SNMP & MRTG

Metin KAYA

EnderUNIX Yazılım Geliştiricisi

Endersys Sistem Mühendisi

metin at enderunix.org

metin.kaya at endersys.com.tr

http://www.enderunix.org

http://www.endersys.com.tr

23 Tem 2007 Pazartesi EEST 23:47:19

İçindekiler

Sn. İsmail YENİGÜL 'e teşekkürler…

1. Giriş

Bu makalede SNMP (Simple Network Management Protocol) ‘den bahsedilip Red Hat türevi Linux sistemlere (Fedora Core 4 ve üzeri, CentOS 4 ve üzeri esas alınmıştır) SNMP ve MRTG (Multi-Router Traffic Grapher) kurulumu, yapılandırması anlatılacaktır. MRTG, SNMP üzerine geliştirilmiş bir yazılım olduğundan ve kurulum-yönetim sürecinde karşılaşılan sorunların birçoğu SNMP kaynaklı olduğundan öncelikle SNMP hakkında bilgi verilecektir.

2. SNMP

2.1 SNMP Nedir?

Çok büyük ağlarda meydana gelen sorunların tespiti, giderilmesi ve bu ağdaki aygıtların gözetlenmesi gerekir. Bu ihtiyacı karşılamak amacıyla ağ yönetim protokolleri geliştirilmiştir.

SNMP, TCP/IP üzerine geliştirilmiş bir protokoldür; ancak IPX, AppleTalk ve OSI desteği de mevcuttur.

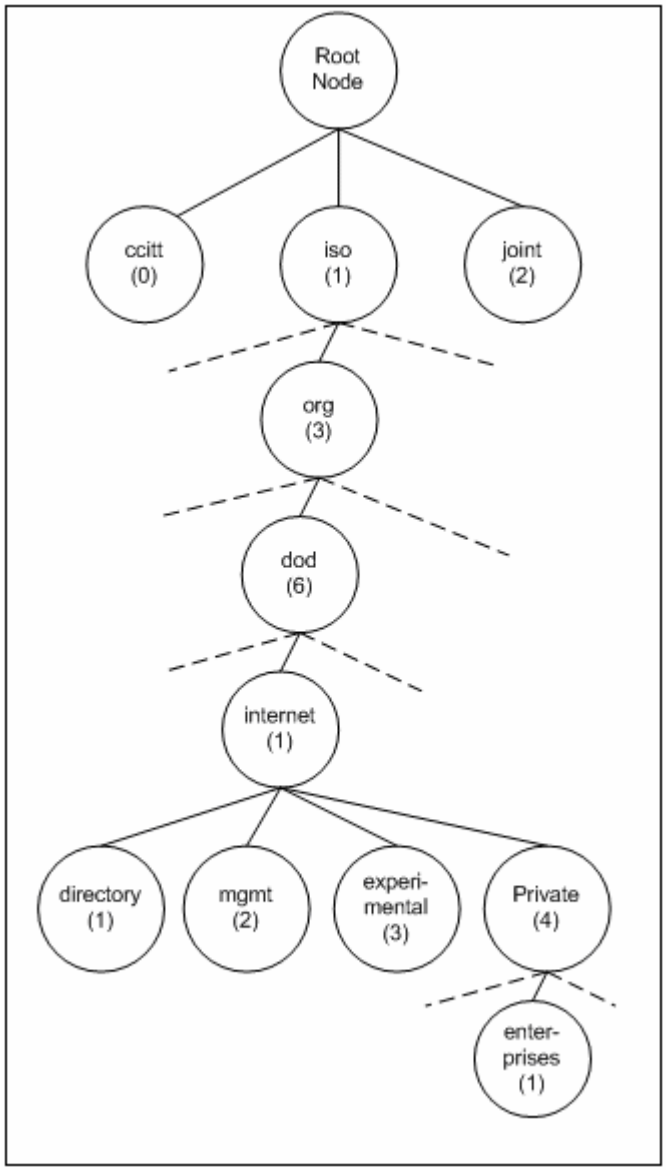
Ağ yönetim merkezi olarak kullanılan makine üzerinde istemci program (management client), denetlenen makineler üzerinde de yönetim merkezinin istemcisinin sorgularına yanıt veren sunucu yazılımlar (management agent) çalışır. İstemci ile sunucu arasındaki iletişim 2 şekilde olabilir: istemci, sunucudan özel bir değişkenin değerini isteyebilir (Örneğin; kaç tane ICMP port erişilemiyor hatası üretildi?) veya sunucu, istemciye önemli bir olayın varlığını haber verir (Örneğin; bir arayüzün devre dışı kalması). Bunlara ek olarak istemci, sunucudaki herhangi bir değişkenin değerini değiştirebilir (Örneğin; ön tanımlı IP TTL değerini 64 olarak değiştir).

TCP/IP ağ yönetimi 3 kısımdan oluşur:

1. **MIB** (Management Information Base): Yönetilecek ağ değişkenlerini saklar. Bu değişkenler istemci tarafından değiştirilebildiği gibi üzerinde sorgu da çalıştırılabilir. RFC 1213 ile MIB-II standardı tanımlanmıştır. MIB içeriği donanım üreticileri tarafından oluşturulur ve dünyada tekildir (her donanım üreticisinin SMI ağacındaki yeri farklıdır).
2. **SMI** (Structure of Management Information): MIB ‘deki değişkenlere referans olan yapılar ve kimliklerden oluşan kümedir. Örneğin; *Counter,* 0 ‘dan başlayıp 4294967295 ‘e kadar ilerledikten sonra tekrar 0 olan değişkendir. SMI, RFC 1155 ‘te tanımlanmıştır.
3. **SNMP**: İstemci ile sunucu arasındaki iletişim protokolüdür. RFC 1157 ‘de tanımlanmıştır. İletişimde UDP paketleri ve ön tanımlı olarak 161. port kullanılır.

Sunucuların, güvenlik duvarlarının ve yönlendiricilerin (router) işlemsel istatistiklerini tuttukları OID (Object Identifier) ‘ler SNMP standardında belirtilen bilgi ağacında (SMI) belirtildiği şekilde düzenlenmiştir. Bilgi ağacı bir kök düğümünden başlayıp dallara, yapraklara doğru ilerler. Ağaçtaki adres yolu oluşturulurken her düğümden sonra bir nokta yazılır.

