Multi Router Traffic Grapher (MRTG)

Sistemin Açıklanması ve Red Hat Linux Üzerine Kurulumu

Celal ÜNALP (celak@ttnet.net.tr)

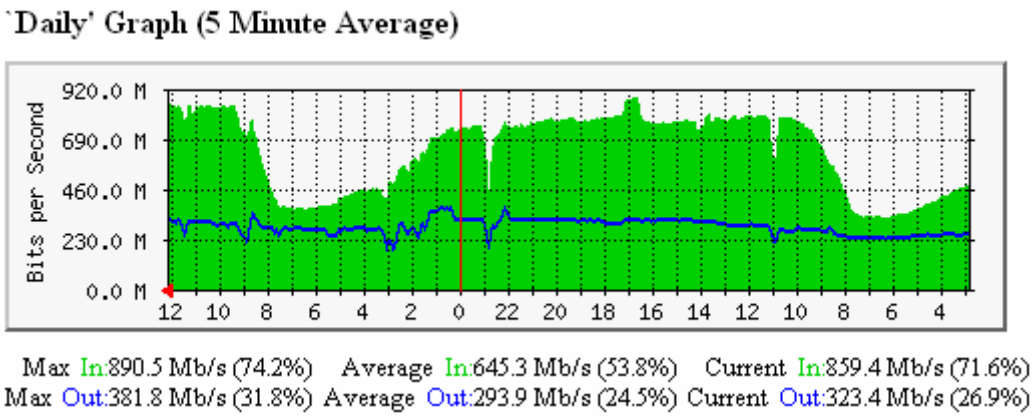
20 Haziran 2003 – ANKARA

Sürüm 0.9

Multi Router Traffic Grapher (MRTG) Nedir?

Multi Router Traffic Grapher, ağ bağlantılarındaki trafik yükünü izlemeye yarayan bir araçtır. MRTG, ağ bağlantılarındaki trafiğin anlık (canlı olarak) izlenmesine olanak veren grafiksel içerikli HTML sayfaları oluşturur. Örnek bir grafik *şekil-1* de görülmektedir. MRTG, Perl ve C programlama dillerini kullanarak çalışır. UNIX ve Windows işletim sistemleri altında çalışabilen MRTG, internet üzerinde bir çok sitede kullanılmaktadır.

Bu belgede, Red Hat Linux işletim sistemi üzerine MRTG kurulumu anlatılacaktır.



Şekil-1 Standart bir MRTG trafik izleme grafiği

Önemli Özellikleri Nelerdir?

Taşınabilir Olması

MRTG, bir çok UNIX ve Windows işletim sisteminde çalışmaktadır. Böylece ihtiyaç durumunda sistemler arasında aktarılması çok kolay olmaktadır.

Perl (Practical Extraction and Report Language)

MRTG, Perl ile yazılmıştır ve tüm koduyla(açık) beraber gelmektedir.

Taşınabilir SNMP

MRTG, kendi taşınabilir SNMP sistemiyle birlikte gelir. Ayrıca bir SNMP paketi kurmaya gerek yoktur.

SNMPv2c Desteği

MRTG, yeni SNMPv2c sayaçlarını okuyabilir. Sayaç sıkıştırmasına gerek kalmamıştır.

Güvenilir Arayüz Tanımlamaları

Cihaz arayüz tanımlamaları, IP adresine göre, özel tanımlara göre veya ağ adreslerine(MAC) göre yapılabilir. Karışıklıklar bu şekilde kolayca önlenebilir.

Sabit Boyutlu Kayıt (Log) Dosyaları

MRTG kayıt dosyalarının, özel konsolide bir algoritma sayesinde, boyutları artmaz.

Otomatik Ayarlanabilme

MRTG, kurulum ve ayarlamayı kolaylaştıran bir çok aracı da yanında getirir.

Performans

Kritik zamanlı işlemler, C programlama diliyle yazılmıştır.

GIF Kullanmayan Grafikler

İzleme grafikleri, Thomas Boutell'in GD kütüphaneleri kullanılarak doğrudan PNG biçiminde yaratılmaktadır. Ticari bir dosya tipi kullanılmamaktadır.

Özelleştirilebilme

MRTG tarafından yaratılan web sayfalarının görünümü, istenildiği gibi düzenlenebilmektedir.

RRDtool

MRTG, bütünleşik olarak RRDtool kullanabilir. Performans kazanmak için gerekebilir.

Ayrıntılar

MRTG, SNMP yoluyla ağ cihazlarının trafik istatistiklerini toplayan bir Perl betiği ile istatistikleri kaydederek bunlara dayalı anlaşılır grafikler çizen bir C programından oluşmaktadır. Web sayfalarına iliştirilen bu grafikler, her türlü güncel web tarayıcısı tarafından görülebilmektedir.

