# SNMP Monitoring

## Prerequisiti

Stazione di gestione (NMS)

- Piattaforma: Linux, Ubuntu 10.04
- Pacchetti:
    - **snmp**: è un insieme di applicazioni per eseguire le richieste ai diversi dispositivi che hanno un agente SNMP e che vogliamo monitorare. Operazioni: *snmpget, snmpgetnext, snmpset, snmpwalk, snmpnetstat, snmptrapd e snmptest*.
    - **MRTG**: Il pacchetto di codice sorgente può essere scaricato dal sito web (http://www.mrtg.org), anche se nella distribuzione Ubuntu è già distribuzione è già presente di default in uno dei repository.
    - **Apache2** minimo

OPZIONALE:

- strumento "**mib browser**". Interfaccia grafica per le operazioni snmp e per la visualizzazione delle MIB. Software: **openssh-server**: per l'amministrazione remota di questo server per mezzo di ssh

Macchina gestita (Agente)

- PC/Server - Linux. Questa apparecchiatura esegue una macchina virtuale, che è a sua volta il server proxy per la rete wifi.
- **snmpd**: è un agente SNMP installato localmente sul dispositivo da monitorare.

Questo progetto utilizzerà: SNMPv1 e SNMPv2, grazie alla loro ampia compatibilità, alla velocità di implementazione e alla non necessità di un rigoroso sistema di sicurezza per l'ambiente in cui si intende implementare.

## Gestione remota del server (NMS):

Per motivi di mobilità e convenienza, per gestire l'NMS si utilizza l'amministrazione remota.

1. Sulla stazione NMS installiamo un server ssh.
   *apt-get install openssh-server*
2. Sull'altra stazione installiamo il programma Putty (o un altro client ssh) per l'accesso remoto.

Kenya Fernández Upanga Mattricola: 659025

```
login as: user2
user2@10.10.127.233's password:
Linux STI2-NMS 2.6.32-31-generic #61-Ubuntu SMP Wed Aug 23 18:24:38
 GNU/Linux
Ubuntu 10.04.2 LTS

Welcome to Ubuntu!
 * Documentation: https://help.ubuntu.com/

Last login: Wed Aug 30 10:04:25 2023 from 192.168.25.47
user2@STI2-NMS:~$
```

*Figura 3.2. Connessione remota all'NMS con Putty*

## IMPLEMENTAZIONE SNMP (AGENTE)

Sul lato Agent, è necessario installare il pacchetto *snmpd*, che implementa un demone la cui funzione è rispondere alle richieste SNMP dell'NMS. L'installazione predefinita include le MIB per le interfacce di rete, la memoria, il disco, i processi e le statistiche della CPU.

*apt-get install snmpd*

File di configurazione:

