SNMP

SNMP (Simple Network Managemetn Protocol) protokolü, networkü monitor edebilmek için networkteki cihazların (router, switch, firewall, server ...) durumu hakkında bilgi toplamak veya belirli kapsamda cihaz üzerinde değişiklikler yapabilmek için kullanılan protokolüdür.

SNMP protokolünün işleyiş sürecinde kullanılan üç yapı bulunmaktadır. Bu yapılar;

- SNMP Agent, durum bilgisi alınmka istenen cihazları temsilen kullanılıyor (UDP 162 portunu kullanır).
- SNMP Manager, SNMP Agent'lara sorgular yapılarak durum bilgilerinin toplandığı cihazdır (UDP 161 portunu kullanır).
- MIB (Managemetn Infromation Base), SNMP Manager tarafından SNMP Agent'a gönderilmek istenen her sorgu MIB üzerinde bir sayısal değere karşılık gelmektedir. Bu sayısal değerler kullanılarak SNMP Agent'a sorguda bulunulabilmektedir.

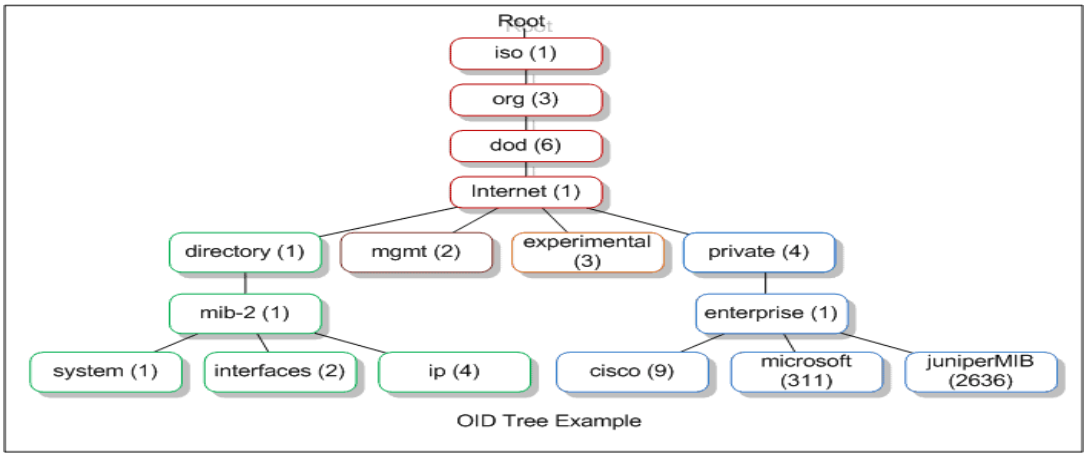
Genel olarak işleyişe bakıldığında, bir cihaz üzerinde SNMP Manager yazılımı, monitor edilmek istenen cihazların üzerinde de SNMP Agent yazılımı kurulur. Bu sayede SNMP Manager topolojide bulunan cihazlara MIB değerleri göz önünde bulundurularak belirli aralıklarda sorgu paketleri gönderebilir. SNMP Agent ise sorgu paketini aldıktan sonra üzerinde bulunan sayısal değerin karşılığını MIB tablosunda arayarak istenen işlemi tespit eder. SNMP Manager tarafından gönderilen isteğin tipine bağlı olarak cihaz üzerinde SNMP Manager'ın belirttiği konfigürasyonları gerçekleştirir veya istenen bilgileri SNMP Manager'a gönderir. Bu süreçte kullanılan birkaç mesaj tipi vardır.

- Get-request, SNMP yöneticisinin bilgi istemek için gönderdiği en yaygın SNMP istek mesajıdır.
- Get-next-request, get-request komutu ile elde edilen bilginin bir sonrakini elde etmek için kullanılan mesaj tipidir.
- Get-bulk-request, büyük boyutlu veri kümelerindeki değerleri almak için kullanılan mesaj tipidir.
- Get-response, SNMP Manager tarafından istek talebinde bulunulduğunda yanıt göndermek için kullanılan mesaj tipidir.
- Set-request, cihaz üzerinde bir değişiklik yapmak için kullanılan mesaj tipidir.
- Trap, SNMP Agent tarafından bir olay gerçekleştiğinde SNMP Manager'a bildirmek için kullanılan mesaj tipidir.

MIB (Management Information Base)

MIB tablosu hiyerarşik (tree) bir yapıdadır. Bu yapıda sorguya eklenen her elemana Object adı verilir. Her Object'i temsil edecek bir ID (OID) değeri atanmıştır. Oluşan hiyerarşik (tree) yapı üzerinde ortak sorgular (her marka/model cihaz için kullanılabilen) bulunabildiği gibi marka bazlı sorgular da bulunuyor. Örnek olarak aşağıdaki görsel göz önünde bulundurulduğunda cihazın herhangi bir arayüzü hakkında bilgi alabilmek için "1.3.6.1.1.1.2..." gibi bir örüntü kullanılarak cihaza istekte bulunuluyor. Marka bazlı bir özellik sorgulanmak istendiğin ise "1.3.6.1.4.1..." gibi bir sıralamanın kullanılması gerekiyor.