Otomatik olarak hazırlanan web sayfalarında, ayrıntılı günlük görünümün yanında, geçmiş 7 günün, geçmiş 5 haftanın ve son 12 ayın istatistikleri de görsel olarak izlenebilmektedir. MRTG, bu izlemeler için geçmişe dönük kayıt tutmaktadır. Bu kayıtları tutmak için kullanılan özel algoritma sayesinde, bir çok kayıt sisteminin aksine, MRTG kayıt dosyası boyutları zamanla artmamaktadır. Bunun yanında geçmiş iki yıla yönelik kayıtlar sorunsuzca saklanabilmektedir.

MRTG sisteminin etkin yapısı sayesinde, sıradan bir UNIX kullanarak 200'ün üzerinde ağ bağlantısını izleyebilirsiniz.

MRTG kullanımı yalnızca ağ trafiği izlemekle sınırlı değildir. İzlemek istediğiniz herhangi bir SNMP değerini tanımlayabilirsiniz. Cihazlardan bilgi toplamak için ayrı bir program da kullanmak mümkündür. MRTG kullanıcıları, ağ istatistikleri yanında, işletim sistemi yükü, oturum işlemleri(login/session/logout), modem havuzları ve yazıcı kullanımlarını da takip etmektedirler. MRTG ile iki farklı veri grubunu tek bir grafikte görüntülemek de önemli kullanım alanlarından biridir.

Lisanslama İlkeleri

MRTG, *GNU General Public License* kuralları kapsamında ücretsiz olarak temin edilebilir.

Red Hat Linux Üzerine MRTG Kurulumu

İşletim Sistemi ve Çevre Bileşenleri:

Kurulumda işletim sistemi olarak Red Hat Linux 8.0 kullanılacaktır. İşletim sistemi hakkında bilgi ve tecrübeye sahip olmak, gerekli güncellemeleri yapmak uygulayıcıya bırakılmış konulardır.

Uygulamanın boyutlarına göre uygun bir donanım seçilmelidir. MRTG, daha önce de açıklandığı üzere anlık bilgiler sağladığı gibi geçmişe dönük izleme ve analiz yapmamıza da olanak sağlayan bir araçtır. Geçmişteki verileri kullanarak geleceğe dair doğru kararlar almak daima etkin bir planlamanın parçasıdır. Bu yüzden seçeceğimiz donanım bizi yarı yolda bırakmayacak türden olmalıdır. Gelecekteki olası bir kapasite artışı ya da azalışı kararı/ihtiyacı, ancak kesintisiz veri toplamayla doğru sonuca ulaşabilecektir.

- Uygulamanın hangi seviyeye kadar inebildiğini göstermek için çok basit bir donanım bileşimi kullanacağım:

Donanım	**Değerler**
IBM PC300	Kişisel Bilgisayar
İşlemci	INTEL Pentium 166 MMX
Bellek	64 MB
Sabit Disk Kapasitesi	10 GB (IDE HDD)
Ağ Kartı	3Com 3C905C-TX 10/100 Mbit

Red Hat Linux kurulumu ihtiyaçlarınıza en uygun şekilde yapılmalıdır. Linux üzerinde sadece MRTG ve web sunucu çalışacağı için diğer gereksiz paketler ya hiç kurulmamalı ya da kurulumdan sonra kaldırılmalıdır. Bu işlem, unutularak açık bırakılan gereksiz servislerin sistem üzerinde yaratacağı yükü azaltacak ve bunlardan doğabilecek olası güvenlik açıklarını en baştan bertaraf edecektir.

Bu aşamada "*Sunucu Kurulumu*" türü seçilerek işletim sistemi yüklenecektir.

Red Hat Linux işletim sisteminde, MRTG sistemini kullanacağınız ağ yapısına uygun olarak TCP/IP ayarlarını yapıp test edin.

Kurduğumuz Linux işletim sisteminde, gerekli TCP/IP ayarlarını yapalım:

```
IP ADDRESS : 192.168.2.213
NETMASK    : 255.255.255.0
```

Aynı ağdaki birkaç farklı IP adresini pingleyerek erişimi test edelim.

- Denemeler için aynı ağ üzerinde çalışmakta olan "Cisco 1751 Router" ve bu ağın internet bağlantısını sağlayan "Motorola SurfBoard SB3100 kablo modem" kullanacağım.
(izlemek istediğiniz cihazlar, linux ile aynı ağ üzerinde olmak zorunda değildir.)

Cisco 1751 Router Hakkında Gerekli Bilgiler :

```
router>show interfaces

FastEthernet0 is up, line protocol is up
  Hardware is PQUICC_FEC, address is 0003.6b9a.1cfc
  Description: connected to EthernetLAN
  Internet address is 192.168.2.254/24
...

Serial0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set
...

Serial0.1 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Description: connected to Cisco1750_1
  Internet address is 10.0.0.2/30
```

Cisco router, SNMP yoluyla bilgi alışverişine hazır hale getirilmelidir:

```
router>enable
Password:
router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#snmp-server community public ro
```

Motorola SurfBoard SB3100 Kablo Modem Hakkında Gerekli Bilgiler :

Kablo TV şebekesi üzerinden internet bağlantısı sağlayan bir çok abone bu modemi kullanmaktadır. Bu modem kullanıldığı ortamdan bağımsız olarak genelde 192.168.100.1 IP adresini almaktadır. Bunu değiştirmek için modem çalışırken http://192.168.100.1/config.html adresine girilebilir. Bu modem için SNMP haberleşmesi her zaman açıktır.