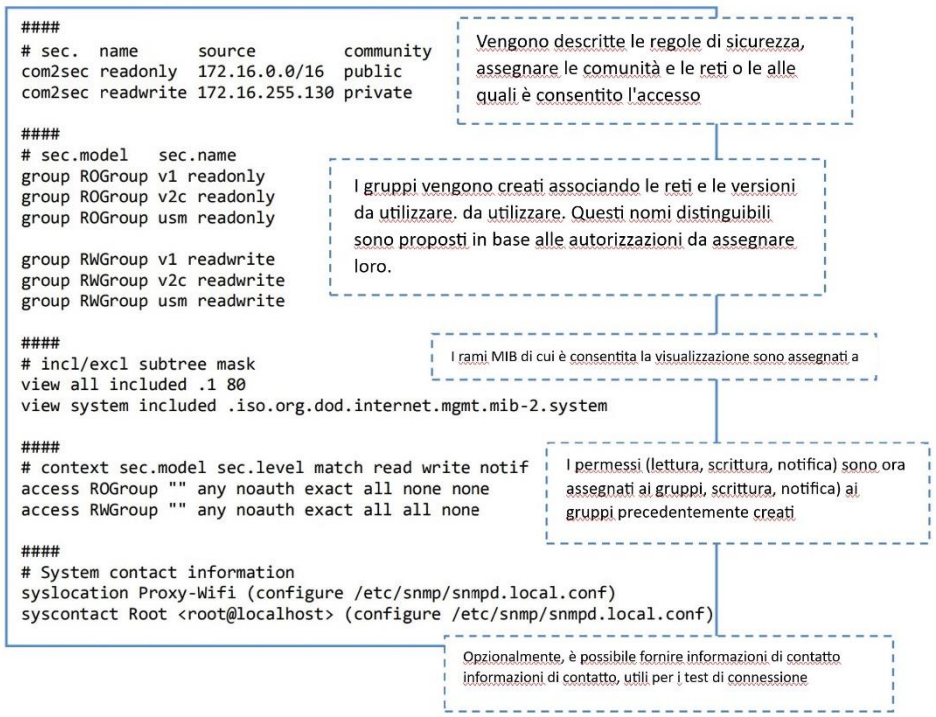
*/etc/defaults/snmpd*

In questo file dobbiamo eliminare: 127.0.0.1

(con questo si dice all'Agente di ascoltare le richieste su tutte le porte).

*/etc/snmp/snmpd.conf*

È configurato come segue:




Avviare l'agente con:

*/etc/init.d/snmpd start*

## IMPLEMENTAZIONE DI SNMP (NMS)

Abbiamo bisogno del seguente pacchetto per eseguire le interrogazioni all'agente per mezzo di operazioni SNMP:

*apt-get install snmp*

Per verificare se SNMP funziona correttamente, si utilizzano alcuni dei seguenti pacchetti operazione snmp:

*snmpget –v2c –c public 172.16.255.120 system.sysDescr.0*

Operazione Versione Comunità IP target OID

E restituisce:

*SNMPv2-MIB::sysDescr.0 = STRING: Linux xen-wifi 2.6.26-2-xen-amd64 #1 SMP Tue Jan 25 06:13:50 UTC 2011 x86_64*

Nel caso in cui non restituisca informazioni, è necessario controllare che siano stati seguiti tutti i passaggi e verificare che la configurazione sia corretta.

Se si desidera ottenere informazioni su una particolare variabile, è possibile accedere alle MIB installate con il pacchetto *snmp* e trovare l'OID appropriato. Le MIB sono memorizzate nella seguente directory:

*/usr/share/snmp/mibs/*

```
mib2c-data  mibs
root@ubuntu-snmp:/usr/share/snmp# cd mibs/
root@ubuntu-snmp:/usr/share/snmp/mibs# ls
AGENTX-MIB.txt                          OSPF-MIB.txt
BGP4-MIB.txt                            OSPF-TRAP-MIB.txt
BRIDGE-MIB.txt                          RFC1155-SMI.txt
DISMAN-EVENT-MIB.txt                    RFC1213-MIB.txt
DISMAN-SCHEDULE-MIB.txt                 RFC-1215.txt
DISMAN-SCRIPT-MIB.txt                   RIPv2-MIB.txt
EtherLike-MIB.txt                       RMON-MIB.txt
GNOME-SMI.txt                           SMUX-MIB.txt
HCNUM-TC.txt                            SNMP-COMMUNITY-MIB.txt
HOST-RESOURCES-MIB.txt                  SNMP-FRAMEWORK-MIB.txt
HOST-RESOURCES-TYPES.txt                SNMP-MPD-MIB.txt
IANA-ADDRESS-FAMILY-NUMBERS-MIB.txt     SNMP-NOTIFICATION-MIB.txt
IANAifType-MIB.txt                      SNMP-PROXY-MIB.txt
IANA-LANGUAGE-MIB.txt                   SNMP-TARGET-MIB.txt
IANA-RTPROTO-MIB.txt                    SNMP-USER-BASED-SM-MIB.txt
IF-INVERTED-STACK-MIB.txt               SNMP-USM-AES-MIB.txt
IF-MIB.txt                              SNMP-USM-DH-OBJECTS-MIB.txt
INET-ADDRESS-MIB.txt                    SNMPv2-CONF.txt
IP-FORWARD-MIB.txt                      SNMPv2-MIB.txt
IP-MIB.txt                              SNMPv2-SMI.txt
IPV6-ICMP-MIB.txt                       SNMPv2-TC.txt
IPV6-MIB.txt                            SNMPv2-TM.txt
IPV6-TCP-MIB.txt                        SNMP-VIEW-BASED-ACM-MIB.txt
IPV6-TC.txt                             SOURCE-ROUTING-MIB.txt
IPV6-UDP-MIB.txt                        TCP-MIB.txt
LM-SENSORS-MIB.txt                      TRANSPORT-ADDRESS-MIB.txt
NET-SNMP-AGENT-MIB.txt                  UCD-DEMO-MIB.txt
NET-SNMP-EXAMPLES-MIB.txt               UCD-DISKIO-MIB.txt
NET-SNMP-EXTEND-MIB.txt                 UCD-DLMOD-MIB.txt
NET-SNMP-MIB.txt                        UCD-IPFWACC-MIB.txt
NET-SNMP-TC.txt                         UCD-SNMP-MIB.txt
NET-SNMP-VACM-MIB.txt                   UDP-MIB.txt
NOTIFICATION-LOG-MIB.txt
```

