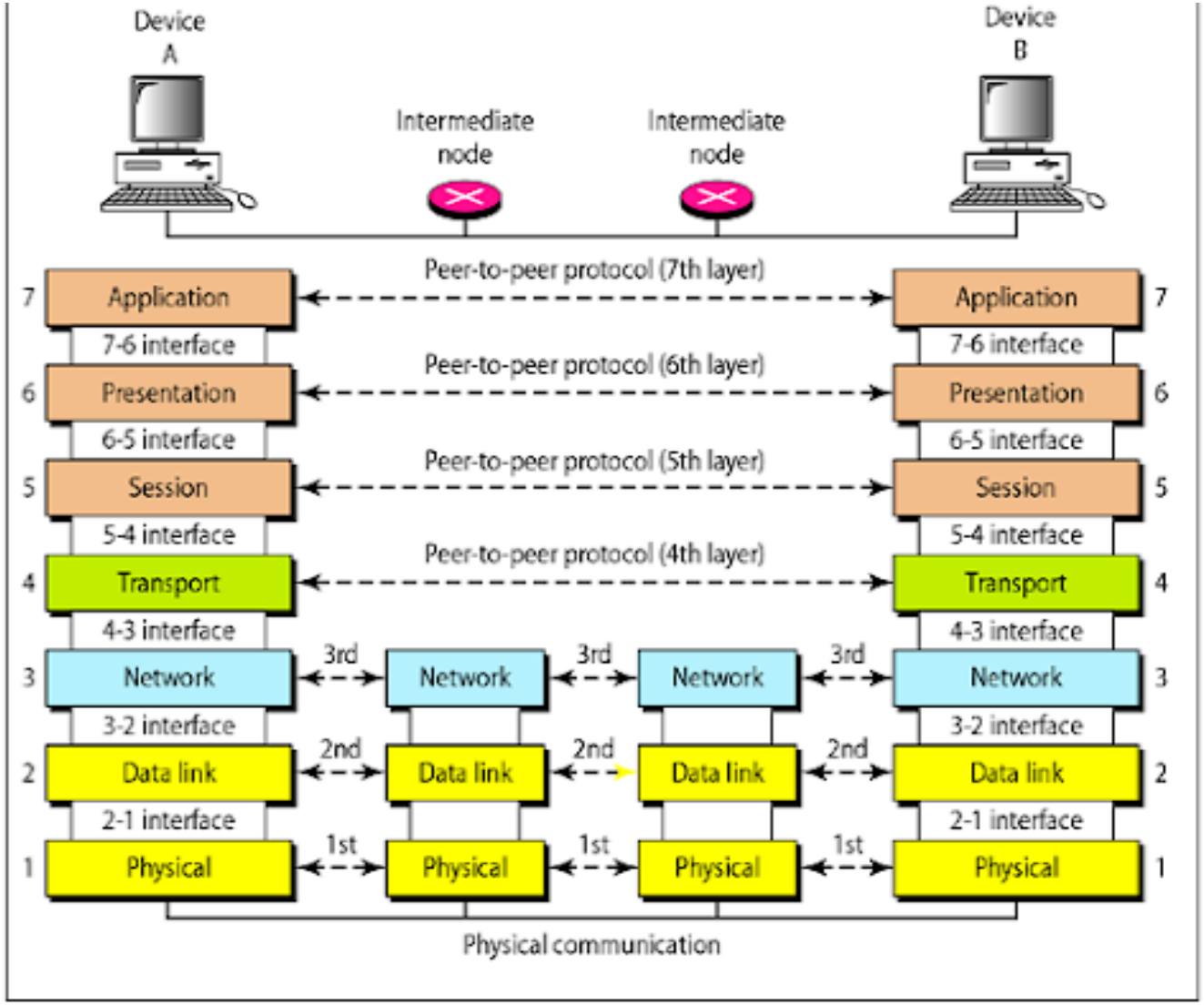
Uygulama Katmanı Protokolleri

(Basit Ağ Yönetim Protokolü)

OSI Referans Modeli Katmansal Gösterim



Basit Ağ Yönetim Protokolü (Simple Network Management Protocol-SNMP)

