Facultad de Ingeniera

Redes de Datos Seguras

Proyecto 2 — ORPHEUS

Monitoreo del tráfico a través del servicio de SNMP graficado con MRTG

Alumnos

- Garrido Czacki Mario Horacio
- Romero Andrade Cristian
- Romero Andrade Vicente

Equipo 3

Profesor: Ing. Edgar Martinez Meza

Índice

1. Resumen

En el siguiente trabajo se implementa un sistema de monitorización de red mediante el uso del protocolo SNMP y el software de monitoreo MRTG. Con esto se busca obtener un seguimiento visual de equipos en una red y poder realizar análisis de su comportamiento.

2. Objetivos

2.1. Objetivos Generales

- Conocer el funcionamiento de los protocolos de acuerdo a sus capas
- Utilizar una aplicacion real para la administracion y monitorizacion de una red
- Tener una presentacion final de la informacion recopilada a travez de la red

2.2. Objetivos Especificos

- Implementar un servicio MRTG que recopile los datos de una impresora o switch por medio de SNMP
- Mostrar los datos tratados por el MRTG en un servidor web seguro

3. Desarrollo

Lo primero a efectuar es la investigacion del funcionamiento de protocolo SNMP el cual tiene una historia y sus casos de uso que lo hacen ideal para la monitorizacion de dispositivos de red.

3.1. SNMP

Fue introducido en 1988 debido a la necesidad creciente de un estándar para administrar dispositivos sobre redes IP. Se trata de un protocolo de capa de aplicación (capa 7, OSI) que facilita el intercambio de información de gestión entre dispositivos de red.

Este protocolo es parte del conjunto de protocolos TCP/IP (Transmission Control Protocol/Internet Protocol) y, por su amplia utilización en redes empresariales, es considerado el estándar de facto en detrimento del protocolo CMIP (Common Management Information Protocol) basado en el modelo OSI, más utilizado en las grandes redes de las operadoras de telecomunicación. SNMP permite a los administradores: gestionar el rendimiento, encontrar y solucionar problemas, y planificar el crecimiento futuro de la red.

Si bien SNMP se diseñó, en un principio, con el propósito de hacer posible supervisar de forma sencilla y resolver problemas en routers y bridges; con su ampliación, este protocolo puede ser utilizado para supervisar y controlar: routers, switches, bridges y hubs de la mayoría de fabricantes, además de servidores y estaciones Windows y Unix, servidores de terminal, etc.

La información que se puede monitorizar son parámetros simples y estandarizados para todos los routers y/o switches (independientemente del fabricante) como por ejemplo la cantidad de tráfico de entrada y salida de una interfaz, el tiempo que llevan encendidos, la carga de CPU, etc. Y parámetros más específicos proporcionados por el fabricante del dispositivo, como puede ser la temperatura.

Se pueden resumir sus características en los siguientes puntos:

- Permite a los administradores gestionar el rendimiento de la red, buscar y modificar la información de los dispositivos que la componen, encontrar y diagnosticar problemas en la red, planificar su crecimiento y generar informes sobre los nodos de la red.
- Es capaz de gestionar eficazmente dispositivos de diferentes fabricantes.
- Ofrece una simple combinación de solicitud-respuesta y un modo de notificación activo, así como tiempo de espera y mecanismos de retransmisión.
- Contiene pocos tipos de paquetes con un formato sencillo, facilitando su resolución e implementación.
- Dispone de mecanismos de autenticación y privacidad como medidas de
- Emplea UDP en el puerto 161 para el envio y recepcion de solicitudes
- Empleta UDP en el puerto 162 para la recepcion de los agentes “traps”
- Existen 3 versiones del protocolo
  - SNMPv1 — version inicial del protocolo estandarizado
  - SNMPv2-c — Solventa problemas de seguridad y sobrecargas en transferencias de datos.
  - SNMPv3 — Añade esquemas de autenticación y encriptación

3.2. SMI y MIB

La SMI (Structure of Managemet Information) se encarga de definir un esquema de nombres únicos para cada uno de los objetos administrados y su comportamiento (denominado OID). El agente posee una lista de los objetos que son supervisados, como puede ser el estado operacional de la interfaz de un router (“up” o “down”).