*Figura 3.3. File MIB 1*

## IMPLEMENTAZIONE MRTG

Ubuntu contiene MRTG in uno dei suoi repository, quindi non dobbiamo compilarlo e possiamo procedere direttamente all'installazione:

*apt-get install mrtg apache2*

Il vantaggio di installare MRTG in questo modo è che installa automaticamente tutte le dipendenze di cui ha bisogno (GD, zlib, libpng). Nel comando includiamo anche l'installazione del server Apache.

Creiamo le cartelle in cui verranno salvati i file utilizzati da MRTG:

1. Per salvare le pagine HTML generate dallo script indexmaker.

*mkdir –p /var/www/mrtg*

2. Per salvare i file di configurazione generati da cfgmaker.

*mkdir /etc/mrtg*

Poiché monitoriamo una sola stazione, possiamo creare un solo file di configurazione. Questo verrà usato per monitorare le interfacce, il carico del sistema, memoria RAM, ecc. di questa macchina.

*cfgmaker --output /etc/mrtg/wifi.cfg public@172.16.255.121*

Eseguire il seguente comando per creare la pagina web index.html, con il file di configurazione MRTG specificato:

*indexmaker --output=/var/www/mrtg/index.html /etc/mrtg/wifi.cfg*

Eseguiamo ora il seguente comando per impostare la variabile d'ambiente e avviare il demone MRTG.

*env LANG=C /usr/bin/mrtg /etc/mrtg/wifi.cfg*

E ora resta da verificare che tutto abbia funzionato come previsto, per fare questo nella barra degli indirizzi di un browser digitare:

http://10.10.127.223/mrtg/index.html e si dovrebbe vedere la pagina index.html generata con indexmaker. è stata generata con indexmaker. Facendo clic su uno dei grafici si ottengono ulteriori informazioni sull'elemento monitorato. informazioni sull'elemento monitorato, con dati giornalieri, settimanali, mensili e annuali, nonché la legenda dei colori utilizzati con il loro significato. significato.

Se è necessario modificare un qualsiasi parametro del file di configurazione, è necesario riavviare il demone MRTG, e se si cambia qualche aspetto che modifica il grafico, inserire nuovamente il comando indexmaker.