- Günümüz ağ topolojileri gerek büyüklükleri gerekse karmaşıklıklarından dolayı ağ yönetimini gerekli hale getirmişlerdir.
- Büyük ağlar, kendi kurumları için maliyet, zaman, performans, güvenilirlik ve güvenlik konularında çok önemli yere sahiptirler. Ancak yine aynı ağlar iyi yönetilemedikleri takdirde aynı başlıklar altında kurumlarına sıkıntı çıkarabilirler.
- Ağ yönetiminin 3 ana amacı vardır:
  - Ağın devamlılığı (çalışır halde tutmak)
  - Ağın performansını yönetmek
  - Maliyeti düşürme

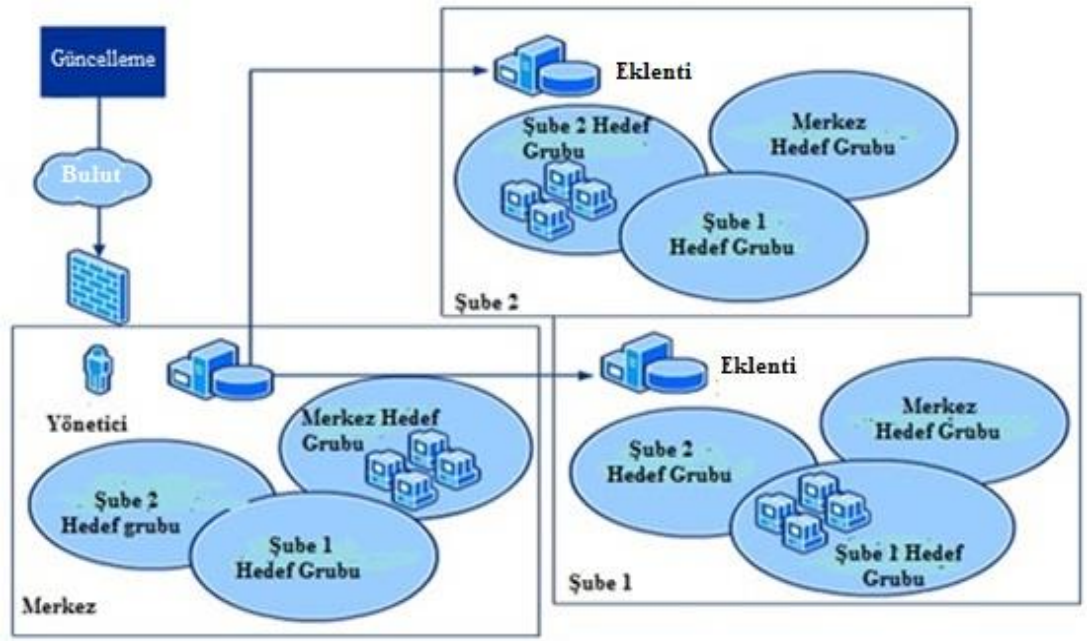
Basit Ağ Yönetim Protokolü (Ağ Yönetim Alanları)

- ISO tarafından kabul görmüş 5 büyük ağ yönetim alanı vardır. Bunlar sırasıyla aşağıda özetlenecektir:
  - Konfigürasyon Yönetimi
  - Oturum Yönetimi
  - Hata Yönetimi
  - Performans Yönetimi
  - Güvenlik Yönetimi

Basit Ağ Yönetim Protokolü (Ağ Yönetim Mimarileri)