RPM Kullanarak MRTG'nin Kurulumu :

Kurulum için öncelikle MRTG'nin RPM kurulum dosyasına ihtiyacınız olacaktır.
Bu dosyayı Red Hat Linux 8.0 kurulum CD'lerinin üçüncüsünden bulabileceğiniz gibi daha güncel bir sürüm için ftp://ftp.linux.org.tr adresini de ziyaret edebilirsiniz.

Kurulum CD'sinden bulmanız gereken dosya ***mrtg-2.9.17-8.i386.rpm*** olacaktır.

Kurulum yapmadan önce, başka RPM dosyalarına ihtiyaç olup olmadığına bakmalısınız :

```
[root@camel /mnt/cdrom/RedHat/RPMS]# rpm -i --test mrtg-2.9.17-8.i386.rpm
warning: mrtg-2.9.17-8.i386.rpm: V3 DSA signature: NOKEY, key ID db42a60e
```

Herhangi bir uyarı vermeden testi tamamladı. Artık RPM paketini kurabiliriz :

```
[root@camel /mnt/cdrom/RedHat/RPMS]# rpm -ivh mrtg-2.9.17-8.i386.rpm
warning: mrtg-2.9.17-8.i386.rpm: V3 DSA signature: NOKEY, key ID db42a60e
Preparing...                ########################################### [100%]
   1:mrtg                   ########################################### [100%]
```

Kurulum da sorunsuz şekilde tamamlandı. MRTG, kullanıma hazır.

Cfgmaker Kullanarak Temel Ayar Dosyalarının Oluşturulması

Daha önce de belirtildiği gibi, MRTG yanında bir çok yardımcı araçla gelmektedir. Bunların en önemlisi "/usr/bin/cfgmaker" betiğidir. Bu dosyayı kullanarak, izlemek istediğimiz cihazlar için otomatik olarak ham bir ayar dosyası yaratabiliriz.

Bu betikle ilgili ayrıntılı bilgi almak için komut satırına herhangi bir parametre vermeden *cfgmaker* yazın. Betiğin kullanımıyla ilgili açıklamalar görüntülenecektir. Daha düzenli bilgi almak için *cfgmaker man* sayfalarına bakabilirsiniz.

Bu belgede, öncelikle ham ayar dosyasını en çok kullanılan şekilde oluşturup daha sonra bu dosya üzerinde istediğim değişiklikleri yapma yolunu takip edeceğim.

İlk olarak Cisco Router ile ilgili bilgileri geçici bir dosya içine almak istiyorum. Bunun için cfgmaker programını daha önce router üzerinde yaptığım ayarlara uygun olarak çalıştırıp bulunduğum dizinde deneme001.cfg adında bir ham ayar dosyası oluşturacağım :

```
[root@camel root]# cfgmaker public@192.168.2.254 > deneme001.cfg
```

Bu komut içinde kullanılan, *public* kelimesi daha önce router üzerinde yaptığımız tanıma uygun olarak *snmp community* anlamına geliyor. Bu kelime router üzerinde yaptığımız tanımla aynı olmalıdır. Snmp string ile cihaz adresini @ sembolü ile ayırmalıyız. Router IP adresi de daha önce belirtildiği üzere 192.168.2.254 olacaktır. Son olarak da betiğin çıktısını bulunduğum dizinde deneme001.cfg adlı yeni dosyaya yönlendiriyorum.

Yukarda verdiğim komut ardından, betiğin bir kısım çıktıları ekranda uzun bir liste halinde görüntülendi. Bu noktada listenin birkaç satırdan oluşup kısa kalması cfgmaker betiğinin router ya da cihaza erişemediğinin belirtisi olabilir.

Kısa süren bu ilk işlemden sonra yarattığımız *deneme001.cfg* isimli dosyayı inceleyip içeriğinde neler olduğuna bakalım :

Dosyanın ilk kısmı şu şekilde olacaktır :

```
# Created by
# /usr/bin/cfgmaker public@192.168.2.254


### Global Config Options

#  for UNIX
# WorkDir: /home/http/mrtg

#  or for NT
# WorkDir: c:\mrtgdata

### Global Defaults

#  to get bits instead of bytes and graphs growing to the right
# Options[_]: growright, bits
```

İlk iki satır bu dosyanın *cfgmaker* betiği tarafından hangi parametreyle oluşturulduğunu gösteriyor ve bu alan # ile kapatılmış durumda. Buradaki bilgiler kullanılmamaktadır.

Global Config Options yazısıyla başlayan kısım, MRTG'yi kullanacağınız işletim sistemine göre daha sonra değişiklik yapmanız gerekecek olan ayarları içeriyor. Burada sadece bir tane işletim sistemi tanımlamaya izin verilmiştir. Dolayısıyla ihtiyaca göre ya UNIX ya da NT Workdir satırının başındaki # kaldırılacaktır. Ve ardından da uygun *workdir* dizini belirtlir.

