Progetto di Gestione delle Reti
Autori: D. Baccega, S. Berti, L. Cocchetti, M. Guani, F. Mecca

TeamViewer[1]

Tipologia di servizio: servizio di video conferenze e assistenza da remoto.

Chi sono gli utenti di TeamViewer? Coloro che vogliono fare conversazione online o coloro che hanno la necessità di controllare un desktop da remoto.

Chi sono gli utenti dell'architettura di network management? Siamo noi (i manager).

Indici di prestazione importanti: **tempo di risposta** (importante l'interattività; ordine dei centesimi di secondo), disponibilità (binaria), throughput (bit/s), jitter (qualità del video) ecc.

Core business: accesso remoto.

Quali sono le problematiche che giustificano un'architettura di network management? Come convinciamo un amministratore delegato ad installare TeamViewer?

- Adattabilità della trasmissione: la rete è dinamica. Dobbiamo interrogare continuamente la rete per poter adattare dinamicamente il servizio (in base allo stato della rete). Se abbiamo a disposizione tutta la banda, facciamo streaming al massimo della definizione. Se la banda cambia, diminuiamo la definizione (come fa Youtube, impostando su auto).
- Tempo di risposta: importante l'interattività del servizio.
- Mancato guadagno: evitare congestione, privilegiare utenti paganti (in modo tale che continuino a pagare), avere un sistema funzionante. Se il servizio è pessimo gli utenti non vorranno pagare l'abbonamento e quindi avremo delle perdite.
- Scalabilità a livello di rete: evitare congestione. Garantire una minima qualità a tutti gli utenti che usano il servizio gestendo, inoltre, tanti dispositivi connessi.
- Disponibilitá.
- Qualità del video.
- Gestione profili utente: privilegiare utenti paganti, gestione abusi (impedire ad un utente senza abbonamento di utilizzare il servizio per scopi di lucro), monitoraggio utilizzi (distinguo licenze domestiche e aziendali, controllo indici di prestazioni per migliorare il servizio).
- Outsourcing: pagamenti (abbonamenti, help desk nel caso in cui dei pagamenti non vadano a buon fine, aiuto installazione e problemi SW), pubblicità, ISP.

Descrizione testuale: TeamViewer è una soluzione all-in-one veloce e sicura che permette di accedere a computer e reti da remoto, con una serie di potenti funzionalità che semplificano il controllo remoto, i meeting e il mantenimento di un service desk basato sul cloud. La configurazione iniziale di TeamViewer non potrebbe essere più semplice: è sufficiente installare il software, indicare il tipo di utilizzo commerciale o privato, creare un nome utente e una password per il tuo computer. Una volta completato il processo di

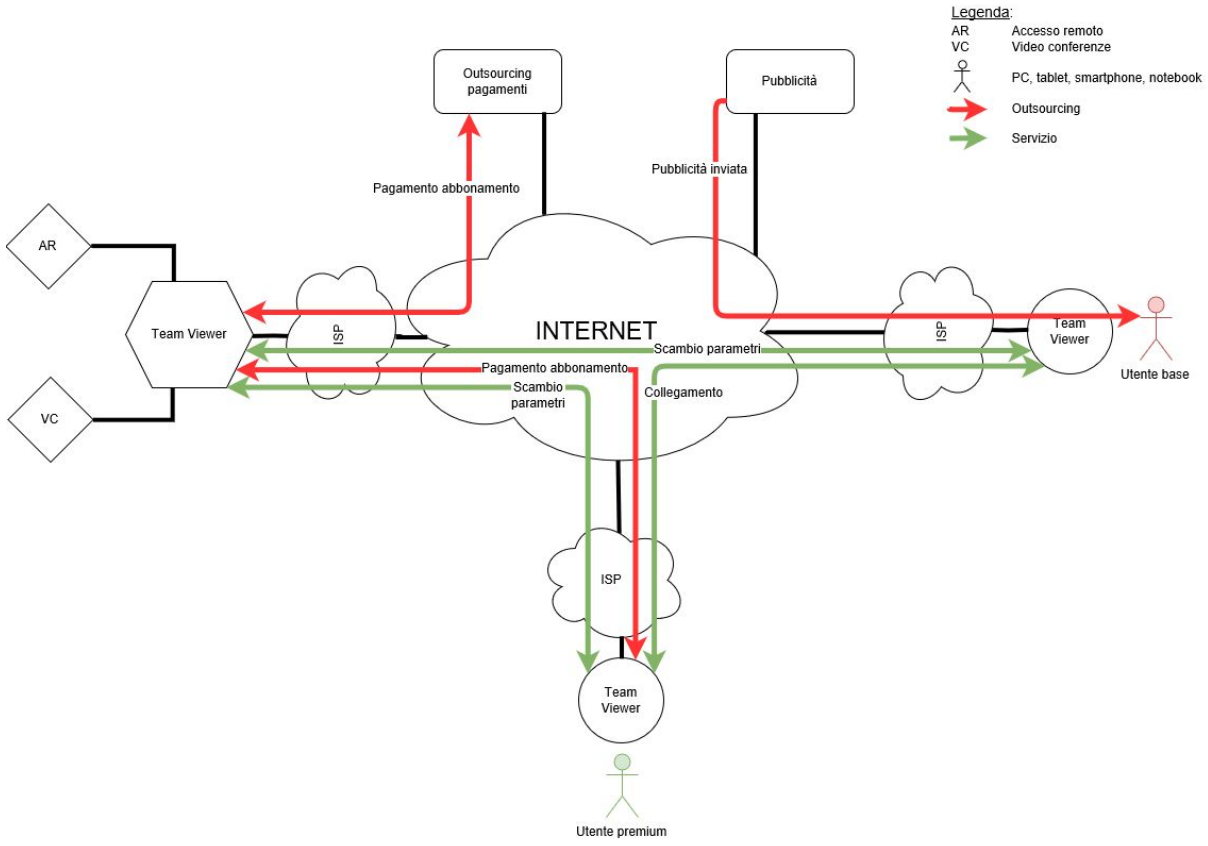
[1] Assunzione di base: TeamViewer funziona correttamente.