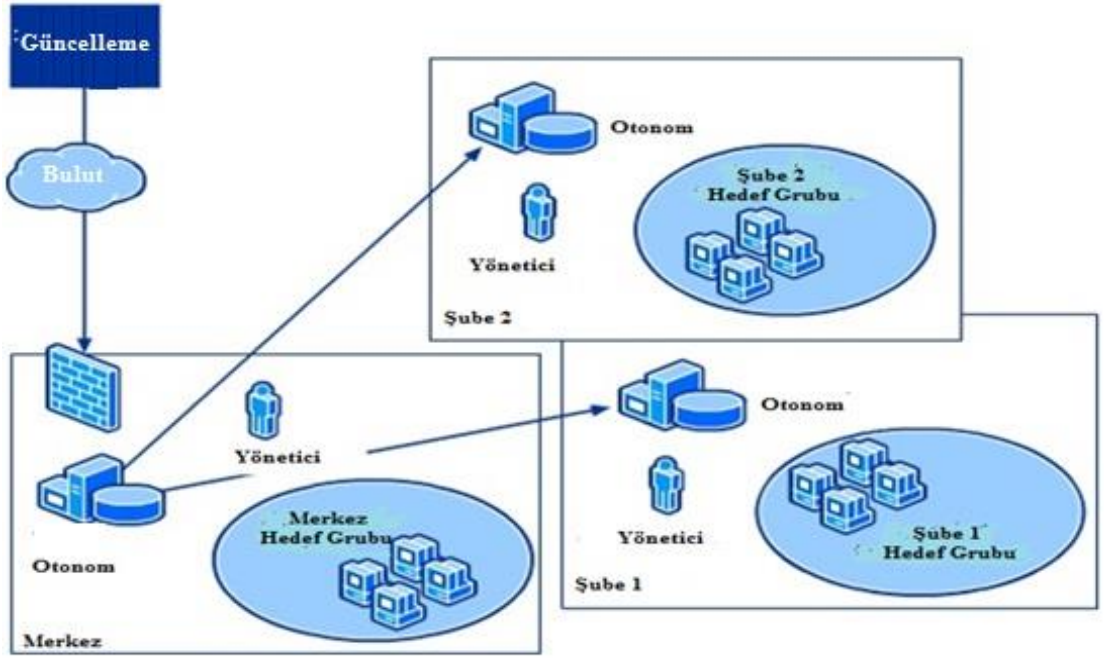
- Genel olarak ağ yönetim mimarilerini 3 ana başlık altında inceleyebiliriz:
  - Merkezi Yönetim
  - Dağıtık Yönetim
  - Hibrid Yönetim

Basit Ağ Yönetim Protokolü (Merkezi Yönetim)



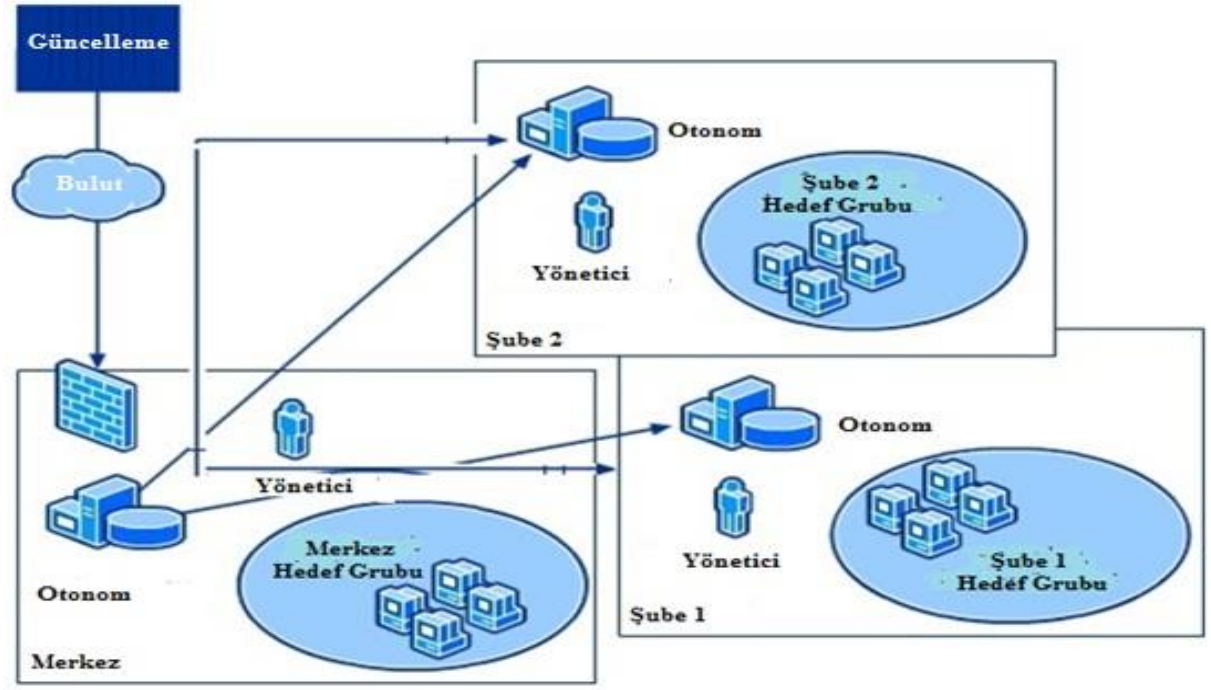
	Avantajlar	Dezavantajlar
1	Hataları ve durumları tek noktandan takip	Tek sistem yedek alma ve hata toleransı için yeterli değil
2	Ağ uygulamalarına ve bilgilere tek noktan erişim	Yeni sistem veya cihaz eklendiğinde, sistemi yenilemek zor olabilir.
3	Güvenlik daha kolay	Tüm istekler bir noktadan geçeceği için trafik yükü

