

Multi Network Traffic Monitor (MNTM)

Sürüm 1.0

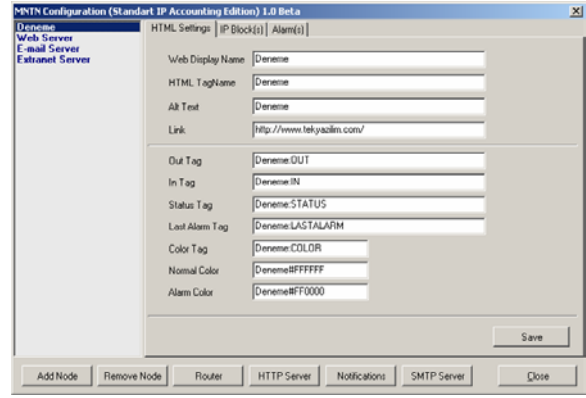
Günümüzde ağ servisleri ve IP uçlarının izlenmesi için birçok araç bulunmaktadır. Bu uygulamaların neredeyse tamamı ICMP paketleri ile (*Ping*) belirlenen IP uçlarını yoklayarak raporlar üretmektedirler. Ancak bu yaklaşım her zaman asıl sorunun tespiti için hızlı bir çözüm sağlamamaktadır. Bir ağ ucunun bir ping paketine cevap vermesi her zaman işlerin yolunda gittiği anlamına gelmemektedir. Örneğin omurga yönlendiricisindeki hatalı bir yönlendirme tanımından dolayı yerel ağdaki bir web sunucusuna dış ağlardan bağlantı sağlanamıyor olabilir. Yerel ağ üzerindeki bir izleme istasyonu web sunucusunun etkin olduğunu rapor etmesine karşın sorunun tespiti ancak Internet kullanıcılarından gelen uyarılardan sonra mümkün olabilecektir.

MNTM bir ağdaki trafik akışlarını izleyerek, belirlenen IP uçları ve ağları için alınan ve verilen trafik hacmini gerçek zamanlı olarak raporlayan, kullanıcı tarafından belirlenen eşik değerlerine göre alarmlar üreten bir uygulamadır. MNTM IP trafik akışı bilgisini aşağıdaki yöntemlerle izleyebilmektedir:

1. **IP Accounting.** IP Accounting verisi omurga yönlendiricisinden (*Cisco, Juniper ve Nortel gibi*) veya yerel ağ üzerindeki bir Linux sunucusundan çekilerek işlenebilmektedir.
2. **Netflow.** Netflow verisi omurga yönlendiricisinden (*Cisco ve Juniper gibi*) ya da yerel ağ üzerindeki Bir Linux sunucusundan (*cflood*) çekilerek işlenebilmektedir.

Program Win32 servisi ve kullanıcı ara yüzünden oluşmaktadır. Kullanıcı ara yüzü, izlenecek IP uçları ve ağları için gerekli yapılandırma bilgisinin girilmesini sağlamaktadır. Servis uygulaması IP akışlarını izleyerek, kullanıcı ara yüzü ile belirlenen IP uçları ve ağları için giriş ve çıkış yönlerindeki trafikleri Kbps olarak hesaplamaktadır. Bu değer kullanıcı tarafından belirlenen eşik değerleri dışına çıkarsa ağ yöneticisine uyarı mesajı (*E-mail, NT Messenger, MSN Messenger ve ICQ*) gönderilmektedir. Servis uygulaması başlatıldığında, Windows görev

çubuğuna eklenen MNTM servis simgesine sağ tuşla kliklenerek gerçek zamanlı olarak kullanıcı tarafından izlenmek üzere belirtilen IP uçları ve ağlarına ilişkin bilgi alınabilmektedir. Aynı bilgiye web tabanlı olarak ulaşılabilmektedir; MNTM servisi dahili olarak web sunucu özelliğine sahiptir. Kullanıcıya görüntülenen web sayfasında, servis simgesine sağ tuşla kliklenerek erişilen penceredeki bilgiler yer almaktadır.