La MIB (Management Information Base) se puede considerar como una base de datos que almacena información (los OIDs con su descripción) de los dispositivos administrados. Al igual que el Agente reside en cada uno de los dispositivos gestionados. Las MIBs contienen objetos que representan parámetros o variables de los equipos gestionados y se ordenan de forma jerárquica siguiendo un esquema de árbol. Estas colecciones de objetos relacionados, definidos como módulos de MIB. Estos módulos están escritos en un lenguaje especial, definido en el estándar de Internet STD 58, y en los RFCs de Internet 2578, 2579 y 2580.

Cada elemento del árbol MIB se identifica por un OID (Object Identifier) numérico o de texto. La lista completa de los objetos y su definición correspondiente está definida en el RFC 1212.

3.3. MRTG

Se trata de una herramienta para monitorizar diversos parámetros de red y generar páginas HTML que contienen imágenes (con formato PNG) que proporcionan una representación gráfica en vivo de los datos que obtiene del protocolo SNMP o de scripts.

Entre las características más importantes de MRTG tenemos las siguientes:

- Está escrito en Perl.
- Utiliza una aplicación SNMP portátil escrito completamente en Perl, por lo que no hay necesidad de instalar ningún paquete externo SNMP.
- Las interfaces de routers pueden ser fácilmente identificadas por su dirección IP, la descripción y la dirección Ethernet además de la interfaz de serie normal.
- Los gráficos son generados directamente en formato PNG
- El aspecto de las páginas web producidas por MRTG así como la configuración de este son altamente configurables.

MRTG consiste en un script de Perl que utiliza el protocolo SNMP para controlar cualquier variable que se elija, y un rápido programa en C que registra el tráfico de datos y crea los gráficos para representarlos. Estos gráficos se incrustan entonces en páginas web.

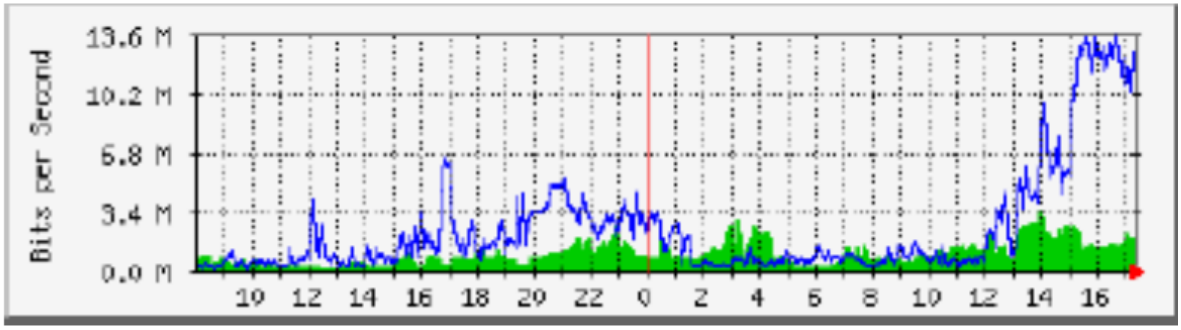

Figura 1: Grafica generada con MRTG.

4. Configuracion

Para esta configuracion se hizo uso de un equipo con las siguientes caracteristicas:

- Computadora conectada via inalambrica a internet
- Archlinux como sistema operativo
- Servidor Nginx configurado con un dominio

Los pasos seguidos son los siguientes:

- Instalar MRTG

```
pacman -S mrtg
```

- Crear el usuario mrtg

```
useradd -d /srv/http/mrtg mrtg
```

- Crear el directorio home del usuario y darle permisos

```
    mkdir /srv/http/mrtg
    chown mrtg:mrtg /srv/http/mrtg