installazione, visualizzerai l'interfaccia principale di TeamViewer, suddivisa in due comode schede: controllo remoto e meeting.
E' possibile installare TeamViewer su computer fissi e notebook con sistema operativo Linux, Mac o Windows. Inoltre è disponibile un'app per tablet e cellulari Android e Apple che offre la possibilità di controllare computer fissi e notebook da remoto oltre a quella di fare videoconferenza.
Il servizio è disponibile in due versioni:

1. Utenze premium, senza limiti di banda e senza banner pubblicitari.
2. Utenze freemium, con licenza domestica e banner pubblicitari durante la fruizione.

All'avvio l'applicativo fornisce all'utente un codice e una password univoca per il controllo remoto. Mentre per quanto riguarda le videoconferenze ogni sessione tra più utenti ha un codice diverso e non necessita di password.
I meccanismi che regolano le videoconferenze e l'accesso remoto sono gestiti tramite Internet. Gli utenti, per connettersi, devono scambiare codici e password esternamente tramite e-mail, chiamata o messaggistica.
Il pagamento delle licenze è gestito con un collegamento a una società in outsourcing che accetta tutti i circuiti di pagamento standard. La pubblicità è affidata a una società in outsourcing che tramite profilazione dell'utente invia pubblicità opportune.

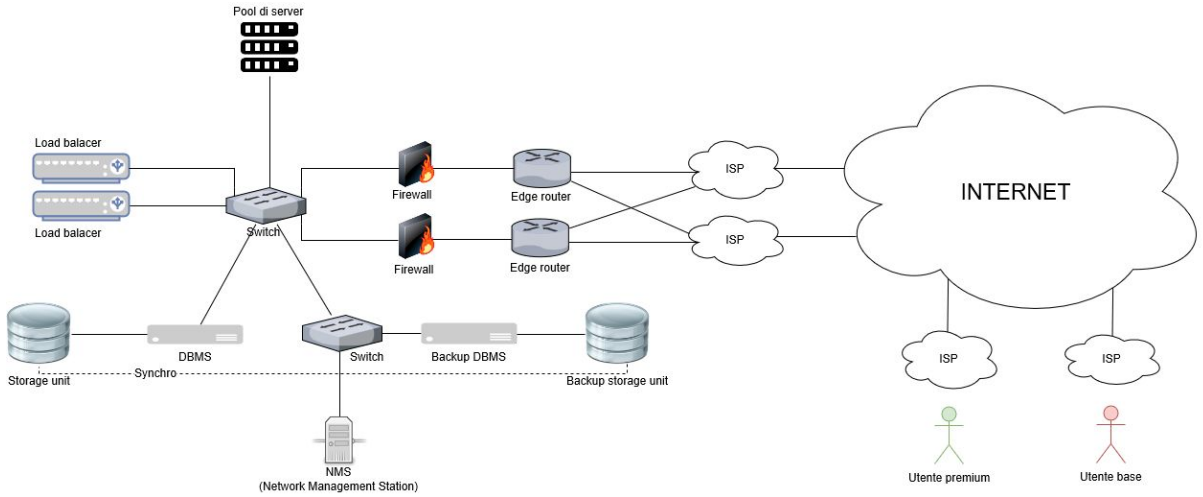
Modello logico:



Funzionalità coinvolte:

- Elaborazione: qualità video, compressori video e audio per accesso remoto e videoconferenze; generazione codice utente e password per accesso remoto e videoconferenze.
- Rete: gestione utenti multipli, load balancing, videoconferenze e accesso remoto.