Son kısımda ise grafikler oluşturulurken hangi kriterlere uyulması gerektiği belirlenebiliyor. Burada # sembolü kaldırılarak yapılacak değişiklikler oluşturulacak tüm grafiksel sayfalara uygulanacaktır. Burada kullanılabilecek seçeneklerle ilgili ayrıntılı bilgi *cfgmaker man* sayfalarından temin edilebilir.

Cfgmaker tarafından yaratılan deneme001.cfg adlı dosyanın bu kısımdan sonraki içeriği, sorguladığımız cihaza bağlı olarak çeşitlilik gösterebiliyor. Hem dosyanın çok uzun olması hem de tekrarlanan içerik yüzünden dosyanın tamamını burada incelemeyeceğim. Yalnızca cfgmaker tarafından anlamlı olarak nitelendirilen birkaç arabirim ve kullanılamayacak türde birkaç arabirime örnek vereceğim.

Cihaz sorgulaması sonucu elde edilen veriler şu şekilde görünecektir :

```
##############################################################################
# System: router
# Description: Cisco Internetwork Operating System Software
#         IOS (tm) C1700 Software (C1700-SV3Y-M), Version 12.2(1), RELEASE SOFTWARE (fc2)
#         Copyright (c) 1986-2001 by cisco Systems, Inc.
#         Compiled Fri 27-Apr-01 08:47 by cmong
# Contact:
# Location:
##############################################################################
```

Burada, Cisco Router üzerinde çalışan IOS hakkında bazı önemsiz bilgiler yer alıyor.

Hemen ardından ilk anlamlı arabirim hakkında çeşitli bilgiler verilmiştir :

```
### Interface 1 >> Descr: 'FastEthernet0' | Name: 'Fa0' | Ip: '192.168.2.254' | Eth: '00-03-6b-9a-1c-fc' ###

Target[192.168.2.254_1]: 1:public@192.168.2.254:
SetEnv[192.168.2.254_1]: MRTG_INT_IP="192.168.2.254" MRTG_INT_DESCR="FastEthernet0"
MaxBytes[192.168.2.254_1]: 12500000
Title[192.168.2.254_1]: Traffic Analysis for 1 -- router
PageTop[192.168.2.254_1]: <H1>Traffic Analysis for 1 -- router</H1>
 <TABLE>
   <TR><TD>System:</TD>     <TD>router in </TD></TR>
   <TR><TD>Maintainer:</TD> <TD></TD></TR>
   <TR><TD>Description:</TD><TD>FastEthernet0 connected to EthernetLAN </TD></TR>
   <TR><TD>ifType:</TD>     <TD>ethernetCsmacd (6)</TD></TR>
   <TR><TD>ifName:</TD>     <TD>Fa0</TD></TR>
   <TR><TD>Max Speed:</TD>  <TD>12.5 MBytes/s</TD></TR>
   <TR><TD>Ip:</TD>         <TD>192.168.2.254 ()</TD></TR>
 </TABLE>
```

İlk satır # ile başlıyor. Bunun anlamı yeni bir arabirim tanımı yapılıyor olmasıdır. Burada arabirim için kullanılabilecek çeşitli tanımlamalar (Descr, Name, Ip, Eth) görülmektedir.

MRTG, verileri inceleyip grafik haline getirmek için bundan sonraki satırları kullanacaktır. Köşeli parantez içindeki tanımlar otomatik olarak oluşturulacak web sayfalarının dosya adlarıdır. Bunlar *cfgmaker* tarafından otomatik olarak tespit edilip hazırlanmıştır. Burada ilk satırdaki Target[192.168.2.254_1] ifadesi sadece bu arabirim için geçerli bir tanımlamadır. Aynı türden başka bir arabirim olsa bile aynı isimli bir tanımlama yapılamaz. Bu satırlar :

Target[192.168.2.254_1]:1:public@192.168.2.254:
Grafiği çizilecek arabirimi ifade etmektedir. 192.168.2.254 adresli cihaz üzerindeki 1 numaralı arabirimdir.

SetEnv[192.168.2.254_1]:MRTG_INT_IP="192.168.2.254" MRTG_INT_DESC=""
Grafiklerin tepesinde yer alacak olan açıklayıcı bilgilerin içeriğini belirler.

Title[192.168.2.254_1]:Traffic Analysis for 1 – router
Otomatik olarak oluşturulacak web sayfasının başlığını ifade etmektedir.

PageTop[192.168.2.254_1]:<H1>Traffic Analysis for 1 – router </H1>
Otomatik olarak oluşturulacak web sayfasında, açıklayıcı bilgilerin üstünde görünecek başlık.