Basit Ağ Yönetim Protokolü (Dağıtık Yönetim)



	Avantajlar	Dezavantajlar
1	Ağı yönetmek için bir çok sistem	Bilgi toplamak daha zor ve zaman kaybı fazla
2	Sistemin yedeği her zaman mevcut	Güvenlik açığı
3	Tek bir sistemdeki trafik yükü azalır.	Maliyet

Basit Ağ Yönetim Protokolü (Hibrid Yönetim)



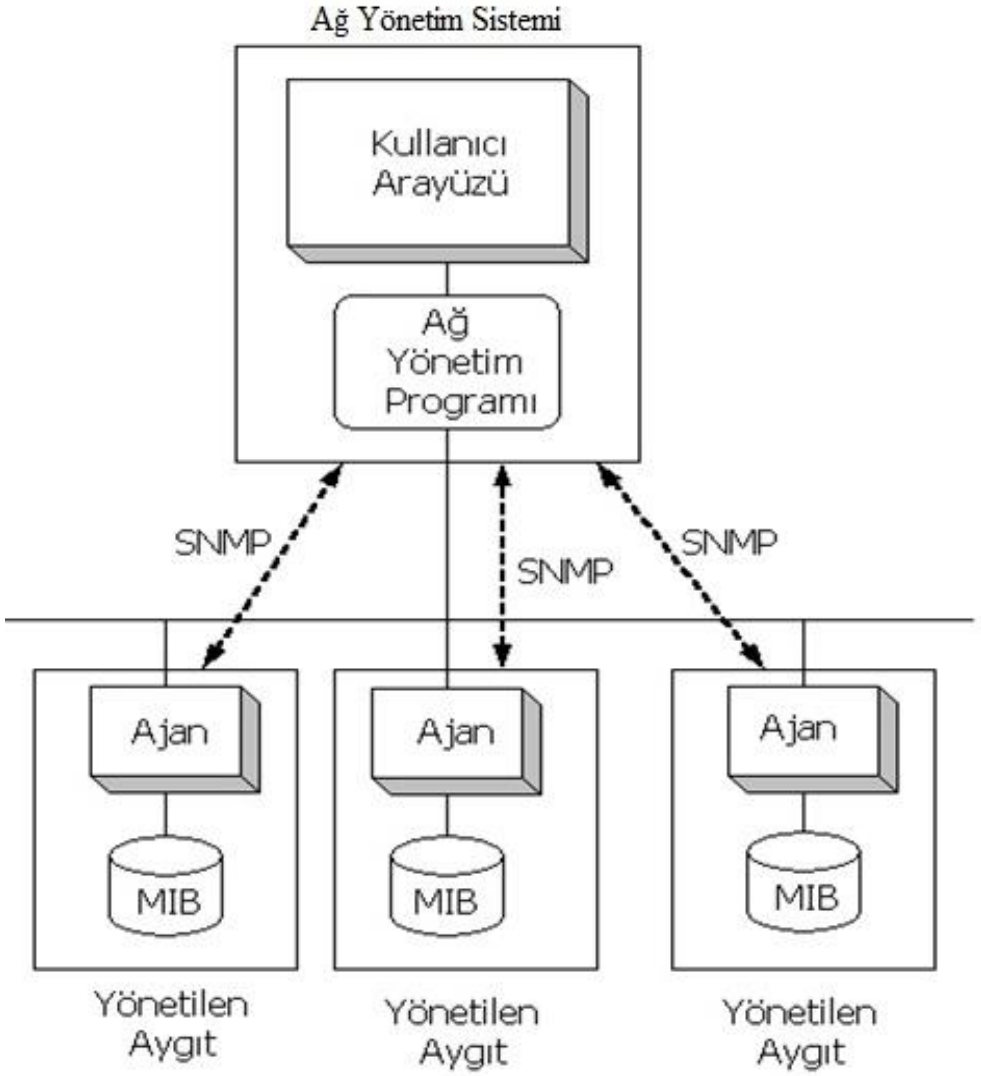
	Avantajlar	Dezavantajlar
1	Hataları ve durumları tek noktandan veya çok noktadan takip	Tüm sistemin manuel olarak tasarlanması gerekir.
2	Ağ uygulamalarına ve bilgilere kolay erişim	Çok erişim noktası olacağından güvenlik problemi
3	Yönetim daha kolay	Maliyet

