R1-2620(config-if)#ip access-group 1 out
```

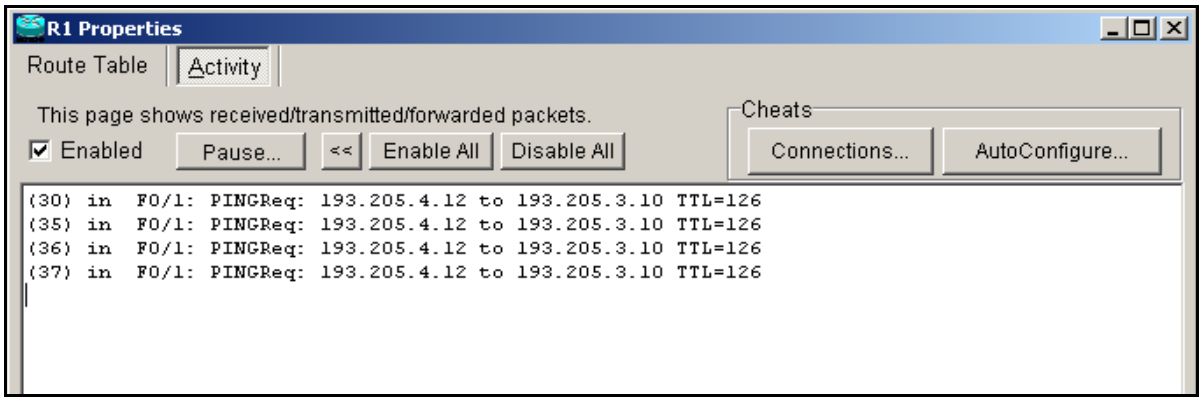
Pinghiamo nuovamente dal PC 4 il server HTTP

```
C:>ping 193.205.3.2

Pinging 193.205.3.2 with 32 bytes of data:

Ping request timed out.
Ping request timed out.
Ping request timed out.
Ping request timed out.
```



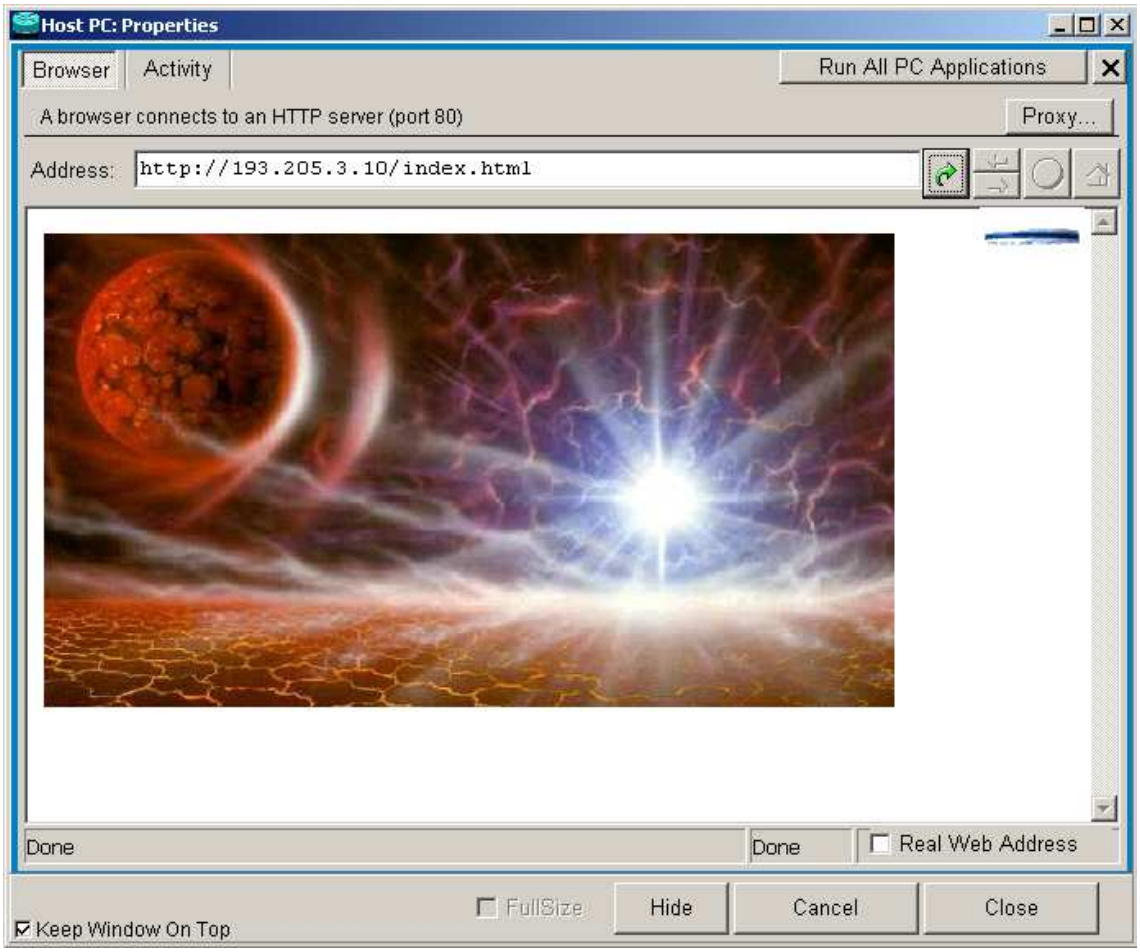
e il PC 1