## ANALISI

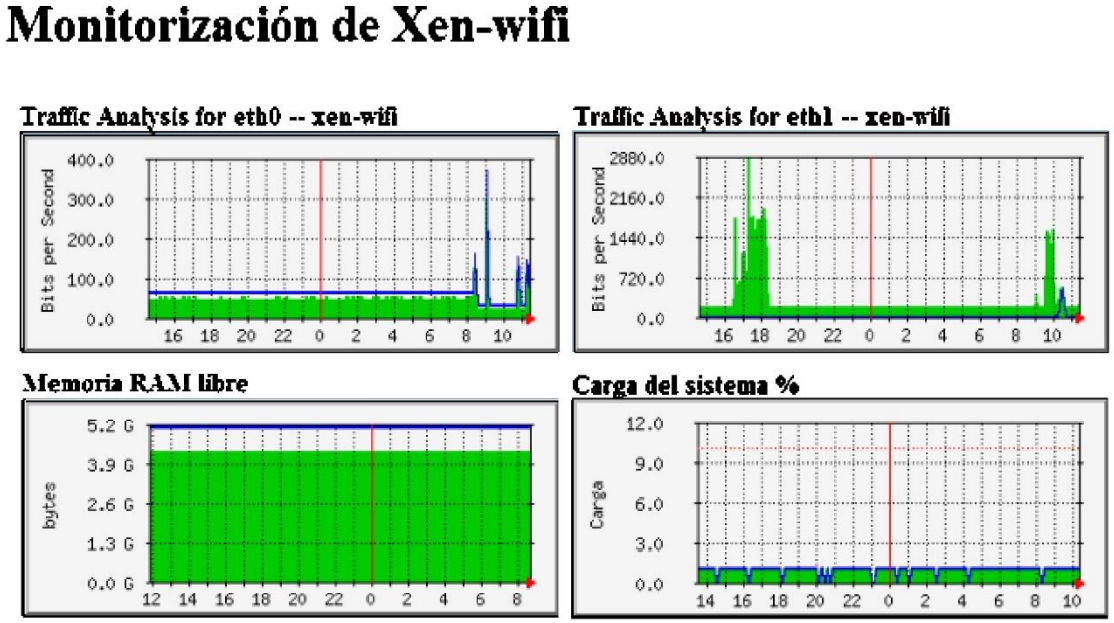



*Figura 4.1. Grafica generata da MRTG 1*

Una volta entrati nella pagina index.html possiamo vedere tutti i grafici configurati nel file wifi.cfg. Come si può vedere nell'immagine, sono stati creati grafici per tutte le interfacce (quelle che vengono caricate), per le interfacce (quelle caricate), per la memoria RAM e per il carico del sistema. Questi grafici corrispondono ai dati attuali (giornalieri), che vengono aggiornati ogni 5 minuti (come indicato nel file di configurazione).

Per capire cosa è rappresentato in ciascuno dei grafici, fare clic su di essi e seguire la legenda. Qui si possono vedere anche i grafici che raggruppano i dati per settimane, mesi e anni. I dati crescono da destra a sinistra e il tempo è regolato da 5 minuti per il grafico giornalieri, da giorni per i grafici settimanali, da settimane per i grafici mensili e da mesi per i grafici mensili.

Per questa analisi, l'attività è stata osservata in una settimana (dal 23° Agosto 2023, mercoledì, all'30 Agosto 2023).

È stata monitorata l'attività dei seguenti elementi:

- Interfaccia eth0 (interfaccia fisica, ip = 172.16.255.120).

- Interfaccia eth1 (interfaccia fisica, ip = 192.168.1.3).

- Memoria RAM

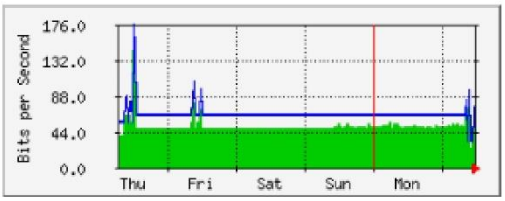
- Carico del sistema

### Interfaccia eth0:

Rappresenta il traffico in ingresso (verde chiaro) e in uscita (blu) su questa interfaccia, con IP: 172.16.255.120. su questa interfaccia, con IP: 172.16.255.120. Si prevede che il traffico a monte sia superiore a quello a valle, poiché questo collegamento è utilizzato per fornire il servizio wifi agli studenti. superiore al traffico downstream, poiché questo collegamento è utilizzato per fornire il servizio wifi agli studenti. Si può notare che questo dato è coerente e si possono distinguere gli orari di maggiore attività: tra le 8:00 e le 13:00, solo nei giorni

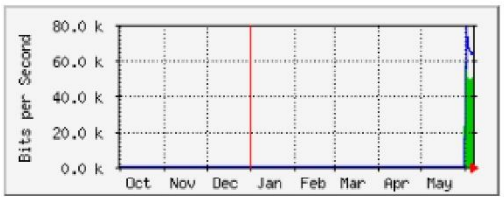
lavorativi. 13:00, solo nei giorni feriali. Non abbiamo osservato molto traffico, con una media di 48b/s per i download e 64b/s per gli upload. Nel grafico annuale si può vedere quando è iniziato il monitoraggio.