Basit Ağ Yönetim Protokolü (SNMP)

- SNMP'inin ağ yönetimide sağlamış olduğu ***avantajlar şu şekildedir:***
  - Basit dizaynı kolay entegrasyon sağlıyor.
  - Kullanım alanı çok geniş
  - Güncelleme işlemi kolay
  - Artan gereksinimlere kolay adaptasyon
  - Bir standart olması
  - Genişletilebilir ve taşınabilir olması
  - Dağıtık ve merkezi yönetimi desteklemesi
- ***Dezavantaj olarak;***
  - UDP'yi kullandığından güvenilirlik düşük (son sürüm hariç)
  - Çok fazla ağ trafiği yaratır.

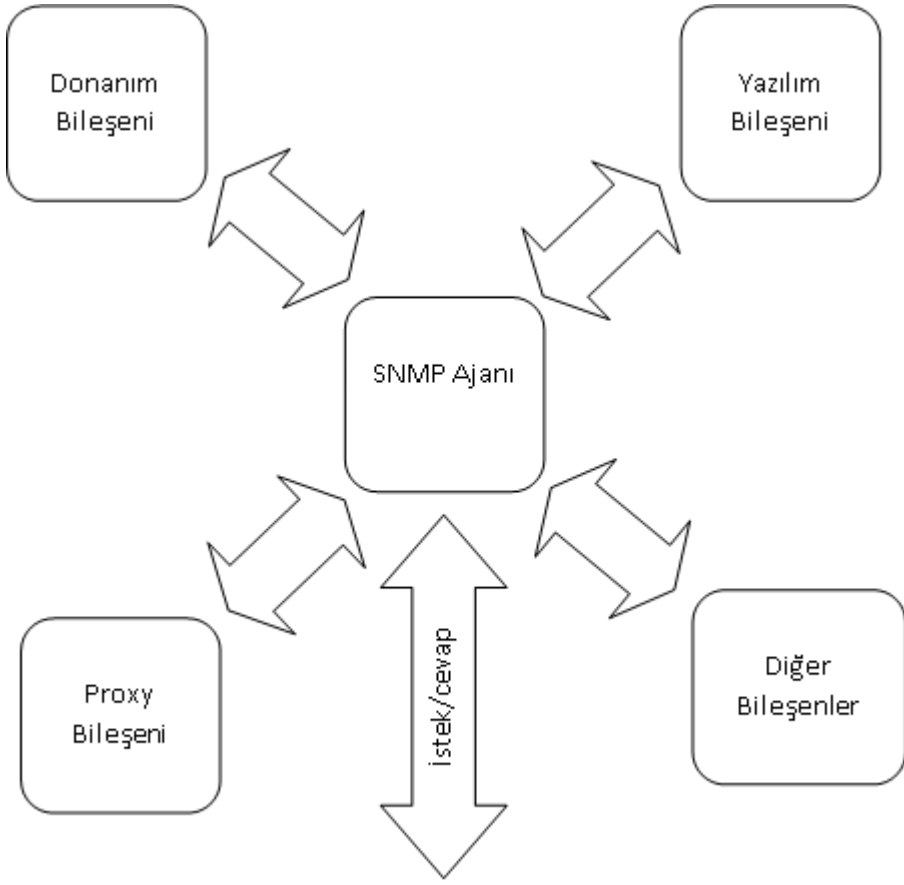
Basit Ağ Yönetim Protokolü (Mimari Yapı)

- SNMP mimarisi ağ yönetim sistemi, ajan ve yönetici kısmından oluşur;
- Üç temel bileşenden oluşan bu mimaride, mimarinin en alt seviyesinde cihazdan istenilen veriyi çekmeyi sağlayan ajan yazılımı bulunur.
- Orta seviyede ise ağ yönetim sistemi ile ajan arasındaki iletişimi kuran yönetici kısmı bulunur.
- Mimarinin en tepesinde ise tüm yönetim işlemlerinin yapıldığı ağ yönetim sistemi bulunur.