Bu sayede yazılımlar kullanılarak cihazlara belirli sıklıklarda sorgular yapılması sağlanıyor ve bu doğrultuda alınan dönüşlerin grafiklerle dökülmesiyle network cihazları monitör edilebiliyor. Bu grafikler sayesinde networkte değişim/anomali tespiti yapılabiliyor (SolarWinds, Cacti, Zabbix ...).



OID Tree Example

SNMP Sürümleri

SNMP'nin birçak sürümü bulunmaktadır. Bu sürümlere bakıldığında;

- SNMPv1, SNMP'nin en eski versiyonudur. SNMP Agent'lardan bilgi alabilmek için basit fonksiyonlar sağlar. 32 bit counter yapısına sahip olduğu için büyük trafiklerde yetersiz kalmaktadır. Şifreleme veya kimlik doğrulama gibi herhangi bir güvenlik desteği bulunmamaktadır.
- SNMPv2c, 64 bit counter yapısını geçilmiştir ama herhangi bir güvenlik desteği bulunmamaktadır. SNMPv2u ve SNMPv2p olmak üzere iki farklı versiyonu daha bulunmaktadır.
- SNMPv3, SNMPv2c özelliklerini içermektedir. Farklı olarak kimlik doğrulama (authentication), şifreleme (encryption), kullanıcı ve grup bazlı yetkilendirme gibi çeşitli güvenlik önlemleri getirilmiştir (Bu mekanizmalar beraberinde konfigürasyon zorluğu da getirmiştir). Desteklenen güvenlik mekanizmaları isteğe bağlı olarak devreye alınabiliyor. Bunun için üç çalışma modu vardır. Bunlar;
    - SNMPv3 noAuthNoPriv, kimlik doğrulama işlemi için sadece topluluk dizesini veya bir kullanıcı adını kullanır (Sadece kullanıcı adı eşlemesi kullanılıyor).
    - SNMPv3 authNoPriv, HMAC-MD5 veya HMAC-SHA algoritmaları kullanılarak kimlik doğrulama sağlar (Veriler için şifreleme desteklenmez).
    - SNMPv3 authPriv, HMAC-MD5 veya HMAC-SHA algoritmaları kullanılarak kimlik doğrulama sağlar. Ek olarak Privacy için ise DES (Data Encryption Standard), 3DES ve AES (Advanced Encryption Standard) gibi protokoller kullanılarak veri gizliliği için şifreleme sağlanır (Özetle kimlik doğrulama ve şifreleme özelliği devreye alınabiliyor).

SNMP protokolünde görüldüğü gibi SNMP Agent'lar gönderilen isteklere karşılık vermek (bu bilgi paylaşmak veya cihaz üzerinde bir değişiklik yapmak olabilir) durumundadır. Bu durum SNMPv1 ve SNMPv2 sürümlerinde de açıklandığı gibi kimlik doğrulama ve şifreleme mekanizmaları desteklenmediği için bu sürümlerin kullanılması kritik güvenlik zafiyetleri oluşturmaktadır. Bir saldırgan cihazlara bir SNMP Manager gibi istek paketleri gönderek cihazlardan bilgi almakla kalmayıp üzerinde değişiklik/konfigürasyon yapabilme yetkisine sahip olacaktır. Bu durumu karşı SNMP sürümlerinde alınabilecek önlemlere bakıldığında;

- SNMPv2 için güvenlik konfigürasyonuda sorgu yapabilecek cihazlar bir ACL tanımlanarak harici bağlantı istekleri filtrelenebiliyor (Bu konfigürasyon CCNA-3.09 – Network Management notlarında da açıklanmıştır).
    - Öncelikle sorgu yapabilmesine izin verilecek cihazların ip adresleri için Standart ACL (İsimlendirilmiş veya numaralandırmış farketmiyor) tanımlanıyor. Tanımlanan Standard ACL numarası veya ismi kullanılarak SNMP konfigürasyonunda kullanılan komutun ("**snmp-server community <Password for Community> <Access Type>**") sonuna ekleniyor.

```
R1(config)#access-list 5 permit 192.168.10.100
R1(config)#snmp-server community MyPass rw 5
R1(config)#
```

    |→ Sorgu yapabilmek için anahtar kelime bilinmese dahi parola denemeleri yapılarak cihazın CPU'su çatlatılabiliyor Bu nedenle erişimleri kısıtlamak gerekiyor.
    |→ **Bu güvenlik önlemi SNMP versiyonu farketmeksizin uygulanabiliyor**