Örneğin; *enterprises* için adres yolu *1.3.6.1.4.1* 'dir. MIB 'ler her bir OID dalının metin halinde ifade edilmesidir. Aşağıdaki şekilde bir OID yapısı görülmektedir:



Şekil 1: OID Yapısı (SMI Bilgi Ağacı)

Örneğin, *1.3.6.1.2.1.7.9.109.1.1.1.1.5* adres yolunu *udp.9.109.1.1.1.1.5* olarak da yazabilirsiniz. Çünkü çok sık kullanılan adres yollarının bazılarına takma adlar (alias) oluşturulmuştur. Bu takma adlardan bazıları aşağıda görülmektedir:

MIB	OID
1.3	org
1.3.6	dod
1.3.6.1	Internet
1.3.6.1.1	directory
1.3.6.1.2	mgmt
1.3.6.1.3	experimental
1.3.6.1.4	private
1.3.6.1.4.1	enterprises
1.3.6.1.2.1	MIB
1.3.6.1.2.1.4	IP
1.3.6.1.2.1.5	ICMP
1.3.6.1.2.1.6	TCP
1.3.6.1.2.1.7	UDP

Şekil 2: Sık Kullanılan Bazı OID 'lerin MIB Karşılıkları

SMI ağacındaki sadece yapraklar anlamlı ve **okunabilir** veri içerir. Bu ağaçtaki yaprak harici düğümler bir diskteki dizinlere, yapraklar da anlamlı veri içeren dosyalara benzetilebilir.

Şu an 3 tane SNMP sürümü bulunmaktadır:

SNMP sürüm 1: SNMP 'nin ilk protokolüdür. Sistem kaynaklarını fazla kullanmadan aygıt istatistikleri ve hata raporlama amaçlıdır. Veri iletişimi şifreli değildir. Okuma/yazma için sadece SNMP istemcisinin IP adresine erişim izni verilmiştir.

SNMP sürüm 2: Bu sürüm 1. sürümle uyumlu olup 1. sürüme çok daha detaylı hata raporlama ve aygıt bilgisi elde etme özelliği eklemiştir.

SNMP sürüm 3: Önceki sürümlerin güvenliği artırılıp uzaktan yönetilebilme özellikleri eklenmiştir. Sadece bir IP adresine değil birden fazla IP kümesine ve SNMP kullanıcılarına okuma/yazma izni verilebilir. Veri iletişimi şifreli olup bu iletişim esnasında oluşan hataları sezme özelliği geliştirilmiştir.

SNMP sürümleri arasındaki farkları bilmeniz SNMP sorguları yaparken lazım olacağından tavsiye edilir.

2.2 SNMP Kurulumu ve Yapılandırması

Aşağıdaki komutla SNMP için gerekli tüm paketler sisteminize kurulur:

```
# yum -y install net-snmp net-snmp-utils net-snmp-devel
```

Bu komuttan sonra */etc/snmp/snmpd.conf* dosyasını düzenlemeniz gerekmektedir (*/var/net-snmp/snmpd.conf* ve */var/net-snmp/snmptrapd.conf* dosyalarını kesinlikle **düzenlemeyiniz**). Bu yapılandırma dosyası ve *snmpd* servisinin çalışması ile ilgili detaylı bilgileri *man 5 snmpd.conf* komutunun çıktısında bulabileceğinizi belirtip bu dosyaya ilişkin bazı açıklamalar yapalım:

- *snmpd.conf* dosyasında # karakteri ile başlayan satırlar açıklama satırları olup *snmpd* servisinin çalışmasına hiçbir etkileri yoktur.

- *# sec.name source community* satırından sonra gelip *com2sec* ile başlayan satırlar sisteminizde SNMP sorguları çalıştırmasına izin verdiğiniz IP adresleri ve makine adlarını belirtir. Ayrıca bu makinelerin SNMP erişim şekilleri (public, private) de burada tanımlanır. SNMP sorunlarının bir kısmı SNMP sorgusu çalıştırması beklenen makinelere bu alanda gerekli erişim izninin verilmemiş olmasının kaynaklanır. Aşağıda örnek *com2sec* satırları görülmektedir:

```
#       sec.name     source          community
com2sec local        localhost       public
com2sec mynetwork    127.0.0.1/32    public
com2sec mynetwork    10.0.0.0/24     private
com2sec user_access  10.0.0.209/32   ulas
```

  com2sec ile başlayan 1. satırda üzerine SNMP kurulmuş makinenin kendisi üzerinde SNMP sorguları çalıştırmasına izin verilmiştir. *sec.name* ile belirtilen alan *security name* 'in kısaltması olup bu alana yazdığınız ismin hiçbir önemi yoktur. *com2sec* ile başlayan 2. satır 1. satır ile aynı işleve sahiptir. *com2sec* ile başlayan 3. satırda ise sadece 10.0.0. ile başlayan IP adreslerinin makinemizde SNMP sorguları çalıştırmasına izin verilmiştir. 10.0.0.0/24 ile 10.0.0. ile başlayan IP adreslerinin tamamına izin verilmiştir. Örneğin; sadece 10.0.0.207 IP adresine izin verilecekse 10.0.0.207/32, 10. ile başlayan tüm IP adreslerine izin verilecekse 10.0.0.0/8 ve 10.0. ile başlayan tüm IP adreslerine izin verilecekse 10.0.0.0/16 yazılmalıdır. Son *com2sec* satırında *ulas* **SNMP kullanıcısının** sadece 10.0.0.209 IP adresinden sistemimize erişmesine izin verilmiştir. SNMP kullanıcısının nasıl oluşturulacağı bu kısımda açıklanacaktır.

- Güvenlik isimleriyle (security name) grup adları eşleştirilip güvenlik isimlerine uygun SNMP erişim izinleri verilmelidir. Bunun için *# sec.model sec.name* satırından sonraki *group* ile başlayan satırlar düzenlenmelidir.

```
#                  sec.model  sec.name
group MyRWGroup    v1         local
group MyRWGroup    v2c        local
group MyRWGroup    usm        local
group MyROGroup    v1         mynetwork
group MyROGroup    v2c        mynetwork
group MyROGroup    usm        mynetwork
group MyRWGroup    v1         user_access
group MyRWGroup    v2c        user_access
group MyRWGroup    usm        user_access
```

group kelimesinden sonra gelen *MyROGroup, MyRWGroup* gibi sözcükler grup adı olup istenen herhangi bir isim atanabilir. *sec.model* (security model) alanında belirtilen *v1*, *v2*, *usm* ise güvenlik isimlerinin ne tür SNMP erişimi yapacağını belirler (SNMP sürüm 1 için *v1*, SNMP sürüm 2 için *v2*, SNMP sürüm 3 için *usm*). Yukarıdaki yapılandırmayla tüm güvenlik isimlerine tüm SNMP sürümleri için erişim izni verilmiştir. Buradaki *sec.name* 'lerin bir önceki maddede anlatılan kısımda tanımlanmış olması gerekir.