```

- asignar el dominio y su configuracion a nginx

```
    cp /configs/mrtg.somch.org /etc/nginx/available-site/
    ln -s /etc/nginx/available-sites/mrtg.somch.org /etc/nginx/
    enabled-sites/mrtg.somch.org
    systemctl reload nginx

```

- Crear el directorio que albergara los archivos PNG y el index

```
    mkdir /srv/http/mrtg/html

```

- Crear el archivo de configuracion mrtg

```
    cfgmaker --output=/srv/http/mrtg/mrtg.cfg --ifref=name --ifref=
    descr --global "WorkDir: /srv/http/mrtg" igg@132.247.103.251

```

- Añaidr los parametros extra al archivo mrtg.cfg generado

```
    ### Global configuration ###
    LoadMIBs: /usr/share/snmp/mibs/UCD-SNMP-MIB.txt
    EnableIPv6: no
    HtmlDir: /srv/http/mrtg/html
    ImageDir: /srv/http/mrtg/html
    LogDir: /srv/http/mrtg
    ThreshDir: /srv/http/mrtg
    RunAsDaemon: Yes
    Interval: 5
    Refresh: 60

```

1. Corresponde a la base de datos gestionada MIB que contiene los parametros de los dispositivos compatibles
2. Deshabilita el IPv6
3. La ruta de los archivos html
4. La ruta de las imagnes PNG
5. La ruta de los archivos log
6. El folder thresh
7. Correr como demonio
8. Intervalo en minutos del demonio, 5 minutos.

9. Intervalo de refresco de archivos html.

- Una vez creado el archivo de configuracion ir al directorio /srv/http/mrtg y crear el index

```
    cd /srv/http/mrtg
    indexmaker ./mrtg.cfg > index.html

```

- Crear el servicio que demonizara el servicio MRTG que obtendra los datos

```
    cp configs/mrtg.service /usr/lib/systemd/system
    systemctl enable mrtg
    systemctl start mrtg

```

- Abrir el dominio en el navegador y observar los resultados

4.1. Archivos de configuracion usados

Archivo de la configuracion del subdominio de nginx

```
server {
    server_name mrtg.somch.org www.mrtg.somch.org;
    root /srv/http/mrtg;
    index index.html index.htm;
    allow 127.0.0.1;
    allow 0.0.0.0/0;
    deny all;
    location ~* .(png|jpg|jpeg|gif|ico)$ {
    }
    include /etc/nginx/custom_error.conf;

    listen 443 ssl; # managed by Certbot
    ssl_certificate /etc/letsencrypt/live/mrtg.somch.org/fullchain.pem; # managed by Certbot
    ssl_certificate_key /etc/letsencrypt/live/mrtg.somch.org/privkey.pem; # managed by Certbot
    include /etc/letsencrypt/options-ssl-nginx.conf; # managed by Certbot
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot

}
server {
    if ($host = mrtg.somch.org) {
        return 301 https://$host$request_uri;
    } # managed by Certbot


    server_name mrtg.somch.org www.mrtg.somch.org;
    listen 80;
    return 404; # managed by Certbot
}
```

Script que ejecuta el demonio

```
#!/bin/bash
LANG=C /usr/bin/mrtg --pid-file=/run/mrtg/mrtg.pid --user=mrtg --group=
    mrtg --daemon /srv/http/mrtg/mrtg.cfg
```

Archivo de configuracion systemd

```
[Unit]
      Description=Multi Router Traffic Grapher
      After=network.target
[Service]
      PIDFile=/run/mrtg/mrtg.pid
      User=mrtg
      Group=mrtg
      ExecStart=/usr/lib/systemd/scripts/mrtg.sh
      ExecReload=/usr/bin/kill -USR2 $MAINPID
      KillSignal=SIGQUIT
      KillMode=mixed
[Install]
      WantedBy=multi-user.target
```

Siglas

M

MRTG Multi-Router Traffic Grapher. 2–4, 6

S

SNMP Protocolo Simple de Administración de Red, del inglés Simple Network Management Protocol. 2–4