Bunun ardından ikinci anlamlı arabirim hakkında çeşitli bilgiler verilmiştir :

```
### Interface 2 >> Descr: 'Serial0' | Name: 'Se0' | Ip: '' | Eth: '' ###

Target[192.168.2.254_2]: 2:public@192.168.2.254:
SetEnv[192.168.2.254_2]: MRTG_INT_IP="" MRTG_INT_DESCR="Serial0"
MaxBytes[192.168.2.254_2]: 193000
Title[192.168.2.254_2]: Traffic Analysis for 2 -- router
PageTop[192.168.2.254_2]: <H1>Traffic Analysis for 2 -- router</H1>
 <TABLE>
   <TR><TD>System:</TD>     <TD>router in </TD></TR>
   <TR><TD>Maintainer:</TD> <TD></TD></TR>
   <TR><TD>Description:</TD><TD>Serial0  </TD></TR>
   <TR><TD>ifType:</TD>     <TD>frame-relay (32)</TD></TR>
   <TR><TD>ifName:</TD>     <TD>Se0</TD></TR>
   <TR><TD>Max Speed:</TD>  <TD>193.0 kBytes/s</TD></TR>
 </TABLE>
```

Ayrı bir grafik çizilerek görüntülenecek ikinci arabirim için diğeriyle aynı ifadeler kullanılmıştır. Bu sefer de HTML kısmıyla ilgili açıklamalar yapalım :

Otomatik olarak oluşturulacak olan web sayfaları içinde tablolamayla düzen sağlanmaktadır. Görüldüğü gibi temel HTML bilgisiyle bu alanlar kolaylıkla düzenlenebilir. Tablo içinde yer alan System, Maintainer, Description, ifType, ifName ve Max Speed ifadeleri ve karşılıkları istenildiği gibi değiştirilebilir. Ancak web sayfalarında doğru ve anlamlı bilgilerin görünmesi için bu değişiklikleri yaparken dikkatli hareket etmek gereklidir.

Cfgmaker tarafından oluşturulan ham ayar dosyası içinde yer yer karşınıza çıkabilecek bazı anlamsız arabirim tanımlamaları olabilir. Bu tanımlamalar ayar dosyasından tamamen çıkarılabilir. Bu tanımlamalar # ile kapatılmıştır. Bunlardan bazılarına örnek verelim :

```
### Interface 3 >> Descr: 'Null0' | Name: 'Nu0' | Ip: '' | Eth: '' ###
### The following interface is commented out because:
### * it is a cisco Null0 interface
```

Ölçülüp grafik çizmeye elverişli olmayan bir tanımlamadır. Bu ve devamındaki ilişkili satırlar dosyadan çıkarılabilir.

```
### Interface 5 >> Descr: 'Foreign Exchange Office 1/0' | Name: 'Foreign Exchange Office 1/0' | Ip: '' | Eth: ''
###
### The following interface is commented out because:
### * has a speed of 0 which makes no sense
```

Ölçülüp grafik çizmeye elverişli olmayan bir tanımlamadır. Çünkü bu bir FXO arabirimidir. Bu ve devamındaki ilişkili satırlar dosyadan çıkarılabilir.

Temel Ayar Dosyalarının İsteğe Göre Düzenlenmesi

Elde ettiğimiz ve içeriğini açıkladığımız temel ayar dosyalarını ihtiyaçlarımıza en uygun hale getirmeye çalışalım :

MRTG kullanarak, Cisco Router ve Kablo Modem hakkında çeşitli verileri toplamak ve bunları web sayfalarına aktarmak istiyoruz. Bunun yaparken hem Cisco Router hem de Kablo Modem için iki farklı ayar dosyası kullanmama gerek yok. Her ikisi için ayrı ayrı oluşturulan ayar dosyalarından istediğim parçaları alıp tek bir ayar dosyasında birleştirmem bu iş için yeterli olacaktır.

Diyelim ki aynı anda Cisco Router üzerindeki *Fast Ethernet* ve *Serial Line* ile Kablo Modem üzerindeki *Ethernet* arabirimi hakkında bilgi görüntülemek istiyoruz.

Linux üzerinde kurulu olan web sunucunun web sayfaları için kullanılan dizin */var/www/html* olduğuna göre, bu tanımlamaya uygun olarak ayar dosyası içine daha önce belirtildiği gibi *Workdir* ifadesini eklemeliyiz. Uygulayıcının tercihine bağlı olarak web sayfaları istenilen dizine yerleştirilebilir. Burada genel kullanımına uygun olarak /var/www/html/mrtg dizini kullanılacaktır.

