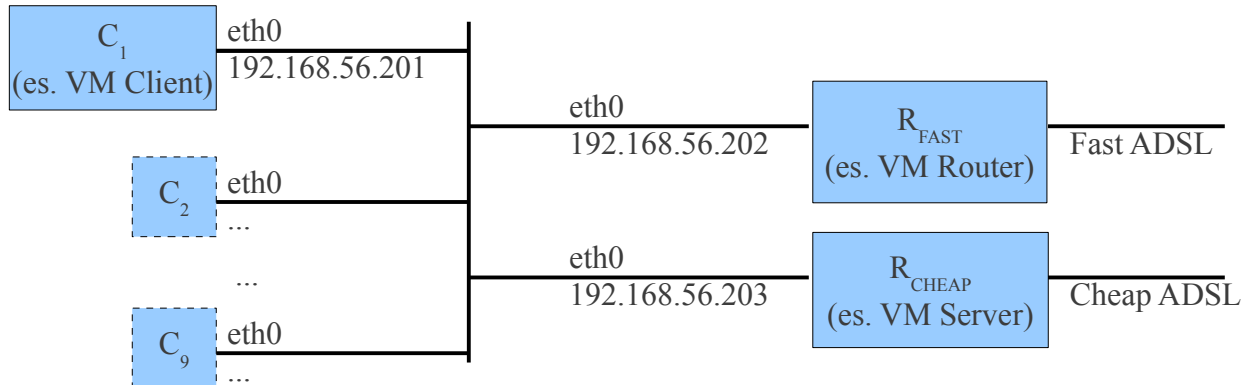


Laboratorio di Amministrazione di Sistemi T

Prova pratica - 11 febbraio 2013

Descrizione generale del problema

Si consideri la rete illustrata in figura, in cui i blocchi C_i (per i compreso tra 1 e 9) rappresentano host funzionanti come client di rete, collocati su di una rete privata su cui sono attestati anche due router/firewall Linux (R_{FAST} ed R_{CHEAP}) ciascuno connesso ad una propria linea ADSL verso Internet.



La linea connessa ad R_{FAST} è più veloce ed affidabile di quella connessa ad R_{CHEAP} , ma ha un costo legato all'utilizzo, mentre la seconda ha un costo indipendente dal traffico smaltito.

Per ricercare un buon compromesso tra costi d'esercizio e qualità del servizio, ogni utente ha a disposizione nell'arco di ogni ora una quota prefissata di traffico utilizzabile su R_{FAST} . Per ipotesi, ogni postazione C_x può essere utilizzata solo da un utente per volta, ed ogni utente può utilizzare solo una postazione per volta.

R_{CHEAP} è sempre utilizzabile. Nel caso l'utente richieda l'uso di R_{FAST} , il sistema soddisferà la richiesta a patto che non sia stata esaurita la quota di traffico assegnato, nel qual caso assegnerà forzatamente l'utilizzo di R_{CHEAP} . Allo stesso modo, se la quota assegnata viene superata durante l'utilizzo di R_{FAST} , il traffico generato dall'utente deve essere automaticamente re-instradato su R_{CHEAP} .

Per tener traccia del traffico generato da ogni utente si utilizza una directory LDAP. Il server LDAP è in esecuzione su R_{CHEAP} .

File da consegnare

utenti.schema - Definire un attributo *utente* di tipo testuale, un attributo *traffico* di tipo intero, ed una classe strutturale *consumi* che li contenga obbligatoriamente entrambi.

router-init.sh – Questo script predispone entrambi i router per il funzionamento (deve distinguere autonomamente su quale dei due è lanciato).

- Configura il packet filter per bloccare tutto il traffico non strettamente necessario (si noti che l'inoltro del traffico è sempre consentito su R_{CHEAP} , mentre per R_{FAST} si veda ping.sh)
- Logga ogni ping (ICMP echo request) ricevuto dalla rete dei client (indicare nei commenti come ottenere che i messaggi siano scritti sul file /var/log/pings attraverso rsyslog)

connetti.sh - Questo è lo script da eseguire sul client per richiedere l'impostazione del percorso di instradamento desiderato. Accetta come parametro una stringa che può valere "FAST" o "CHEAP", e non termina finché l'utente non preme Ctrl-C. Ogni minuto invia un ping al router indicato, e stampa a video qual è il router effettivamente impostato come default gateway.

snmpd.conf – file di configurazione dell'agent snmp dei client che consente di rilevare l'utente che ha in esecuzione il programma connetti.sh

ping.sh - Questo script deve essere permanentemente in esecuzione su entrambi i router (specificare nei commenti come si può ottenere che questo avvenga fin dal boot, garantendo il riavvio automatico in caso di terminazione accidentale) per osservare continuamente il file /var/log/pings.

Quando rileva un nuovo messaggio:

- se è in esecuzione su R_{CHEAP} imposta sul client richiedente il default gateway a R_{CHEAP}
- se è in esecuzione su R_{FAST} , individua via SNMP l'utente che ha inviato il ping e verifica via LDAP il traffico registrato per l'utente, dopodiché:
 - in caso il valore sia inferiore a 10MB, imposta sul client richiedente il default gateway a R_{FAST} , e abilita nel firewall le connessioni dal client ad Internet. Se le regole nel firewall esistono già, aggiorna il traffico dell'utente su LDAP incrementandolo del valore riportato da iptables.
 - in caso l'utente abbia superato la quota assegnata, imposta sul client richiedente il default gateway a R_{CHEAP}

resetta.sh - Questo script viene eseguito allo scadere di ogni ora (specificare nei commenti come si può ottenere questo effetto) per azzerare il valore dell'attributo *traffico* in ogni entry LDAP di classe *consumi*.

commenti.txt – vi sono situazioni in cui questo sistema può consentire accessi indesiderati o attribuzioni errate del traffico generato da un utente ad un altro utente? Nel caso, come si potrebbe risolvere il problema?