

## SNMP

### Mehmet Ali KARAGÖL / İTÜ'BİDB 2009

#### SNMP Nedir?

SNMP, adında anlaşılacağı gibi basit bir network yönetim protokolüdür. UDP bazlı çalışan SNMP, Internet protokolünün bir parçası olarak ve genellikle network yönetim sistemlerinde ağın ya da ağdaki cihazların durumlarını izlemek ve olası durumlarda ağ yöneticisinin hemen müdahale edebilmesini sağlamak için oluşturulmuş ve geliştirilmiştir. Uygulama katmanında çalışan bir protokoldür.

#### SNMP'yi Oluşturan Bileşenler

SNMP temel olarak üç bileşenden oluşur. Bunlar;

**Agent:** Ağdaki cihazlar üzerinde çalışan bir uygulamadır. Bu uygulama sayesinde gerekli bilgiler toplanıp kayıtlı tutularak (örneğin, o cihaz tarafından alınmış hatalı paketlerin sayısı) ağ yöneticisine aktarılır, aynı şekilde yöneticiden gelen ve cihaz üzerinde yapılması istenen değişiklikler cihaza uygulanır.

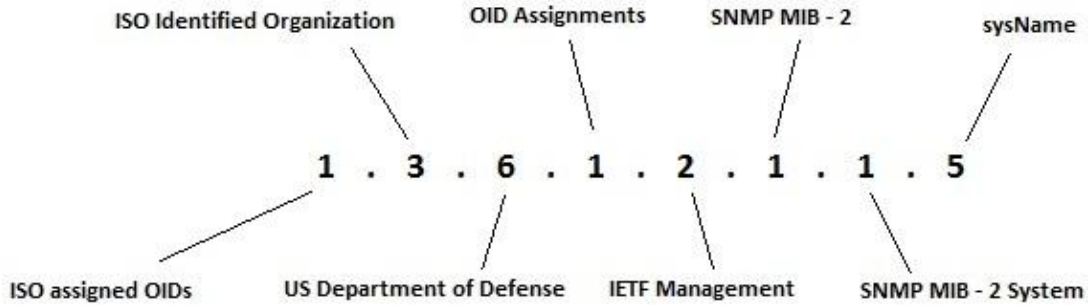
**Managed object:** Bir bakıma agent uygulama ile yönetici arasındaki bilgi alışverişini sağlayan uygulamadır. Ajan uygulamadan gerekli bilgileri alır yöneticiye iletir, yöneticiden aldığı değişiklik isteklerini de cihazlara iletir.

Network Management System: Ağ yöneticisi tarafından çalışan ve tüm ağ üzerindeki bulunan cihazların eş zamanlı olarak izlenmesini sağlayan uygulamaya verilen isimdir.

#### SNMP Yönetim Bilgi Birimleri (MIB – Management Information Base)

Yöneticinin cihazlar hakkında almak istediği her bir bilgi için önceden tanımlanmış parametreler bulunmaktadır. Bu parametrelerin tutulduğu birime de Yönetim Bilgi Birimi (MIB) denir. Aynı zamanda yöneticinin Agent Uygulama'dan isteyebileceği bilgilerin tutulduğu birim şeklinde de ifade edilebilir.

MIB hiyerarşisi, her bir seviyesi farklı bir organizasyon ya da kuruluş tarafından belirlenmiş ya da standartlaştırılmış bir ağaç yapısı olarak düşünülebilir. Örneğin aşağıda bir ağda bulunan cihazın üreticisi tarafından verilen açıklamasını incelersek;



Burada verilen açıklama, baştan başlayarak hiyerarşide bulunan organizasyonların isimlerini görebiliriz. Açıklamanın sonunda ise böyle bir sorgunun ağ ya sistemdeki herhangi bir cihaza yapıldığı zaman vereceği cevabı görebiliriz. 5 koduyla da belirtilmiş olan “sistem isim bilgisini” yöneticiye cevap olarak döndürür. Bu ve buna benzer açıklamalar sayesinde sistemler ve network kolaylıkla izlenebilmekte ve anlık olarak cihazlarla ilgili öğrenilmesi istenen özellikler, cihazların durumu, performansı ve buna benzer daha birçok bilgiye ulaşılabilmektedir.

### SNMP Nasıl Kullanılır?

SNMP temel olarak istek gönderme ve gönderilen bu isteklere cevap verme üzerine çalışır. Bunu yaparken UDP ve çok az da olsa IP gibi iletişim protokollerinden birisi kullanılabilir. SNMP'nin çalışması aşağıdaki yöntemlerle gerçekleştirilir;

**Get:** yönetici birim tarafından yönetim birimindeki veya başka bir bilgi birimindeki değerleri (uzaktaki bir network cihazı için herhangi bir değer olabilir) elde etmek için kullanılan istek komutu olarak nitelendirilmektedir.

**Getnext:** Get komutuyla elde edilmek istenen bilgiden bir sonraki bilgiyi elde etmek için gönderilen istek komutudur. Yukarıda verdiğimiz örnekte inceleyecek olursak;

1.3.6.1.2.1.1 → bu bilgiyi get yöntemiyle aldığımızı kabul edelim;

Getnext komutuyla ise bu ağaç yapısında bulunan bir sonraki OID değerini sorgulayabiliriz. Örnek olarak yukarıda öğrendiğimiz sistem ismi (1.3.6.1.2.1.1.5) olabilir.

**Set:** yönetim biriminin yönetmekte olduğu bir cihaz üzerinde değiştirmek istediği değerleri ya da özellikleri uygulamak için kullandığı komuttur.

**Trap:** Bu işlemin gerçekleştirilmesi için yönetici biriminden bir istek gönderilmiş olmasına gerek yoktur. İzlenen cihazlarda ve sistemde, yani üzerinde ajan uygulama çalışan birimlerde alışılmadık bir durumda bir durum fark edildiğinde bunun yönetici birime bildirilmesini sağlayan işlemdir.

SNMP'nin 3 tane sürümü bulunmaktadır. Yukarda açıkladığımız 4 işlem de SNMPv1'in elemanlarıdır. SNMP2'de bu işlemlerin üzerinde iki işlem daha eklenmiştir. Bunlar Getbulk ve Inform işlemleridir. Bunların yanında SNMPv3 sürümü de bulunmaktadır ki, kimlik denetimi, gizlilik ve erişim kontrolü sağlamasıyla en güvenli SNMP sürümüdür. Ajan uygulamanın çalıştığı cihazlarla iletişim şifreli bir şekilde yapılır.

### **SNMP Uygulamaları ve Kullanım Alanları**

Bizim yaptığımız gibi büyük bir ağı yöneten ve dolayısıyla çok fazla sayıda uzaktan yönetilme zorunluluğu isteyen cihazlara sahip olan yöneticiler için SNMP son derece kullanışlıdır. Bu ağ içerisinde routerlar, sunucular, switchler, access pointler, modemler ve kişisel bilgisayarlar gibi cihazlar bulunur ve bunların hepsinde birer tane SNMP ajanı bulunabilir. Bu ajan uygulamalar ile cihazlar kendilerinden istenen bilgilerini ve müdahale edilmesi gereken acil durumlardaki değişiklikleri yönetici birimine bildirirler. Güvenliğin çok önemli bir husus olmasından dolayı SNMP kişisel ağlarda çok fazla kullanılmaz. SNMPv3 ile bu güvenlik sorunu aşılmış olsa da yine de kullanımı çok yaygın değildir.