`Weekly' Graph (30 Minute Average)




| | Max | Average | Current |
|---|---|---|---|
| In | 144.0 b/s (0.0%) | 48.0 b/s (0.0%) | 64.0 b/s (0.0%) |
| Out | 176.0 b/s (0.0%) | 64.0 b/s (0.0%) | 80.0 b/s (0.0%) |

`Yearly' Graph (1 Day Average)

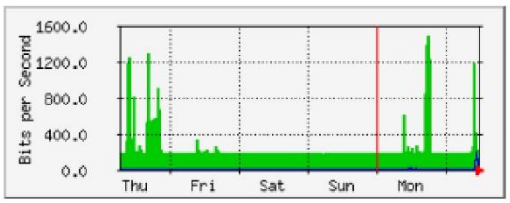



| | Max | Average | Current |
|---|---|---|---|
| In | 56.0 b/s (0.0%) | 48.0 b/s (0.0%) | 48.0 b/s (0.0%) |
| Out | 72.0 b/s (0.0%) | 64.0 b/s (0.0%) | 64.0 b/s (0.0%) |

## Interfaccia eth1:

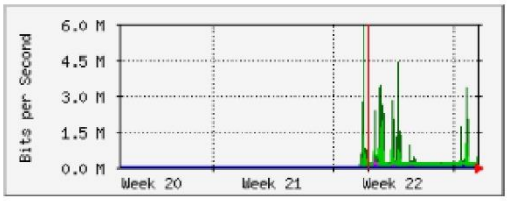
Rappresenta il traffico in entrata o download (verde chiaro) e in uscita o upload (blu) su questa interfaccia, con IP: 192.168.1.3. Su questa interfaccia, il tasso di download è superiore a quello di upload, il che è ragionevole dato che è qui che il traffico viene reindirizzato all'interfaccia precedente. Si notano dei picchi, anche se molto sporadici, in alcuni momenti della giornata, soprattutto nelle ore del mattino, e solo nei giorni lavorativi, in coincidenza con il grafico precedente. Questo schema suggerisce che c'è poco traffico su questa interfaccia, il che indica che la linea utilizzata è adeguata.

`Weekly' Graph (30 Minute Average)




| | Max | Average | Current |
|---|---|---|---|
| In | 1472.0 b/s (0.0%) | 240.0 b/s (0.0%) | 200.0 b/s (0.0%) |
| Out | 184.0 b/s (0.0%) | 0.0 b/s (0.0%) | 0.0 b/s (0.0%) |

`Monthly' Graph (2 Hour Average)

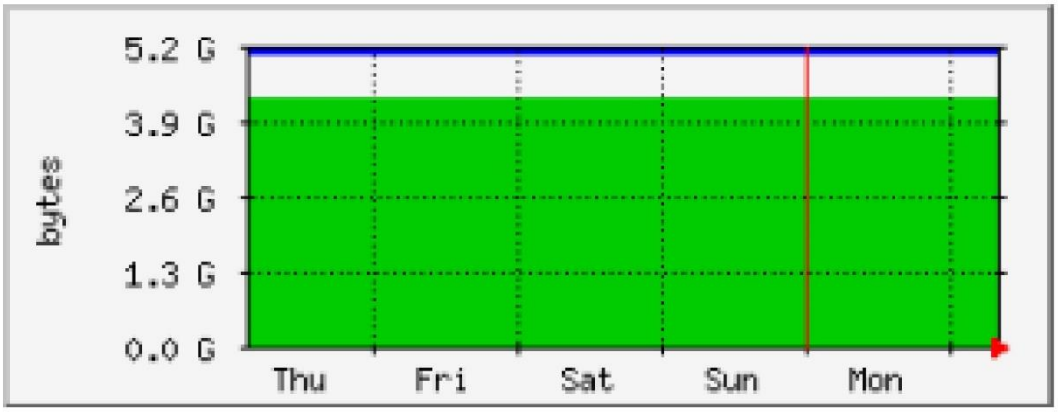



| | Max | Average | Current |
|---|---|---|---|
| In | 5976.0 b/s (0.0%) | 312.0 b/s (0.0%) | 456.0 b/s (0.0%) |
| Out | 280.0 b/s (0.0%) | 0.0 b/s (0.0%) | 0.0 b/s (0.0%) |

## Memoria RAM:

Rappresenta la memoria RAM totale (blu) e libero (verde chiaro), ne consegue che lo spazio lasciato vuoto è il RAM occupata o attiva. Potere dire che l'apparecchiatura monitorata ha 5 GB di RAM in totale e più 4 GB rimangono liberi. Questo risultato è stato osservato nella maggior parte o in tutti i tempo in cui il monitoraggio. A giudicare da questi dati questo computer ha una RAM più che sufficiente per eseguire queste e altre ancora numero di compiti.