- SNMPv3 konfigürasyonu için uygulanabilecek güvenlik önlemleri;
    - Öncelikle sorgu yapabilmesi istenen cihazlar için Standar ACL oluşturularak filreleme yapılabiliyor.
    - SNMP Manager'ın kullanabileceği MIB değerleri "**snmp-server view <MIB Value> <MIB View Name> <included | excluded>**" komutuyla gruplandırılabiliyor ve bunlara View deniyor (Tanımlanan bu View'ler de gruplara veya kullanıcılara uygulanabiliyor).
    - "**snmp-server group <Group Name> v3 priv read <View Name> access <ACL Number | ACL Name>**" komutuyla grup bazlı kısıtlamalar tanımlanabiliyor.
    - "**snmp-server user username <Group Name> v3 auth <md5 | sha> <Auth Password> priv <DES | 3DES | AES {128 | 192 | 256}> <Priv Password>**" komutuyla kullanıcı bazlı güvenlik önlemleri ve kısıtlamalar tanımlanabiliyor

Group

```
R1(config)#snmp-server group Group1 ?
  v1   group using the v1 security model
  v2c  group using the v2c security model
  v3   group using the User Security Model (SNMPv3)

R1(config)#snmp-server group Group1 v3 ?
  auth    group using the authNoPriv Security Level
  noauth  group using the noAuthNoPriv Security Level
  priv    group using SNMPv3 authPriv security level

R1(config)#snmp-server group Group1 v3 priv ?
  access   specify an access-list associated with this group
  context  specify a context to associate these views for the group
  notify   specify a notify view for the group
  read     specify a read view for the group
  write    specify a write view for the group
  <cr>

R1(config)#snmp-server group Group1 v3 priv read ?
  WORD  read view name

R1(config)#snmp-server group Group1 v3 priv read View1 ?
  access  specify an access-list associated with this group
  notify  specify a notify view for the group
  write   specify a write view for the group
  <cr>

R1(config)#snmp-server group Group1 v3 priv read View1 access ?
  <1-99>  Std IP accesslist allowing access with this group
  WORD    Access-list name
  ipv6    Specify IPv6 Named Access-List
  <cr>

R1(config)#snmp-server group Group1 v3 priv read View1 access ACL1
```

User

```
R1(config)#snmp-server user UName1 ?
  WORD  Group to which the user belongs

R1(config)#snmp-server user UName1 G1 v3 ?
  access     specify an access-list associated with this group
  auth       authentication parameters for the user
  encrypted  specifying passwords as MD5 or SHA digests
  <cr>

R1(config)#snmp-server user UName1 G1 v3 auth ?
  md5  Use HMAC MD5 algorithm for authentication
  sha  Use HMAC SHA algorithm for authentication

R1(config)#snmp-server user UName1 G1 v3 auth sha ?
  WORD  authentication pasword for user

R1(config)#snmp-server user UName1 G1 v3 auth sha MyPass ?
  access  specify an access-list associated with this group
  priv    encryption parameters for the user
  <cr>

R1(config)#snmp-server user UName1 G1 v3 auth sha MyPass priv ?
  3des  Use 168 bit 3DES algorithm for encryption
  aes   Use AES algorithm for encryption
  des   Use 56 bit DES algorithm for encryption

R1(config)#snmp-server user UName1 G1 v3 auth sha MyPass priv aes 256 ?
  WORD  privacy pasword for user

R1(config)#snmp-server user UName1 G1 v3 auth sha MyPass priv aes 256 PrivMyPa$
R1(config)#
```

Uygulamalı örnek vermek gerekirse aşağıdaki görselde;

- İlk satırda, 192.168.10.100 kaynak ip adresine izin veren Standart ACL tanımı yapıldı.
- İkinci satırda, SNMPView isimli View için 1.3.6.1.4.1.1991 değerinin kullanılabilir olması sağlandı.
- Üçüncü satırda G1 isimli grup çin okuma yetkisi verildi ve yapılabilecek sorguları kısıtlamak için oluşturulan View uygulandı. Son olarak da oluşturulan Standart ACL uygulanarak belirli ip adreslerinde gruba erişilebilmesi sağlandı.
- Dördüncü satırda, User1 isimli bir kullanıcı G1 isimli grup için tanımlanmıştır. Tanımlamada kullanılacak şifreleme algoritamları ve erişim için kullanılacak parola bilgileri tanımlanmıştır.

```
R1(config)#access-list 5 permit 192.168.10.100
R1(config)#snmp-server view SNMPView1 1.3.6.1.4.1.1991 included
R1(config)#snmp-server group G1 v3 priv read SNMPView1 access 5
R1(config)#snmp-server user User1 G1 v3 auth sha MyPass priv aes 128 PrivMyPass
```

NOT

- Bir SNMP Agent birçok SNMP Manager ile iletişim halinde olabilir. Bunun için SNMP Agent'ı SNMP'nin bütün versiyonlarıyla iletişim kuracak şekilde yapılandırmak mümkündür.