Cfgmaker tarafından yaratılan temel ayar dosyalarından, isteğe göre alınan parçaların birleştirilmesiyle oluşan son ayar dosyası aşağıda görülmektedir :

Bu dosyayı *deneme003.cfg* adıyla /var/www/html/mrtg dizini altına kopyalayalım.

```
#/var/www/html/mrtg/deneme003.cfg
WorkDir: /var/www/html/mrtg

### Interface 1 >> Descr: 'FastEthernet0' | Name: 'Fa0' | Ip: '192.168.2.254' | Eth: '00-03-6b-9a-1c-fc' ###

Target[192.168.2.254_1]: 1:public@192.168.2.254:
SetEnv[192.168.2.254_1]: MRTG_INT_IP="192.168.2.254" MRTG_INT_DESCR="FastEthernet0"
MaxBytes[192.168.2.254_1]: 12500000
Title[192.168.2.254_1]: WAN Router için Trafik Analizi - Fastethernet
PageTop[192.168.2.254_1]: <H1>Cisco WAN Router için Trafik Analizi</H1>
 <TABLE>
   <TR><TD>System:</TD>     <TD>router in Ankara</TD></TR>
   <TR><TD>Maintainer:</TD> <TD><a href="mailto:celak@ttnet.net.tr">Celal UNALP</a></TD></TR>
   <TR><TD>Description:</TD><TD>FastEthernet0 connected to EthernetLAN </TD></TR>
   <TR><TD>ifType:</TD>     <TD>ethernetCsmacd (6)</TD></TR>
   <TR><TD>ifName:</TD>     <TD>Fa0</TD></TR>
   <TR><TD>Max Speed:</TD>  <TD>12.5 MBytes/s</TD></TR>
   <TR><TD>Ip:</TD>         <TD>192.168.2.254 ()</TD></TR>
 </TABLE>


### Interface 2 >> Descr: 'Serial0' | Name: 'Se0' | Ip: '' | Eth: '' ###

Target[192.168.2.254_2]: 2:public@192.168.2.254:
Options[192.168.2.254_2]: bits
SetEnv[192.168.2.254_2]: MRTG_INT_IP="" MRTG_INT_DESCR="Serial0"
MaxBytes[192.168.2.254_2]: 193000
Title[192.168.2.254_2]: WAN Router için Trafik Analizi - Serial
PageTop[192.168.2.254_2]: <H1>Cisco WAN Router için Trafik Analizi</H1>
 <TABLE>
   <TR><TD>System:</TD>     <TD>router in Ankara</TD></TR>
   <TR><TD>Maintainer:</TD> <TD><a href="mailto:celak@ttnet.net.tr">Celal UNALP</a></TD></TR>
   <TR><TD>Description:</TD><TD>Serial0  </TD></TR>
   <TR><TD>ifType:</TD>     <TD>frame-relay (32)</TD></TR>
   <TR><TD>ifName:</TD>     <TD>Se0</TD></TR>
   <TR><TD>Max Speed:</TD>  <TD>193.0 kBytes/s</TD></TR>
 </TABLE>


### Interface 1 >> Descr: 'Ethernet MAC: Crystal LAN CS89000' | Name: 'cs0' | Ip: '192.168.100.1'| Eth: '00-20-40-62-31-6b' ###

Target[192.168.100.1_1]: 1:public@192.168.100.1:
SetEnv[192.168.100.1_1]: MRTG_INT_IP="192.168.100.1" MRTG_INT_DESCR="Ethernet MAC: Crystal"
MaxBytes[192.168.100.1_1]: 1250000
Title[192.168.100.1_1]: SB3100 Kablo Modem için Trafik Analizi
PageTop[192.168.100.1_1]: <H1>SB3100 Kablo Modem Trafik Analizi</H1>
 <TABLE>
   <TR><TD>System:</TD>     <TD>SB3100 in Ankara</TD></TR>
   <TR><TD>Maintainer:</TD> <TD><a href="mailto:celak@ttnet.net.tr">Celal UNALP</a></TD></TR>
   <TR><TD>Description:</TD><TD>Ethernet MAC: Crystal LAN CS89000  </TD></TR>
   <TR><TD>ifType:</TD>     <TD>ethernetCsmacd (6)</TD></TR>
   <TR><TD>ifName:</TD>     <TD>cs0</TD></TR>
   <TR><TD>Max Speed:</TD>  <TD>1250.0 kBytes/s</TD></TR>
   <TR><TD>Ip:</TD>         <TD>192.168.100.1 ()</TD></TR>
 </TABLE>
```

Son Ayar Dosyası ile MRTG'nin Çalıştırılması

İsteklerimize göre düzenlediğimiz ayar dosyasını, çalışacağı konuma aldıktan sonra ilk defa çalıştırmayı deniyoruz :

```
[root@camel /var/www/html/mrtg]# mrtg deneme003.cfg
```

Bu komutu verdikten sonra bazı hata mesajları gelecektir. Kayıt dosyalarının ilk defa yaratılması sırasında oluşan bu hatalar komutun arka arkaya birkaç defa verilmesi ile ortadan kalkacaktır.

- Üzerinde çalıştığımız ayar dosyası bir şablon olarak düşünülmelidir. Bu dosya bir defaya mahsus olarak oluşturulur ve özenle düzenlenir. Bundan sonra MRTG, her çalıştırıldığında bu dosyada belirlenen kriterlere göre cihazları sorgular ve istenen verileri çeşitli dosyalar halinde hazırlar.