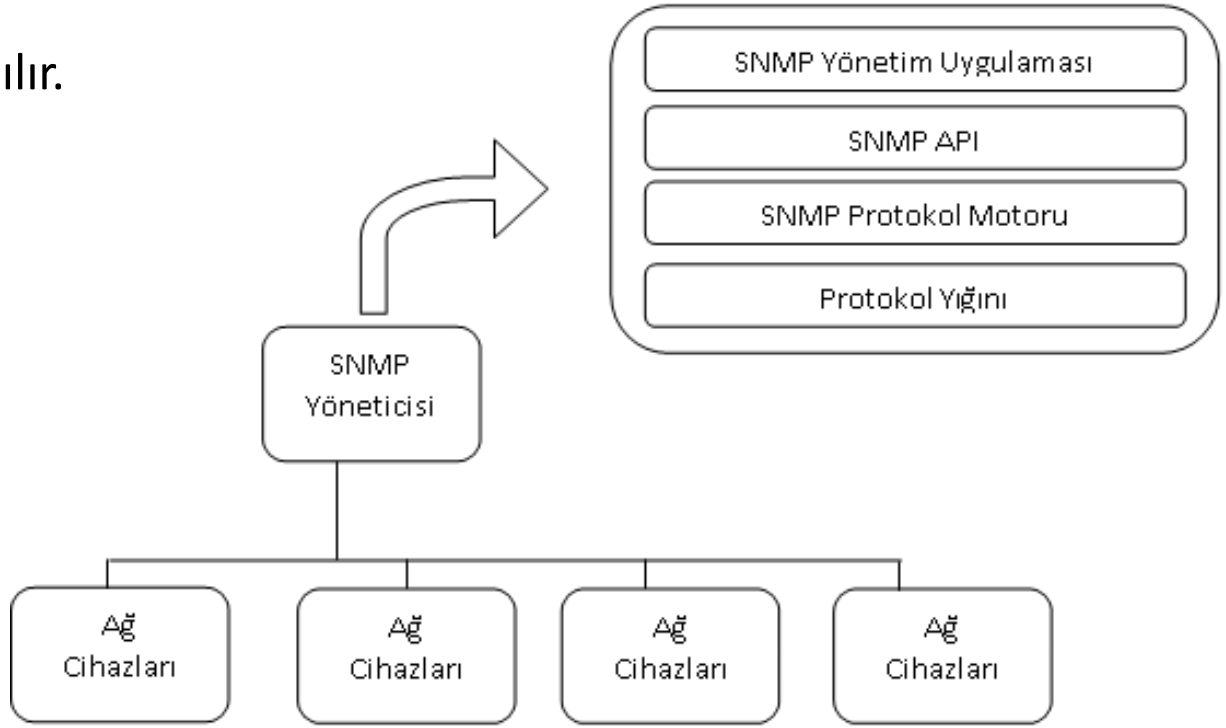
Basit Ağ Yönetim Protokolü (SNMP Ajanı)

- SNMP ajanı, kontrol veya takip edilen sistem düğümlerinden her birinde aktif edilen bir yazılımdır.
- Bu yazılım şekillendirmiş yapı içinde öğelerin her birine bir arayüz sağlar.
- Bu öğeler de yönetim bilgi tabanı dediğimiz MIB (Management Information Base, Yönetim Bilgi Tabanı)'lerde depolanır.
- Cihaz, üzerindeki tüm SNMP iletişimini kontrol eder.
- SNMP ajanı aktif edilmeden önce sistemin ne tarz bir ajana ihtiyacı olduğu tespit edilir. Bu da SNMP sürümü ile alakalıdır.