Modello fisico:



Risk Management - Indici di prestazione:

Indici di prestazione che andiamo a monitorare:

- Tempo di risposta: timestamp di arrivo - timestamp di invio. Assumiamo di memorizzare all'interno della MIB degli agenti queste differenze. Associato alla problematica tempo di risposta. Gestita con polling e trap.
- Jitter (fluidità video): varianza dei tempi di interarrivo dei pacchetti.

  $$\sigma_X^2 = \mathbb{E}\left[\left(X - \mathbb{E}[X]\right)^2\right]$$

  dove X è la variabile casuale della differenza tra il timestamp di arrivo e di invio dei pacchetti.
  Assumiamo di memorizzare all'interno della MIB degli agenti queste differenze. Associato alle problematiche qualità del video e tempo di risposta. Gestita con polling.
- Throughput: assumiamo che l'informazione sia disponibile sugli agenti. Associato alla problematica adattabilità della trasmissione. Gestita con trap.
- Disponibilità: percentuale di tempo in cui il servizio è attivo e disponibile. Ping: ci dà informazioni su disponibilità e latenza (deve essere bassa la latenza). Immaginiamo che il manager invii un ping a ciascun dispositivo all'interno della sottorete ogni tot secondi. Associato alla problematica della disponibilità. Gestita con polling.
- Utilizzazione banda: ((bps trasmessi + bps ricevuti) / banda nominale) * 100. Ogni tot secondi prendiamo questa misura. Le informazioni sui bit trasmessi e ricevuti li abbiamo sugli edge router (ci interessano le interfacce verso gli ISP). Associato alla problematica adattabilità della trasmissione e della scalabilità a livello di rete (congestione). Gestita con trap (tramite una soglia, 75/80%).

- Utilizzazione risorse: utilizzazione CPU (Busy time / (Busy time + Idle time)) * 100 e RAM (RAM occupata / RAM totale) * 100. Ci interessa l'utilizzazione delle risorse dei server e dei load balancer. L'utilizzazione deve essere simile per ogni server. Se un server ha un'utilizzazione molto più alta degli altri, probabilmente il load balancer non sta funzionando bene. Informazioni memorizzate dentro ai server e ai load balancer. Associato alla problematica della disponibilità, del mancato guadagno e del tempo di risposta. Gestita con trap e polling (tramite una soglia, 60-70%).
- Fairness.

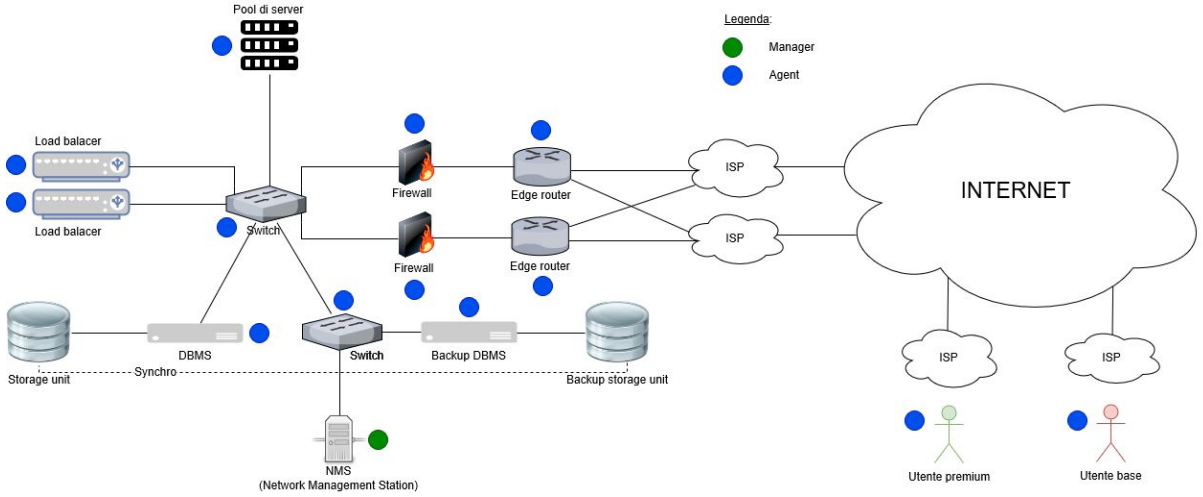
$$\mathcal{J}(x_1, x_2, \ldots, x_n) = \frac{(\sum_{i=1}^{n} x_i)^2}{n \cdot \sum_{i=1}^{n} {x_i}^2}$$

dove $x_1, x_2, \ldots, x_n$ rappresentano i throughput relativi ad n connessioni aperte.
A partire dalla formula generale, possiamo distinguere i seguenti casi:

1. fairness globale.
2. fairness tra i premium.
3. fairness tra i freemium.
4. fairness premium vs freemium.