- Gruplara erişim izni verilmelidir. *# context sec.model sec.level match read write notif* satırından sonraki *access* ile başlayan satırlar düzenlenmelidir:

```
#               context  sec.model  sec.level   match   read  write   notif
access MyROGroup   ""       any       noauth     exact    all   none    none
access MyRWGroup   ""       any       noauth     exact    all   all     none
```

Yukarıdaki yapılandırmayla *MyROGroup* grubuna sadece yazma, *MyRWGroup* grubuna ise hem okuma hem de yazma izni verilmiştir.

- Yapılandırma dosyasının sonlarında yer alan *syslocation* ve *syscontact* satırlarını aşağıdaki gibi düzenlemeniz ilerde oluşturacağınız MRTG grafiklerinizin de anlam kazanmasını sağlar:

```
syslocation Endersys Head Office, Istanbul
syscontact  Metin KAYA <metin.kaya@endersys.com.tr>
```

Yapılandırma işlemi sona erdiğine göre *snmpd* ve *snmptrapd* (SNMP mesajlarını alıp bilgi kayıtlarını tutan servistir. Ön tanımlı olarak UDP 162. portu kullanır. Ayrıntılı bilgi için: *man 8 snmptrapd*) servislerini başlatabiliriz:

```
# /etc/init.d/snmpd start
# /etc/init.d/snmptrapd start
```

Bu servislerin her açılışta otomatik olarak başlatılması için aşağıdaki komut verilmelidir:

```
# chkconfig snmpd on
# chkconfig snmptrapd on
```

NOT: */etc/init.d/snmpd.conf* dosyasında yapılan değişikliklerin etkinleşmesi için sadece *snmpd* servisinin yeniden başlatılması yeterlidir:

```
# service snmpd restart
```

2.3 SNMP Kullanıcısı Oluşturma

SNMP kullanıcısı oluşturulmadan önce *snmpd* servisi çalışıyorsa *service snmpd stop* veya */etc/init.d/snmpd stop* ile durdurulmalıdır. Aşağıdaki komutla kullanıcı adı *ulas*, parolası *sifre123*, parolası MD5 algoritmasıyla şifrelenecek olan, sistem MIB 'lerini sadece okumasına (-ro) izin verilen ve SNMP sürüm 3 kullanacak SNMP kullanıcısı oluşturulur:

```
# net-snmp-config --create-snmpv3-user -ro -a MD5 -A sifre123 ulas
```

-ro seçeneği kullanılmazsa kullanıcıya ön tanımlı olarak MIB 'leri hem okuma hem de değiştirme (read-write) izni verilmiş olur. SNMP kullanıcılarıyla yapılan bilgi alış verişinin şifreli gerçekleşmesini istiyorsanız yukarıdaki komutu şöyle kullanabilirsiniz:

```
# net-snmp-config --create-snmpv3-user -a MD5 -A sifre123 –x –DES –X
veri_sifresi ulas
```

Yukarıdaki komutla MIB 'leri hem okuma hem de yazma izni olan *ulas* kullanıcısının MD5 ile şifrelenmiş SNMP erişim parolası *sifre123*, SNMP verilerinin parolası DES algoritmasıyla şifrelenmiş olup *veri_sifresi* 'dir.

NOT*: snmpd* servisi çalışırken *snmpusm* komutuyla sisteme SNMP sürüm 3 kullanıcısı eklenebilir, kullanıcıların şifreleri değiştirilebilir. Detaylı bilgi için: *man 1 snmpusm.*

2.4 SNMP Sorguları

Öncelikle şunu belirtmeliyiz ki: *snmpget* komutunun çıktısı sadece belirtilen yaprağa ait verilerdir; *snmpwalk* komutununki ise belirtilen dalın altındaki tüm yapraklara ait verilerdir. Bu komutların alabileceği parametreler ve seçenekler hakkında ayrıntılı bilgi için: *man 1 snmpcmd*

Sorguların basit yazım şekli şöyledir:

```
# [snmpwalk || snmpget] –v sürüm_numarası –c kullanıcı_adı \
[hedef_aygıtın_makine_adı || hedef_aygıtın_IP_adresi] hedef_MIB
```

Aşağıdaki komutlarla *interface* ve *system* MIB 'leri hakkında bilgi alınabilir (komut çıktıları aşağıdakine benzer şekildeyse SNMP okuma işlemi yapabiliyorsunuz demektir):

```
# snmpwalk -v 1 -c public localhost interface

...

IF-MIB::ifNumber.0 = INTEGER: 4
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifIndex.4 = INTEGER: 4
IF-MIB::ifIndex.6 = INTEGER: 6
IF-MIB::ifDescr.1 = STRING: venet0
IF-MIB::ifDescr.2 = STRING: lo
IF-MIB::ifDescr.4 = STRING: eth0
IF-MIB::ifDescr.6 = STRING: sit0

...

IF-MIB::ifPhysAddress.1 = STRING:
IF-MIB::ifPhysAddress.2 = STRING:
IF-MIB::ifPhysAddress.4 = STRING: 0:c:29:aa:16:c2
IF-MIB::ifPhysAddress.6 = STRING:

...
```

```
# snmpwalk -v 1 -c public localhost system
SNMPv2-MIB::sysDescr.0 = STRING: Linux enderunix.org 2.6.18-
8.1.4.el5.028stab035.1 #1 SMP Sat Jun 9 01:43:20 MSD 2007 i686
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
SNMPv2-MIB::sysUpTime.0 = Timeticks: (775137) 2:09:11.37
SNMPv2-MIB::sysContact.0 = STRING: Metin KAYA metin.kaya@endersys.com.tr
SNMPv2-MIB::sysName.0 = STRING: enderunix.org
SNMPv2-MIB::sysLocation.0 = STRING: Endersys Head Office, Istanbul
...
```

İlk komutun çıktısındaki *IF-MIB::ifPhysAddress.4 = STRING:* satırında okunan değer MAC adresidir. Eğer sadece MAC adresini öğrenmek istiyorsanız aşağıdaki komutu vermelisiniz:

```
# snmpget -v 1 -c public localhost ifPhysAddress.4
IF-MIB::ifPhysAddress.4 = STRING: 0:c:29:aa:16:c2
```

Bu MAC adresinin doğru olup olmadığını aşağıdaki komutla öğrenebilirsiniz:

```
# ifconfig -a | grep eth0 | awk '{print $5}'
00:0C:29:AA:16:C2
```