Komut çalıştırıldıktan sonra bulunduğumuz dizinde, amacımıza çok yaklaştığımızı gösteren bazı dosyalar oluşacaktır. Bu dosyalardan bir kısmının açıklamasını yaparsak :

192.168.2.254_1.html

Bu dosya izlemek istediğimiz Cisco Router cihazının ilk arabirimi olan FastEthernet için otomatik olarak oluşturulan HTML dosyasıdır. Yukardaki komut her çalıştırıldığında bu dosya yeniden oluşturulur.

192.168.2.254_1.log

Bu dosya, daha önce de açıklandığı gibi boyutu sabit kalan ve bu arabirimle ilgili bilgileri saklayan kayıt dosyasıdır. Yukardaki komut her çalıştırıldığında yeniden düzenlenir.

192.168.2.254_1-day.png

Bu dosya, izlenen arabirimin web sayfasında görüntülenecek anlık veri grafiklerini içermektedir. Yukardaki komut her çalıştırıldığında yeniden oluşturulur.

192.168.2.254_1-week.png

Bu dosya, izlenen arabirimin web sayfasında görüntülenecek haftalık veri grafiklerini içerir.

192.168.2.254_1-month.png

Bu dosya, izlenen arabirimin web sayfasında görüntülenecek aylık veri grafiklerini içerir.

192.168.2.254_1-year.png

Bu dosya, izlenen arabirimin web sayfasında görüntülenecek yıllık veri grafiklerini içerir.

MRTG'nin Rutin Olarak Çalıştırılması

MRTG'nin düzenli aralıklarla çalıştırılması için, *cron* sisteminden faydalanacağız. Genel kabul görmüş bir ilke olarak MRTG'nin cron tarafından her 5 dakikada bir çalıştırılması uygun olacaktır.

- Burada dikkat edilmesi gereken bir nokta daha gündeme gelmektedir. Linux işletim sistemi tarafından kullanılan sistem zamanı doğru olmalıdır. Grafiklerin içeriği her ne kadar doğru olsa bile, gösterdiği zaman yanlış ise bir anlam ifade etmeyecektir. Dolayısıyla sistem saatini düzenli aralıklarla kontrol etmekte fayda vardır.

Cron sistemine MRTG ile ilgili komutun girilmesi için verilecek komut :

```
[root@camel /var/www/html/mrtg]# crontab –e
```

Cron sistemine eklenecek satır ise :

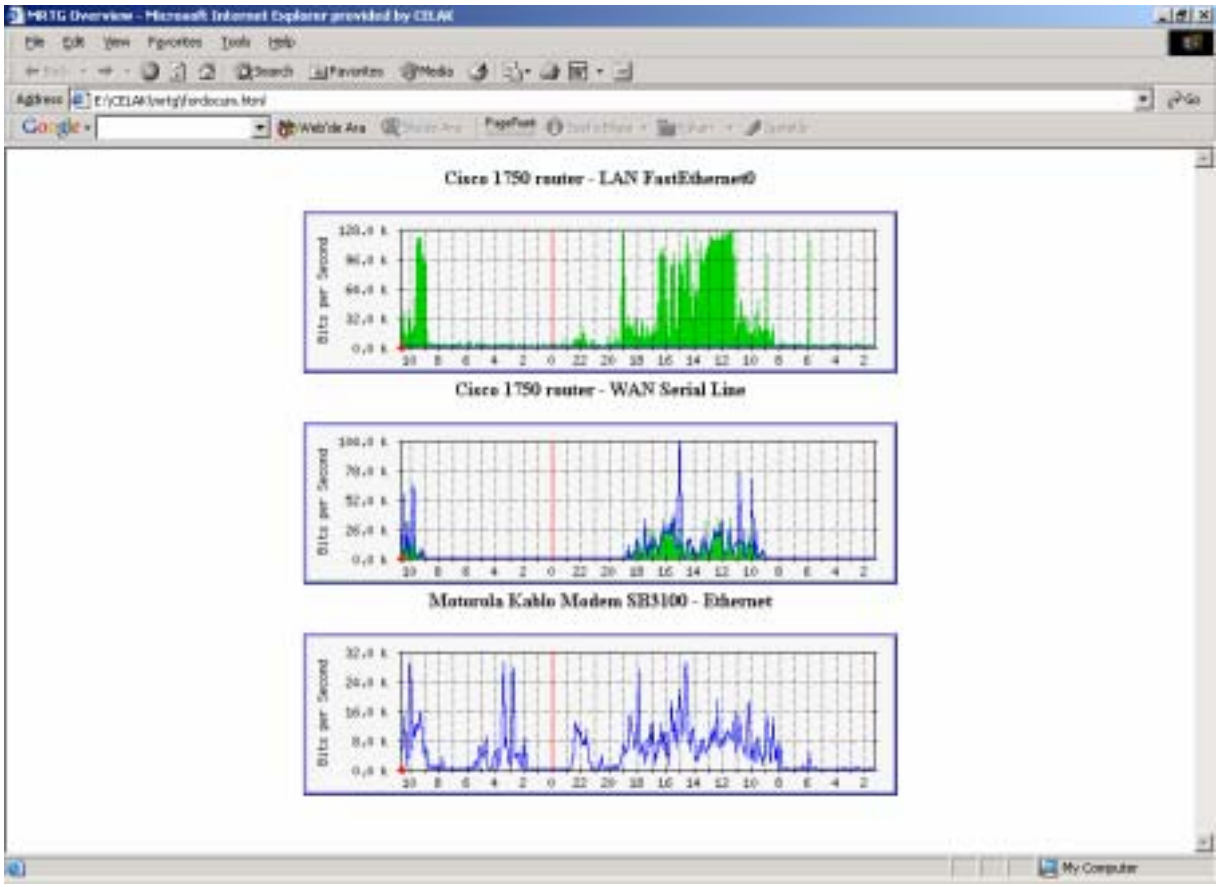
```
*/5 * * * * /usr/bin/mrtg /var/www/html/mrtg/deneme003.cfg >/dev/null 2>&1
```