# `Weekly' Graph (30 Minute Average)

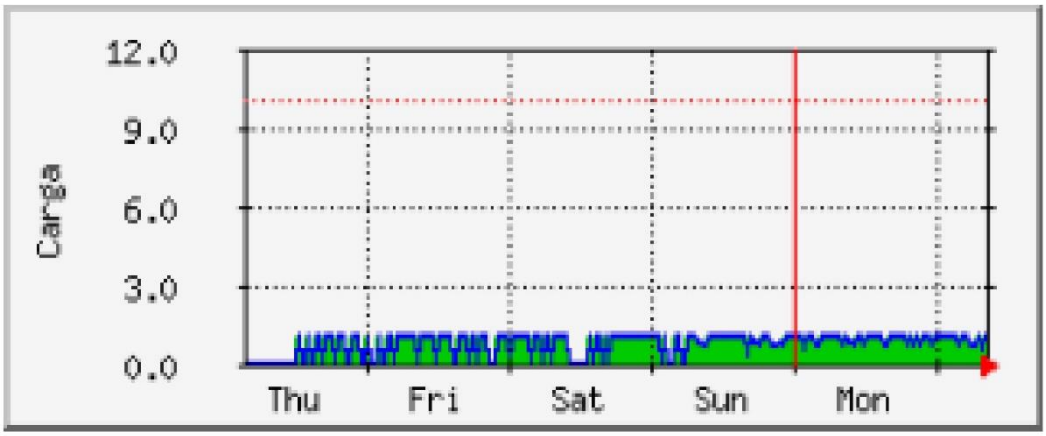



| | Max | Average | Current |
|---|---|---|---|
| Libre | 4292.8 Mbytes | 4277.2 Mbytes | 4266.7 Mbytes |
| Total | 5082.1 Mbytes | 5082.1 Mbytes | 5082.1 Mbytes |

Carico del sistema:

Rappresenta la media, negli ultimi minuto, la percentuale di tempo in cui i processori (4) avevano attività. In questo caso, 2 elementi non sono rappresentati, ma 1, il carico del sistema in percentuale (blu e verde chiaro). Come si può vedere, non lo so numero fino al 100% poiché non potrebbe essere distinguere il grafico che oscilla tra 1% e 0% la maggior parte delle volte. Deve essere evidenziare che le richieste che fai Gli MRTG si verificano ogni 5 minuti (il minimo consentito), il che renderebbe il tutto difficile incontrare picchi puntuali. Come possiamo vedere, in generale, la carica di questo sistema è molto basso, tenendo conto che al suo interno gira una macchina virtuale che funge da proxy, Ciò significa un impatto quasi nullo sulle prestazioni di questa apparecchiatura.

# `Weekly' Graph (30 Minute Average)




| | Max | Average | Current |
|---|---|---|---|
| Activo | 1.0 % | 1.0 % | 1.0 % |

Considerando quanto sopra, questa apparecchiatura è sufficientemente capace gestire il traffico che lo attraversa e funzionare correttamente sin dalla prestazione non è stato influenzato in nessun momento e i grafici suggeriscono che ne è capace per sopportare una maggiore quantità di attività, senza la necessità di sostituire il componenti menzionati.

Mostra

FILE DI CONFIGURAZIONE (wifi.cfg)

# Created by # /usr/bin/cfgmaker --output=/etc/mrtg/wifi.cfg public@172.16.255.120 ### Global Config Options # for Debian WorkDir: /var/www/mrtg ### Global Defaults # to get bits instead of bytes and graphs growing to the right Options[_]: growright, bits EnableIPv6: no RunAsDaemon: yes Interval: 5 Refresh: 305 #Suppress[_]: y WithPeak[_]: m XSize[_]: 250 YSize[_]: 100
######################################################################
# System: xen-wifi
# Description: Linux xen-wifi 2.6.26-2-xen-amd64
#1 SMP Tue Jan 25 06:13:50 UTC # Contact: Root (configure /etc/snmp/snmpd.local.conf)
# Location: Unknown (configure /etc/snmp/snmpd.local.conf)
######################################################################
########################
### Interface 12 >> Descr: 'eth0' | Name: 'eth0' | Ip: '172.16.255.120' | Eth: '$
Target[172.16.255.120_eth0]: #eth0:public@172.16.255.120:
SetEnv[172.16.255.120_eth0]: MRTG_INT_IP="172.16.255.120" MRTG_INT_DESCR="eth0"