Assumiamo che i throughput siano disponibili sugli agenti. Associata alla problematica gestione profili utente e alla scalabilità a livello di rete (congestione). Gestita con polling.

<u>Architettura di Network Management</u>:



Strategia di Controllo:
Problematiche scelte:

- tempo di risposta (indici: tempo di risposta, utilizzazione risorse)
- disponibilità (indici: disponibilità e utilizzazione risorse).

Tempo di risposta:
Tecnica di Monitoring: polling e trap.
Indici: tempo di risposta, utilizzazione risorse.

Assumiamo di memorizzare all'interno delle MIB degli agenti degli oggetti che fanno riferimento alle differenze tra il timestamp di arrivo e di invio dei pacchetti.
Quando un agente su un client registra nella MIB una differenza troppo grande fra il timestamp di arrivo e di invio di un pacchetto, notifica tramite trap il manager.
Quando il manager viene avvisato di una differenza di tempi maggiore rispetto alla norma, andiamo ad interrogare, tramite polling, ogni componente del sistema sul quale abbiamo una MIB (e quindi un agente) in modo tale da capire dove è avvenuto il rallentamento e/o la congestione e successivamente intervenire.
Assumiamo di avere nel server una MIB vendor con all'interno un oggetto chiamato notificaOk che permetta di notificare al Manager lo stato del sistema. Se i problemi non derivano dai componenti del sistema, allora il manager setta notificaOk a TRUE nella MIB del server. Il server successivamente notifica a livello applicativo il manager (umano) comunicandogli che non ci sono problemi all'interno del sistema. Inoltre notifica il client comunicandogli che i problemi sono lato client.

Intervento strutturale: eventuale aggiunta di HW.

- Problema dovuto al server: il manager tramite polling recupera l'utilizzazione delle risorse dai server. Se l'utilizzazione dei server è abbastanza bilanciata allora potrebbe essere necessario aggiungere ulteriore hardware sui server. Se l'utilizzazione dei server non è bilanciata, potrebbero esserci dei problemi sul/sui load balancer. A questo punto andiamo a recuperare, tramite polling, l'utilizzazione delle risorse sui load balancer e identifichiamo eventuali problemi (ad es. uno o più load balancer potrebbero aver subito un guasto; oppure i load balancer potrebbero essere sovraccarichi, in questo caso potrebbe essere necessario aggiungerne uno o aumentare le risorse di quelli presenti). In alternativa, il/i server e/o il/i load balancer notificano tramite trap il manager se notano che l'utilizzazione delle risorse ha superato la soglia stabilita.

Operazioni di controllo automatico:

- Problema dovuto alla rete: re-indirizzamento del traffico (andiamo a monitorare i componenti di rete) tramite la modifica delle tabelle di routing. Modifichiamo il campo ip (ipRouteTable) nella MIB-II degli edge router.
- Problema dovuto al server: riduzione della dimensione dei pacchetti inviati (qualità video) in caso di congestione delle risorse del server o della rete. In questo caso il manager modifica il parametro di configurazione del client

relativo alla dimensione dei pacchetti tramite modifica nella MIB dell'oggetto dimensionePacchetti.
- Nel caso non vengano individuati problemi nell'infrastruttura di rete sul server viene notificato il client tramite l'utilizzo dell'oggetto notificaOk. In questo modo il client saprà che c'è un problema su di sé, anche se non gli viene comunicato a cosa è dovuto.

Interventi manuali:
Nel caso in cui determinati problemi si ripetano nel tempo dovrà essere valutata una procedura di adeguamento dell'infrastruttura offerta.

Disponibilità:
Tecnica di Monitoring: polling e trap.
Indici: disponibilità e utilizzazione delle risorse.

Il manager periodicamente monitora la disponibilità di ogni componente dell'infrastruttura del servizio, tramite ping. Se non riceve risposta da un particolare componente oppure riceve risposta, ma con latenza elevata, allora significa che quel componente non è disponibile a causa di un guasto o momentaneamente non disponibile (e.g. perché le risorse sono congestionate).
Se l'utilizzazione delle risorse di un particolare componente (e.g. server o load balancer) supera la soglia prestabilita, agiamo come nel caso del tempo di risposta.

Intervento strutturale e manuale: eventuale aggiunta di HW.
- Problema dovuto al server: vedi tempo di risposta.
- Problema dovuto all'infrastruttura: analisi dei picchi di congestione dei router oppure guasti alle apparecchiature.
- In caso di guasti o congestione si valuta l'adeguamento dell'infrastruttura o la sostituzione delle componenti danneggiate con materiale più performante (tutto ciò eseguito dal personale di gestione).