Bu kayda göre, MRTG her 5 dakikada bir hazırladığımız ayar dosyasını esas alarak cihazları sorgulayacak ve grafikleri yeni verilerle güncelleyecektir.

MRTG Web Sayfasının Görünümü

Yaptığımız tüm işlemler sonunda, bir dizin içinde sürekli güncellenen HTML sayfaları elde etmiş oluyoruz. Kimilerine göre bu aşama yeterli olabilir. Ancak dizindeki tüm dosyaların web üzerinden görülebilmesi her zaman uygun olmayabilir. Bu amaçla */var/www/html/mrtg* dizini için bir *index.html* sayfası hazırlamak uygun olacaktır. Aşağıda verdiğim örnek, uzun zamandan bu yana bir çok web sitesinde mrtg giriş sayfası olarak kullanılmaktadır.

```
<html>
<HEAD>
   <TITLE>MRTG Overview</TITLE>
   <META HTTP-EQUIV="Refresh" CONTENT="300">
   <META HTTP-EQUIV="Cache-Control" content="no-cache">
   <META HTTP-EQUIV="Pragma" CONTENT="no-cache">
</HEAD>
<body>
<div align=center>
<B>Cisco 1750 router - LAN FastEthernet0</B>
<P><A HREF="192.168.2.254_1.html"><IMG BORDER=1 SRC="192.168.2.254_1-day.png"></A>
<BR>
<B>Cisco 1750 router - WAN Serial Line</B>
<P><A HREF="192.168.2.254_2.html"><IMG BORDER=1 SRC="192.168.2.254_2-day.png"></A>
<BR>
<B>Motorola Kablo Modem SB3100 - Ethernet</B>
<P><A HREF="192.168.100.1_1.html"><IMG BORDER=1 SRC="192.168.100.1_1-day.png"></A>
<BR>
</body>
</html>
```



Şekil-2 Basit ve kullanışlı bir MRTG giriş sayfası

MRTG Web Sayfasının Güvenliği

Uygulayıcının ihtiyaçları doğrultusunda, MRTG istatistikleri sadece ilgili kişilerin görebileceği şekilde güvenlik altına alınabilir. Bu konuda Red Hat Linux işletim sistemi üzerinde standart olarak kullanılan Apache Web sunucusundan faydalanabiliriz.

Akla gelen ilk şey, *httpd.conf* içinde gerekli (*AuthConf*) değişiklikleri yapmak. Bundan sonra */var/www/security* dizini yaratılmalı ve bu konumda bir parola dosyası oluşturulmalıdır:

```
[root@camel /var/www/security]# htpasswd –c mrtg.passwd celak
```

Parola dosyası hazırlandıktan sonra */var/www/html/mrtg* dizini altında *.htaccess* dosyası oluşturulmalıdır. Bu dosyada yapılan tanımlamalara göre, yalnızca bir kullanıcı adı ve parolası olanlar bu dizinin içeriğini web üzerinden görebilecektir :

```
AuthType Basic
        AuthName "Ağ Bağlantı İstatistikleri"
        AuthUserFile /var/www/security/mrtg.passwd
        require valid-user
```

İnternet Web Adresleri :

http://people.ee.ethz.ch/~oetiker/webtools/mrtg - MRTG Resmi Web Sitesi

http://www.somix.com/support/mrtg_repository.php - Örnek MRTG Şemaları

http://www.perl.com – Perl Web Sitesi

http://www.perl.org – Perl Web Sitesi

http://www.cpan.org – Perl Arşiv Web Sitesi

http://www.redhat.com – Red Hat Linux Resmi Web Sitesi

http://www.linux.org.tr – Özgür Yazılım, Özgür Gelecek

http://www.belgeler.org – Linux Belgelendirme Çalışma Grubu Web Sitesi

http://www.apache.org – Apache Web Sunucusu Resmi Web Sitesi

http://www.gnu.org/copyleft/gpl.html - GNU General Public License

MRTG MULTI ROUTER TRAFFIC GRAPHER

Tobias Oetiker : oetiker@ee.ethz.ch
Dave Rand : dlr@bungi.com

Yasal Açıklamalar

Belge Telif Hakkı ve Lisans

Feragatname