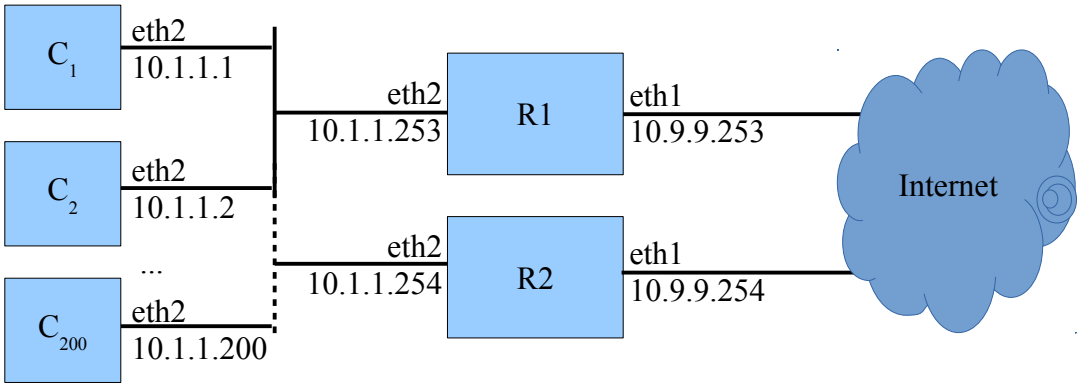
Laboratorio di Amministrazione di Sistemi T

Prova pratica – 15 gennaio 2016

Descrizione generale del problema

Si consideri la rete illustrata in figura, in cui i blocchi C_i (per i compreso tra 1 e 200) rappresentano workstation disponibili all'utenza, da usare come client, collocate su di una rete privata connessa a Internet attraverso due router/firewall configurati per garantire alta disponibilità.



I router possono essere utilizzati indifferentemente; i client operano la scelta in base al numero di connessioni servite, basandosi su di un registro conservato in directory LDAP replicata sui due router, e mantengono sotto controllo il router scelto per commutare sull'altro in caso di guasto.

File da consegnare

tutti gli script/file sono eseguiti/utilizzati su entrambi i router, salvo indicazione contraria

usage.schema – Definire gli attributi LDAP *client* e *router* (testuali) e *timestamp* (intero), e la classe *user* che li contenga obbligatoriamente tutti. Le entry di classe *user* rappresentano l'informazione che *client* ha scelto il *router* come default gateway all'istante *timestamp.*

route.sh (in funzione sui client) – Questo script interroga una directory LDAP (su R1 o su R2 indifferentemente, e se non risponde prova l'altra) per determinare quale router ha il minor numero di client che lo stanno utilizzando, e impostarlo come default gateway del client su cui viene lanciato. Successivamente non termina, ma inizia a inviare un "ping" ogni secondo al router prescelto, e nel caso non riceva risposta per tre volte consecutive commuta il default gateway sull'altro router, proseguendo con lo stesso tipo di monitoraggio sul nuovo router.
Ogni volta che lo script effettua una scelta di default gateway, tenta di registrarla su entrambe le directory LDAP, assicurandosi che l'entry che riguarda il proprio client sia unica.

init.sh – Questo script, appena avviato deve

- configurare il packet filter locale per consentire solo il traffico necessario ai vari script di questo testo;
- sostituire l'intero contenuto della directory LDAP locale col contenuto della directory dell'altro router.

Indicare nei commenti come far eseguire questo script al boot.

check.sh – Questo script rileva su quale router è in esecuzione, determina dalla directory LDAP locale quali client lo stanno utilizzando come default gateway, e per ognuno controlla via SNMP che lo script `route.sh` sia in esecuzione. Nel predisporre il controllo, si tenga conto del numero elevato di client, e si garantisca che possano essere raccolte tutte le risposte nel giro di pochi secondi.
Per ogni client su cui non viene trovato il processo, deve essere attivata su entrambi i router una regola di iptables che permetta di loggare ogni pacchetto da e per tale client.
Indicare nei commenti:

- come eseguire automaticamente lo script ogni 2 minuti;
- come configurare gli agenti snmp dei client per consentire il controllo;
- come predisporre i router perché possano eseguire l'uno comandi sull'altro;
- come configurare i router perché ogni messaggio di iptables generato su ognuno dei router venga scritto sul file `/var/log/orphans.log` di entrambi i router.

reset.sh – Questo script esamina continuamente il file `/var/log/orphans.log`. Per ogni riga che legge, determina se l'IP client in essa contenuto è stato osservato più di 10 volte nei due minuti precedenti.
Se si verifica questa condizione

- si collega al client e termina tutti i processi di utenti diversi da `root`
- rimuove su entrambi i router la relativa regola di logging inserita da `check.sh`