Aşağıdaki komutla *ulas* SNMP kullanıcısı ile 10.0.0.207 IP adresli makinede sorgu çalıştırılmıştır (Bu kullanıcının parolası MD5 ile şifrelenmiş olup *sifre123* 'tür. *authPriv* seçeneği ile veri transferinin şifreli olması sağlanmıştır.):

```
# snmpget -v 3 -u ulas -l authPriv -a MD5 -A sifre123 10.0.0.207 SNMPv2-MIB::sysORDescr.8
SNMPv2-MIB::sysORDescr.8 = STRING: The management information definitions for the SNMP User-based Security Model.
```

NOT*:* Farklı bir makinede SNMP sorguları çalıştıracaksanız bu ağda SNMP izlemeye izin verilmiş olması gerekir. Örneğin; aynı ağda bulunduğunuz farklı bir makinede SNMP sorguları çalıştırabilmeniz için modemden SNMP izlemeye izin vermiş olmanız gerekir. İzin tipinin *private* olması ağınızın dışındaki makinelerin sizin ağınızda SNMP sorguları çalıştırmasını engeller.

snmpset komutu ile istenen OID 'lerin değeri değiştirilebilir. Komut yazımı şöyledir:

```
# snmpset genel_seçenekler oid tip değer [oid tip değer …]
```

tip değişkeni *s (STRING), u (UNSIGNED), b (BIT), i (INTEGER), x (HEX STRING), d (DECIMAL STRING), n (NULLOBJ), o (OBJID), t (TIMETICKS)* ve *a (IPADDRESS)* olabilir.

Aşağıdaki komutla *sysLocation.0* değişkeninin değeri STRING tipinde "Endersys Mersin Ofisi" ve *ifIndex.1* değişkeninin değeri INTEGER tipinde 9 olarak değiştirilecektir:

```
# snmpset –c private –v 1 localhost system.sysLocation.0 s "Endersys Mersin Ofisi" interface.ifIndex.1 = 9
```

2.5 SNMP Sorunları

SNMP sorunlarına karşılık aşağıdaki çözüm zinciri önerilebilir:

- *snmpd* ve *snmptrapd* servislerinin çalıştığından emin olunuz (*service snmpd status* ve *service snmptrapd status*).
- */etc/snmp/snmpd.conf* dosyasında yapılan değişikliklerin *snmpd* servisi yeniden başlatılınca etkinleşeceğini hatırlayınız.
- SNMP istemcisi ile sunucusu arasında iletişimi engelleyen bir güvenlik duvarı veya */etc/hosts.deny* ve */etc/hosts.allow* dosyalarında herhangi bir sorun olmamalıdır.
- Ağınızda SNMP izlemeye izin verilmiş olmalıdır.
- SNMP sürümünüzün doğru olması gerekir.

- SNMP sorgusu çalıştırılacak hedef makinenin IP adresini kontrol ediniz.
- */var/log/messages* ve */var/log/snmpd.log* dosyalarındaki hata mesajlarını dikkatle okuyunuz.

/etc/snmp/snmpd.conf dosyasındaki düzenlemelerin bu makalenin 2.2 bölümüne göre yapılması durumunda herhangi bir sorunla karşılaşılması beklenmemektedir.

3. MRTG

3.1 MRTG Nedir?

MRTG ağ bağlantılarındaki trafik yükünü izlemeye yarayan bir araçtır. MRTG, ağ bağlantılarındaki trafiğin **canlı** olarak izlenmesine olanak veren grafikler (PNG biçiminde) içeren HTML sayfaları oluşturur. MRTG, Perl ve C programlama dillerini kullanarak çalışır. UNIX ve Windows işletim sistemleri altında çalışabilir ve açık kodludur. GNU GPL kapsamında ücretsiz temin edilebilir.

MRTG, SNMP aracılığıyla istenen OID değeri hakkında istatistiksel veri toplayan Perl betikleri ve bu verilerden anlamlı grafikler çizebilen C kodundan oluşmaktadır. Grafikler GD kütüphanesi kullanılarak oluşturulur. MRTG tarafından oluşturulan HTML sayfaları Mozilla Firefox, Internet Explorer ve Opera gibi web tarayıcıları tarafından görüntülenebilir.

MRTG son 2 yıla ilişkin kayıtları sorunsuzca saklayabilmektedir.

3.2 MRTG Kurulumu ve Yapılandırması

Aşağıdaki komutla MRTG için gerekli paketler sisteminize kurulacaktır:

```
# yum -y install mrtg
```

Şimdi MRTG araçlarından *cfgmaker* ile yapılandırma dosyamızı oluşturalım:

```
# cfgmaker --global 'WorkDir: /var/www/mrtg'     \
           --global 'Options[_]: bits,growright' \
           --output /etc/mrtg/mrtg.cfg           \
             public@localhost
```

Yukarıdaki komutun ilk satırında MRTG ‘nin web sayfası oluşturmak için kullandığı dosyaların bulunacağı dizin belirtilir. 2. satırdaki *bits* seçeneği ile grafiklerde byte türünde değerler varsa bunların bit cinsinden ifade edilmesi, *growright* seçeneğiyle de grafiğin sağa doğru ilerlemesi (en güncel değer en sağda olacak şekilde) sağlanır. 3. satırda ise bu komutun ardından oluşturulacak yapılandırma dosyasının kaydedileceği dizin belirtilir (dosyanın adı mrtg.cfg ‘dir). Son satırda ise bu yapılandırma dosyasının hangi kullanıcı ve makine için oluşturulduğu gösterilir. Buraya *ulas@10.0.0.207*

(kullanıcı@hostname) gibi bir satır da yazılabilirdi. Hangi makine MRTG ile izlenecekse *hostname* kısmına o makinenin adı veya IP adresi yazılmalıdır. Ayrıca MRTG ile izlenecek makinede SNMP kurulmuş olmalıdır. Bu ağda SNMP izlemeye izin verilmiş olması da gerekir.