MaxBytes[172.16.255.120_eth0]: 1250000
Title[172.16.255.120_eth0]: Traffic Analysis for eth0 -- xen-wifi
PageTop[172.16.255.120_eth0]:

# Traffic Analysis for eth0 -- xen-wifi

| | |
|---|---|
| System: | xen-wifi in Unknown (configure /etc/snmp/snmpd.local.conf) |
| Maintainer: | Root <root@localhost> (configure /etc/snmp/snmpd.local.conf) |
| Description: | eth0 |
| ifType: | ethernetCsmacd (6) |
| ifName: | eth0 |
| Max Speed: | 1250.0 kBytes/s |
| Ip: | 172.16.255.120 () |

### Interface 13 >> Descr: 'eth1' | Name: 'eth1' | Ip: '192.168.1.3' | Eth: " ###
Target[172.16.255.120_eth1]: #eth1:public@172.16.255.120:
SetEnv[172.16.255.120_eth1]: MRTG_INT_IP="192.168.1.3"
MRTG_INT_DESCR="eth1"
MaxBytes[172.16.255.120_eth1]: 1250000 Title[172.16.255.120_eth1]: Traffic Analysis for eth1 -- xen-wifi
PageTop[172.16.255.120_eth1]:

# Traffic Analysis for eth1 -- xen-wifi

| | |
|---|---|
| System: | xen-wifi in Unknown (configure /etc/snmp/snmpd.local.conf) |
| Maintainer: | Root <root@localhost> (configure /etc/snmp/snmpd.local.conf) |
| Description: | eth0 |
| ifType: | ethernetCsmacd (6) |
| ifName: | eth0 |
| Max Speed: | 1250.0 kBytes/s |
| Ip: | 192.168.1.3 () |

####RAM
LoadMIBs: /usr/share/snmp/mibs/ UCD-SNMP-MIB.txt
Target[wifi_mem]: memAvailReal.0&memTotalReal.0:public@172.16.255.120:::::2
PageTop[wifi_mem]:

# Memoria RAM libre

Options[wifi_mem]: nopercent,gauge,growright
Title[wifi_mem]: Memoria Libre
MaxBytes[wifi_mem]: 265300000000
YLegend[wifi_mem]: bytes
ShortLegend[wifi_mem]: bytes LegendI[wifi_mem]:  Libre
LegendO[wifi_mem]:  Total

Legend1[wifi_mem]: Memoria libre
Legend2[wifi_mem]: Memoria total

####Carga del sistema (suma de los 4 procesadores)
LoadMIBs: /usr/share/snmp/mibs/HOST-RESOURCES-MIB.txt
Target[wifi_load]:
hrProcessorLoad.768&hrProcessorLoad.768:public@172.16.255.120:::::2 +
hrProcessorLoad.769&hrProcessorLoad.769:public@172.16.255.120:::::2 +
hrProcessorLoad.770&hrProcessorLoad.770:public@172.16.255.120:::::2 +
hrProcessorLoad.771&hrProcessorLoad.771:public@172.16.255.120:::::2
MaxBytes[wifi_load]: 10
AbsMax[wifi_load]: 100
Title[wifi_load]: Carga del sistema
PageTop[wifi_load]:

# Carga del sistema %

Unscaled[wifi_load]: ymwd

ShortLegend[wifi_load]: %

YLegend[wifi_load]: Carga

Legend1[wifi_load]: Carga del sistema

LegendI[wifi_load]: Activo

Options[wifi_load]: nopercent,growright,gauge

---

MIBs

/usr/share/snmp/mibs/HOST-RESOURCES-MIB.txt

hrProcessorLoad OBJECT-TYPE

SYNTAX Integer32 (0..100)

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The average, over the last minute, of the percentage of time that this processor was not idle. Implementations may approximate this one minute smoothing period if necessary." ::= { hrProcessorEntry 2 }

/usr/share/snmp/mibs/UCD-SNMP-MIB.txt

memTotalReal OBJECT-TYPE

SYNTAX Integer32

UNITS "kB"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The total amount of real/physical memory installed on this host." ::= { memory 5 }

memAvailReal OBJECT-TYPE

SYNTAX Integer32

UNITS "kB"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The amount of real/physical memory currently unused or available." ::= { memory 6 }