```
C:>ping 193.205.3.10

Pinging 193.205.3.10 with 32 bytes of data:

Ping request timed out.
Ping request timed out.
Ping request timed out.
Ping request timed out.
```

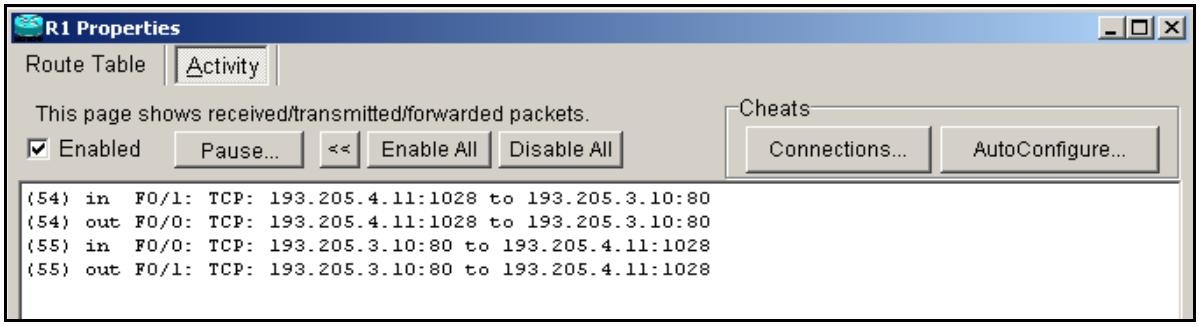


Vediamo ora di risolvere l'obiettivo 2

Andiamo sul PC 3 e proviamo con il browser a connetterci via http al pc 1



Mentre la finestra delle Activity di R1 riporta:

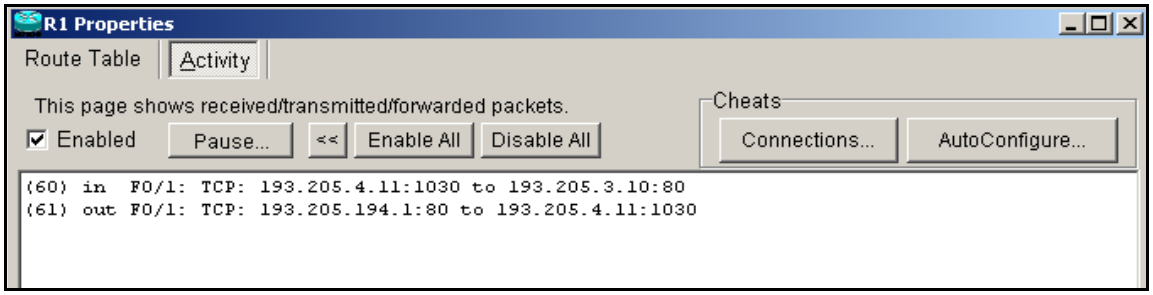


Impostiamo le ACL estese su R1 in modo da negare al PC3 l'accesso via http a PC 1

```
R1-2620(config)#access-list 102 deny tcp host 193.205.4.11 host 193.205.3.10 eq www
R1-2620(config)#access-list 102 permit ip 193.205.4.0 0.0.0.255 any
R1-2620(config)#interface F0/1
R1-2620(config-if)#ip access-group 102 in
R1-2620(config-if)#exit
R1-2620(config)#exit
```

Andiamo sul PC 3 e tramite il browser apriamo una connessione verso il server http sul PC 1

Vediamo che che non riusciamo a connetterci in quanto l'interfaccia F0/1 del router blocca i pacchetti.



Per verificare di aver operato correttamente attiviamo un http server sul PC dove è già attivo HTTP server (193.205.3.2).

Connettendosi con un browser a questo PC dal PC 3 si riesce a connettersi senza problemi. Quindi le ACL scritte sono congruenti con quanto voluto.