Veri transferinin bir doğrulama mekanizmasıyla şifrelenmiş olarak gerçekleşmesini istiyorsanız MRTG yapılandırma dosyasını şu komutla oluşturmalısınız (verilerin şifrelenmesini istemiyorsanız *privpassword* ve *privprotocol* seçeneklerini kullanmanıza gerek yoktur):

```
# cfgmaker --global 'WorkDir: /var/www/mrtg'     \
           --global 'Options[_]: bits,growright' \
           --output /etc/mrtg/mrtg.cfg           \
           --enablesnmpv3 --username=ulas --authpassword=sifre123         \
           --authproto=md5 --privpassword=veri_sifresi --privprotocol=des \
           ulas@10.0.0.207
```

Burada dikkat etmeniz gereken konu ise yukarıdaki satırda yazdığınız SNMP kullanıcısı ve parola bilgilerinin makalenin 2.3 bölümünde yaptığınız ayarlarla uyuşması gerektiğidir. Yani SNMP kullanıcısı *ulas*, parolası *sifre123*, veri transfer parolası *veri_sifresi* 'dir. Ayrıca kullanıcının parolasını MD5 ile veri transferi parolasını da DES algoritmasıyla şifreliyoruz. Bu verilerle makalenin 2.3 bölümündekiler tutarlı olmalıdır. Bu güvenlik desteklerini kullanabilmeniz için SNMP sürüm 3 'ün sisteminizde kurulu olması gerekir.

cfgmaker komutunu başarıyla çalıştırdıktan sonra */etc/mrtg/mrtg.cfg* yapılandırma dosyasını açıp herhangi bir sorun olup olmadığını kontrol ediniz. Sorunlu kısımların çoğunda */etc/snmp/snmpd.conf* dosyasını düzenlemeniz yönünde uyarılar yazacaktır. SNMP yapılandırmanızı makalenin 2.2 bölümündeki gibi yaptıysanız herhangi bir sorun kalmayacaktır. *cfgmaker* komutu ile oluşturulan MRTG yapılandırma dosyasında ön tanımlı olarak tüm ethernet arayüzlerinizin TCP bağlantılarının grafikleri için gereken satırlar yazılıdır. Her ethernet arayüzü için farklı kısımlar oluşturulur. Web sayfanızda takip etmek istediğiniz ethernet arayüzüne ilişkin satırların önündeki # karakterini kaldırmanız gerekir (### ile başlayan satırlar açıklama satırlarıdır. Bu karakterleri silmeyiniz.). Birden fazla ethernet arayüzünün trafiğini görüntüleyebilirsiniz. Gerekli düzenlemeleri yaptıktan sonra MRTG yapılandırma dosyası şu şekildedir (*/etc/mrtg/mrtg.cfg* dosyasındaki terimlerin açıklamaları bu bölümün sonunda açıklanacaktır):

```
# cat /etc/mrtg/mrtg.cfg
# Created by
# /usr/bin/cfgmaker --global 'WorkDir: /var/www/mrtg' --global 'Options[_]:
bits,growright' --output /etc/mrtg/mrtg.cfg public@localhost


### 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

EnableIPv6: no
WorkDir: /var/www/mrtg
Options[_]: bits,growright

######################################################################
# System: mrtg.endersys.com.tr
# Description: Linux mrtg.endersys.com.tr 2.6.18-8.1.4.el5.028stab035.1 #1
SMP Mon Jul 23 14:37:32 EDT 2007 i686
# Contact: Metin KAYA <metin.kaya@endersys.com.tr>
# Location: Endersys Head Office, Istanbul
######################################################################

Target[localhost]: 2:public@localhost:
SetEnv[localhost]: MRTG_INT_IP="10.0.0.207" MRTG_INT_DESCR="eth0"
MaxBytes[localhost]: 1250000
Title[localhost]: Traffic Analysis for 1 -- mrtg.endersys.com.tr
PageTop[localhost]: <h1>Traffic Analysis for -- mrtg.endersys.com.tr</h1>
               <div id="sysdetails">
                       <table>
                               <tr>
                                       <td>System:</td>
                                       <td>mrtg.endersys.com.tr in Right here, right now.</td>
                               </tr>
                               <tr>
                                        <td>Maintainer:</td>
                                        <td>Metin KAYA &lt;metin.kaya@endersys.com.tr&gt;</td>
                               </tr>
                               <tr>
                                        <td>Description:</td>
                                        <td>eth0  </td>
                               </tr>
                               <tr>
                                        <td>ifType:</td>
                                        <td>ethernetCsmacd (6)</td>
                               </tr>
                               <tr>
                                        <td>ifName:</td>
```

```
                        <td>eth0</td>
                    </tr>
                    <tr>
                        <td>Max Speed:</td>
                        <td>1250.0 kBytes/s</td>
                    </tr>
                    <tr>
                        <td>Ip:</td>
                        <td>10.0.0.207 (mrtg.endersys)</td>
                    </tr>
                </table>
            </div>
```

MRTG yapılandırmamızda bir sorun olmadığını, işlerin yolunda gittiğini görmek için aşağıdaki komutları verebiliriz:

```
[metin@enderunix]# env LANG=C /usr/bin/mrtg /etc/mrtg/mrtg.cfg
Rateup WARNING: /usr/bin/rateup could not read the primary log file for
localhost_10.0.0.207
Rateup WARNING: /usr/bin/rateup The backup log file for
localhost_10.0.0.207 was invalid as well
Rateup WARNING: /usr/bin/rateup Can't remove localhost_10.0.0.207.old
updating log file
Rateup WARNING: /usr/bin/rateup Can't rename localhost_10.0.0.207.log to
localhost_10.0.0.207.old updating log file
[metin@enderunix]# env LANG=C /usr/bin/mrtg /etc/mrtg/mrtg.cfg
Rateup WARNING: /usr/bin/rateup Can't remove localhost_10.0.0.207.old
updating log file
[metin@enderunix]# env LANG=C /usr/bin/mrtg /etc/mrtg/mrtg.cfg
[metin@enderunix]#
```

Aynı komut 3 kez çalıştırıldı. Çünkü ilk 2 çalıştırmada kayıt dosyalarının döndürülmesi haliyle mümkün olmadığından (çünkü henüz bazı kayıt dosyaları oluşturulmadı) uyarılar alınır. Ancak 3. çalışmadan sonra hatasız-uyarısız çalışmaya devam edilebilir.

cfgmaker ile yapılandırma dosyasını oluşturduktan sonra *indexmaker* ile MRTG grafiklerini görüntüleyeceğimiz web sayfalarını oluşturmalıyız:

```
# indexmaker --output=/var/www/mrtg/index.html \
  --title="System Administration at Endersys"  \
  --sort=name --enumerate /etc/mrtg/mrtg.cfg
```

Bu komutun ardından */var/www/mrtg/* dizininde *index.html* dosyası oluşur. Bu dosya sayesinde web üzerinden MRTG grafikleri görüntülenebilir. *title* seçeneğiyle MRTG web sayfasının başlığı belirtilir.

3.3 MRTG Cron İşi

MRTG için gerekli paketleri yum ile kurduğunuz için bazı ayarlar (*cron* işi ve Apache yapılandırması) otomatik olarak yapılmıştır.