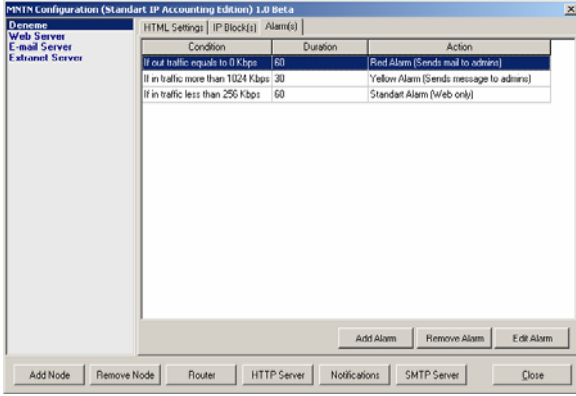
Şekil 1. - MTNM Setup Penceresi

Trafik akışları izlenerek belirli bir zaman aşımından sonra belirli bir IP ucu için hiç trafik alış verişi gözlemlenmiyorsa ya da belirlenen bir değer altında trafik alış verişi gerçekleşiyorsa MNTM ile ağ yöneticisinin uyarılması mümkündür. Benzeri şekilde olağandışı bir trafik akışının tespit edilmesi durumunda da MTNM alarm üretebilmektedir. MTNM ile sadece yerel ağdaki değil, ağ dışındaki IP uçları ve IP aralıkları ile olan trafik akışlarını izlemek mümkündür (*Örneğin kullanıcıların çok bağlandıkları yerel ağ dışında bulunan bir web sunucusu gibi*).

MNTM'de izlenecek IP ucu ve IP ağları için aşağıdaki tanımlar ve eşik değerleri belirlenebilmektedir:

1. **Tanım.** İzlenecek IP ya da IP aralığı için bir tanım girilebilir.
2. **IP veya IP aralığı.** Giriş ve çıkış trafiği izlenecek tek bir IP, alt ağ maskesi ile belirlenmiş bir IP ağı ya da başlangıç ve bitiş IP adresleri verilmiş bir IP aralığı girilebilir.

3. **Alarm eşik değerleri.** İzlenecek IP ya da IP aralığı için giriş/çıkış trafiğinin hiç gözlemlenmemesi, belirli bir değerin üzerine çıkması ya da altında seyretmesi durumları belirlenebilir. Söz konusu eşik değerinin ne kadar süre gözlemlendikten sonra alarmın üretileceği de belirlenebilmektedir.



Şekil 2. - MNTM Alarmlar Penceresi

Kullanıcı tarafından izlenmek üzere girilebilecek IP ya da IP aralığı sayısında teorik bir sınır bulunmamaktadır. Ancak izlenecek IP ya da IP aralığı sayısı arttıkça MNTM'in çalıştırıldığı sunucuda ihtiyaç duyulan işlem gücünün de artacağı unutulmamalıdır.

MNTM izlenmek üzere veritabanına girilen tüm IP ve IP aralıkları için üretilen alarmlar için ayrıca bir kayıt dosyası tutmaktadır.

Aşağıda MNTM web ara yüzünden erişilebilen örnek rapor ekranı bulunmaktadır:

IP Model	Description	In Traffic	Out Traffic	Current Alarm	Current Alarm Start	Last Alarm	Last Alarm Duration
192.168.0.10	Web Server	4 Kbps	4 Kbps	Out traffic higher than 512 Kbps for Week days (09:00-17:00)	10/20/14/08/2003	10/20/14/08/2003	11:12:14.08.2003 (72 Minutes)
192.168.0.24	Company Network	228 Kbps	44 Kbps	No Alarm			
192.168.0.32	Company Laptop	180 Kbps	32 Kbps	No Alarm		Out traffic higher than 512 Kbps for Weekdays (09:00-17:00)	10/20/14/08/2003 - 11:12:14.08.2003 (72 Minutes)

Şekil 3. - MNTM Web Arayüzü

Sistem Gereksinimleri

- Pentium III üzeri işlemci, 512 MByte RAM
- Asgari 20 GByte disk alanı (*Log büyüklüğüne göre belirlenmelidir.*)
- Windows NT, Windows 2000, XP işletim sistemi.
- Ağ erişimi
- Cisco Ağ cihazı (*IOS sürüm 11.0+, Cisco IP Accounting için*)

Tek Yazılım tarafından geliştirilmiştir. Her hakkı saklıdır. Burada verilen bilgiler önceden haber verilmeksizin değiştirilebilir. İsmi geçen markalar üreticilerinin koruması altındadır.

© 2003 Tek Yazılım - Her hakkı saklıdır - info@tekyazilim.com / <http://www.tekyazilim.com/>