MRTG grafikleriniz ön tanımlı olarak 5 dakikada bir güncellenecektir. Yani *env LANG=C /usr/bin/mrtg /etc/mrtg/mrtg.cfg* komutu 5 dakika arayla çalıştırılır. Bu ayarı */etc/cron.d/mrtg* dosyasını düzenleyerek değiştirebilirsiniz. Örneğin; satır başındaki 5 'i 1 yaparsanız MRTG grafikleriniz her 1 dakikada bir güncellenir:

```
[metin@enderunix]# cat /etc/cron.d/mrtg
*/1 * * * * root LANG=C LC_ALL=C /usr/bin/mrtg /etc/mrtg/mrtg.cfg --lock-
file /var/lock/mrtg/mrtg_l –confcache-file /var/lib/mrtg/mrtg.ok
```

Burada ön tanımlı MRTG yapılandırma dosyası olarak */etc/mrtg/mrtg.cfg* kullanılır. Farklı bir yapılandırma dosyası kullanılacaksa */usr/bin/mrtg* 'den sonraki dosya adı uygun şekilde düzenlenmelidir.

3.4 MRG - Apache Yapılandırması

MRTG grafiklerinizin web tarayıcısıyla görüntülenebilmesi için */etc/httpd/conf.d/mrtg.conf* dosyasını düzenlemeniz gerekebilir. */etc/httpd/conf.d/mrtg.conf* dosyasında *Alias /mrtg* ile başlayan satırın devamında MRTG web sayfasının bulunduğu tam dizin adresi yazılmalıdır. Makaledeki yapılandırmaya göre bu satır şöyle olmalıdır:

```
Alias /mrtg /var/www/mrtg
```

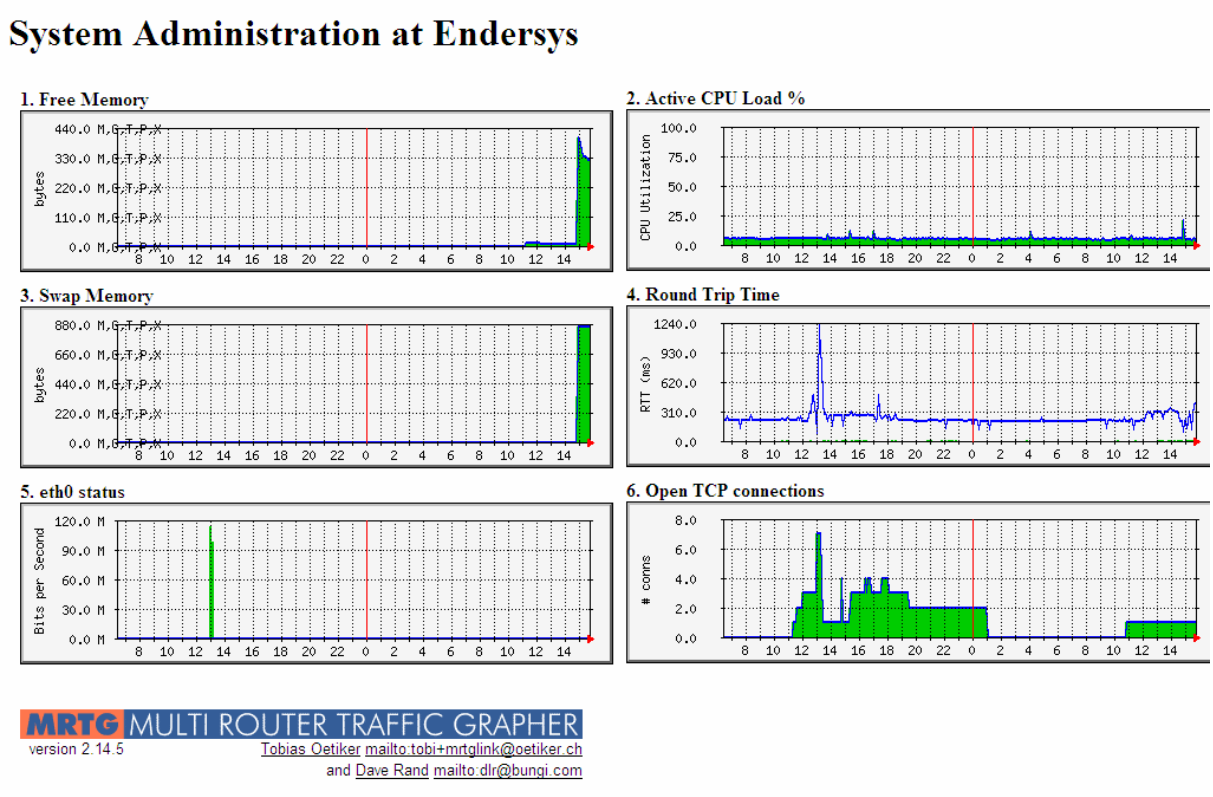
Ayrıca MRTG web sayfasının başkaları tarafından görülebilmesi için gerekli izinlerin verilmiş olması gerekir. Örneğin; bu sayfanın sadece kendi ağınızdan (örneğin 10.0.0.0 ağındaki bilgisayarlar) görüntülenmesini istiyorsanız */etc/httpd/conf.d/mrtg.conf* dosyasının ilgili kısmı aşağıdaki gibi olmalıdır:

```
<Location /mrtg>
    Order deny,allow
    Deny from all
    Allow from localhost 10.0.0.0/24
</Location>
```

Eğer MRTG sayfalarının internette herkes tarafından görüntülenebilmesini istiyorsanız bu satırlar şöyle olmalıdır:

```
<Location /mrtg>
    Order deny,allow
    Allow from all
</Location>
```

Bu aşamada tüm MRTG ayarları sona erdi. *http://mrtg_server_ip/mrtg* (örneğin http://10.0.0.207/mrtg) linkine tıklandığında MRTG web sayfasını görüntüleyebilirsiniz:



Şekil 3: Örnek MRTG Web Sayfası

3.5 Örnek MRTG Grafikleri

Aşağıda göstereceğimiz grafik oluşturmak için gerekli satırların hepsini makalenin 3.2 bölümünün sonunda gösterdiğimiz örnek */etc/mrtg/mrtg.cfg* dosyasına eklemeniz gerekir. Bu web sayfasında görülen 1. grafiği (boş bellek miktarı) elde etmek için */etc/mrtg/mrtg.cfg* dosyasına yazılması gereken satırlar şöyledir:

```
Target[freemem]:.1.3.6.1.4.1.2021.4.6.0&.1.3.6.1.4.1.2021.4.6.0:public@localhost
LoadMIBs: /usr/share/snmp/mibs/HOST-RESOURCES-MIB.txt
Options[freemem]: nopercent,growright,gauge,noinfo
Title[freemem]: <H1>Free Memory</H1>
PageTop[freemem]: <H1>Free Memory</H1>
MaxBytes[freemem]: 1000000
kMG[freemem]: k,M,G,T,P,X
YLegend[freemem]: bytes
ShortLegend[freemem]: bytes
LegendI[freemem]:  Free Memory:
LegendO[freemem]:
Legend1[freemem]: Free memory, not including swap, in bytes
```

2. grafiği (*nice*, kullanıcılar ve sistem tarafından kullanılan toplam CPU miktarı) elde etmek için */etc/mrtg/mrtg.cfg* dosyasına yazılması gereken satırlar şöyledir (*Target* ile başlayan satırdan *RouterUptime* ile başlayan satıra kadar olan satırlar tek satır olarak yazılmalıdır):

```
LoadMIBs: /usr/share/snmp/mibs/UCD-SNMP-MIB.txt
Target[localhost.cpu]:ssCpuRawUser.0&ssCpuRawUser.0:public@localhost +
ssCpuRawSystem.0&ssCpuRawSystem.0:public@localhost +
ssCpuRawNice.0&ssCpuRawNice.0:public@localhost
RouterUptime[localhost.cpu]: public@localhost
MaxBytes[localhost.cpu]: 100
Title[localhost.cpu]: CPU Load
PageTop[localhost.cpu]: <H1>Active CPU Load %</H1>
Unscaled[localhost.cpu]: ymwd
ShortLegend[localhost.cpu]: %
YLegend[localhost.cpu]: CPU Utilization
Legend1[localhost.cpu]: Active CPU in % (Load)
Legend2[localhost.cpu]:
Legend3[localhost.cpu]:
Legend4[localhost.cpu]:
LegendI[localhost.cpu]:  Active
LegendO[localhost.cpu]:
Options[localhost.cpu]: growright,nopercent
```

3. grafiği (takas bellek alanı) elde etmek için */etc/mrtg/mrtg.cfg* dosyasına yazılması gereken satırlar şöyledir:

```
Target[localhost.swap]:memAvailSwap.0&memAvailSwap.0:public@localhost
LoadMIBs: /usr/share/snmp/mibs/UCD-SNMP-MIB.txt
PageTop[localhost.swap]: <H1>Swap Memory</H1>
Options[localhost.swap]: nopercent,growright,gauge,noinfo
Title[localhost.swap]: Free Memory
MaxBytes[localhost.swap]: 1000000
kMG[localhost.swap]: k,M,G,T,P,X
YLegend[localhost.swap]: bytes
ShortLegend[localhost.swap]: bytes
LegendI[localhost.swap]:  Free Memory:
LegendO[localhost.swap]:
Legend1[localhost.swap]: Free memory avail, in bytes
```

4. grafiği (sisteminizin kendisine atılan bir pinge ortalama kaç saniyede cevap verdiğini gösterir) elde etmek için */etc/mrtg/mrtg.cfg* dosyasına yazılması gereken satırlar şöyledir:

```
Title[ping]: Round Trip Time
PageTop[ping]: <H1>Round Trip Time</H1>
Target[ping]: `/etc/mrtg/ping.sh`
MaxBytes[ping]: 2000
Options[ping]: growright,unknaszero,nopercent,gauge
LegendI[ping]: Pkt loss %
LegendO[ping]: Avg RTT
Legend1[ping]: Maximum Round Trip Time in ms
Legend2[ping]: Minimum Round Trip Time in ms
YLegend[ping]: RTT (ms)
```

Burada kullanılan *ping.sh* dosyası ise şöyledir (bu betiği */etc/mrtg/ping.sh* olarak kaydedip *chmod 755 /etc/mrtg/ping.sh* komutu ile çalışma izni vermelisiniz):

[metin@enderunix]# cat /etc/mrtg/ping.sh

```
#!/bin/sh

PING="/bin/ping"
ADDR="localhost"
DATA=`$PING -c10 -s500 $ADDR -q `
LOSS=`echo $DATA | awk '{print $18 }' | tr -d %`

echo $LOSS

if [ $LOSS = 100 ];
then
        echo 0
else
        echo $DATA | awk -F/ '{print $5 }'
fi
```

5. grafiği elde etmek için makalenin 3.2 bölümünün sonunda gösterilen örnek MRTG yapılandırma dosyasındaki (*/etc/mrtg/mrtg.cfg*) *Target[localhost]: 2:public@localhost:* satırından dosya sonuna kadar olan kısmı kullanabilirsiniz.

6. grafiği (açık TCP bağlantı sayısı) elde etmek için */etc/mrtg/mrtg.cfg* dosyasına yazılması gereken satırlar şöyledir:

```
Target[tcpopen]:.1.3.6.1.2.1.6.9.0&.1.3.6.1.2.1.6.9.0:public@localhost
Options[tcpopen]: nopercent,growright,gauge,noinfo
Title[tcpopen]: Open TCP connections
```

```
PageTop[tcpopen]:<h1> Open TCP connections</h1>
MaxBytes[tcpopen]: 1000000
YLegend[tcpopen]: # conns
ShortLegend[tcpopen]: connections
LegendI[tcpopen]:  Connections:
LegendO[tcpopen]:
Legend1[tcpopen]: Open TCP connections
```

3.6 MRTG Terimlerinin Açıklamaları

/etc/mrtg/mrtg.cfg dosyasında kullandığımız bazı terimlerin açıklamaları Şekil 4 'te gösterilmiştir.

UCD – SNMP – MIB Nesne DeğiUşkeni	**MIB Tipi**	**MRTG Tipi**	**Açıklama**
ssCpuRawUser	Counter	Counter	Sistem başlatıldığından itibaren *root* hakkı olmayan kullanıcıların çalıştırdıkları uygulamaların kullandığı toplam CPU miktarıdır. Bu değere *ssCpuRawSystem* ve *ssCpuRawNice* değerleri eklenirse kullanılan toplam CPU miktarı hakkında anlamlı bir veri elde edilebilir.
ssCpuRawSystem	Counter	Counter	Sistem başlatıldığından itibaren *root* hakkı olan kullanıcıların çalıştırdığı uygulamaların harcadığı CPU miktarıdır.
ssCpuRawNice	Counter	Counter	Ön tanımlı öncelik değerinde çalışmayan uygulamaların kullandığı CPU miktarıdır.
ssCpuRawIdle	Counter	Counter	Kullanılmayan CPU miktarıdır. Bu sayı 100 'den çıkarılırsa kullanılan toplam CPU miktarı hakkında fikir verir.
memAvailReal	Integer	Gauge	Makinedeki kullanılabilir toplam fiziksel bellek miktarıdır.
tcpActiveOpens	Counter	Counter	Etkin (kurulumu tamamlanmış) TCP bağlantı sayısıdır.
tcpCurrEstab	Gauge	Gauge	Henüz kurulum aşamasındaki TCP bağlantı sayısıdır.
tcpInErrs	Counter	Counter	Hatalı (checksum error) TCP bağlantı sayısıdır.

Şekil 4: MRTG Yapılandırma Dosyasındaki Bazı Terimlerin Karşılıkları

MRTG yapılandırma parametreleri aşağıdaki biçimde yazılır:

```
Parametre[grafik_adı]: değer1
```

Buradaki *değer1* grafiğin giriş OID parametresidir. Çıkış OID parametresi de yazılacaksa ilgili satır şu biçimde olmalıdır (*değer2* çıkış parametresidir):

```
Parametre[grafik_adı]: değer1&değer2
```

Grafiğin giriş OID parametresini *LegendI* veya *Legend1* olarak ifade edilir. Çıkış OID parametresi de *LegendO* veya *Legend2* olarak tanımlanır. *YLegend* ise grafiğin Y eksenini ifade eder.

Grafiklerin üzerinde görülen başlık yazıları *PageTop* ile ifade edilir ve bu yazı *<h1>* ve *</h1>* arasında yazılmalıdır (*<H1>* ve *</H1>* de olabilir). Örneğin; *PageTop[tcpopen]: <h1> Open TCP connections </h1>*.

EnableIPv6, *Options[_]* ve *WorkDir* değişkenleri global değişkenler olup MRTG yapılandırma dosyasında sadece bir kez yazılmalıdır.

MRTG yapılandırma dosyasının başındaki *Options[_]:* ile başlayan satır tüm grafiklere uygulanacak seçenekleri ifade eder. *Options[grafik_adı]:* ile başlayan satırlar ise sadece ilgili grafiğe uygulanacak seçenekleri belirtir.

MaxBytes seçeneği ise MRTG 'nin grafik üzerine en fazla kaç veri çizeceğini belirtir. Bu değerden fazla sayıda veri olursa bunlar grafikte gösterilmez.

MRTG grafiği oluştururken *Target* seçeneğinde bir betik kullanılmıyorsa her zaman 2 MIB OID nesnesi kullanılır. *Target* seçeneğinin yazım biçimi şöyledir (MIB nesnelerinin isimleri *.0* ile bitmelidir. IP adresi yerine makine adı da yazabilirsiniz. SNMP parolası ise *public* olabilir.):

```
Target[grafik_adı]: MIB_nesnesi1.0&MIB_nesnesi2.0:SNMP_parolası@IP_adresi
```

Betik kullanılıyorsa aşağıdaki gibi olmalıdır:

```
Target[grafik_adı]:`betik_adı`
```

Eğer aynı grafikte birden fazla MIB nesnesi değeri kullanılacaksa bu durumda *Target* satırı şöyle olmalıdır (**tek satır olarak yazılmalıdır**):

```
Target[grafik_adı]: MIB_nesnesi1.0&MIB_nesnesi2.0:SNMP_parolası@IP_adresi +
MIB_nesnesi3.0&MIB_nesnesi4.0:SNMP_parolası@IP_adresi +
MIB_nesnesi5.0&MIB_nesnesi6.0:SNMP_parolası@IP_adresi + …
```

Target satırında toplama (+) , çıkarma (-), çarpma (*), bölme (%), ve parantezler (()) kullanılabilir. Yalnız bu karakterlerden önce ve sonra mutlaka boşluk (Space veya TAB) olmalıdır.

4. Olası MRTG Hataları ve Çözümleri

► HTTP 403 YASAK

MRTG web sayfasını görmek istediğinizde bu hatayı alıyorsanız izin sorununuz vardır. Sorunun çözümü için makalenin 3.4 bölümünü inceleyiniz.

► MRTG web sayfasına tıkladığınızda (örneğin; http://10.0.0.207/mrtg) grafikleri göremiyorsanız MRTG çalışma dizinlerinde bir tutarsızlık vardır. */etc/httpd/conf.d/mrtg.conf* dosyasındaki *Alias* satırını uygun şekilde düzeltip Apache 'yi yeniden başlatınız (*service httpd restart*). Esasında sorun MRTG 'nin grafikleri oluşturmak için kullandığı resimlerin Apache tarafından bulunamamasıdır. Bu durum */var/log/http/error_log* dosyasına bakarak anlaşılabilir:

```
# tail /var/log/http/error_log
[Tue Jul 10 03:15:37 2007] [error] [client 10.0.0.203] File does not exist:
/var/www/mrtg/localhost_2-day.png, referer: http://10.0.0.207/mrtg/
[Tue Jul 10 03:15:37 2007] [error] [client 10.0.0.203] File does not exist:
/var/www/mrtg/mithril.ping-day.png, referer: http://10.0.0.207/mrtg/
```

►LANG Çevre Değişkeni

/usr/bin/mrtg veya *mrtg* gibi komutları çalıştırdığınızda *LANG* çevre değişkeninin UTF-8 olmasından kaynaklanan bir hata alıyorsanız bu komutları şu şekilde çalıştırınız:

```
[metin@enderunix]# /usr/bin/mrtg /etc/mrtg/mrtg.cfg
ERROR: Mrtg will most likely not work properly when the environment
variable LANG is set to UTF-8. Please run mrtg in an environment
where this is not the case. Try the following command to start:

env LANG=C /usr/bin/mrtg
[metin@enderunix]# env LANG=C /usr/bin/mrtg /etc/mrtg/mrtg.cfg
[metin@enderunix]#
```

► Kullandığınız IP adresi (makine adı) ve SNMP kullanıcı adlarının doğru olduğundan emin olunuz.

► MRTG yapılandırma dosyasında (*/etc/mrtg/mrtg.cfg*) yapmaya çalıştığınız SNMP *walk* ve SNMP *get* işlemlerini yapabildiğinizden emin olmak için ilgili komutları elle çalıştırmayı deneyiniz (makalenin 2.4 kısmına bakabilirsiniz).

5. Kaynaklar

- TCP/IP Illustrated, Volume 1: The Protocols, W. Richard Stevens, Addison-Wesley, 1994, ISBN 0-201-63346-9
- http://www.linuxhomenetworking.com/wiki/index.php
- http://www.belgeler.org/howto/mrtg.html
- Komutların kılavuz sayfaları (man pages)