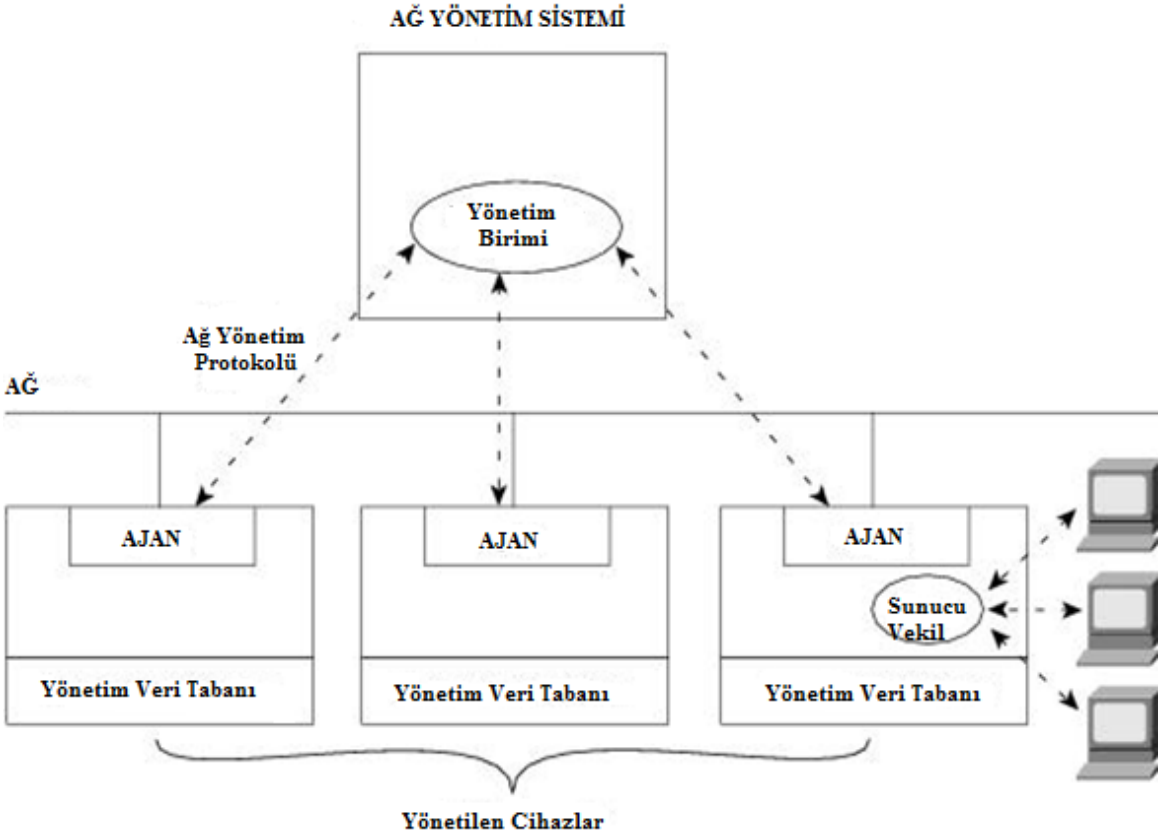
Basit Ağ Yönetim Protokolü (SNMP Yöneticisi)

- Ajan uygulamadan ihtiyaç duyulan bilgileri alıp kullanıcıya gösteren ve kullanıcının değiştirmek istediği değerleri cihaza gönderen yazılımdır.
- SNMP ajanına istek gönderir ve gerekli bildirimleri ve cevapları ajandan alır.
- SNMP yöneticisi istek gönderirken oturumlar açılır.



Basit Ağ Yönetim Protokolü (Ağ Yönetim Sistemi)

- Yönetici birimde çalışan ve bir ağa bağlı tüm cihazların izlenmesini ve yönetimini sağlayan uygulamaya verilen isimdir.
- SNMP ajanı ve SNMP yönetici arasındaki bilgi akışından iletişime kadar her türlü işlemi gerçekleştirir.



Basit Ağ Yönetim Protokolü (SNMP Sürümleri-SNMPv1)

- İlk SNMP sürümüdür. UDP, IP ve IPX protokolleri üzerinde çalışabilir.
- Çalışma mantığında ise SNMP, özetle bir sorgu-cevap protokolü olduğu için bu işlem, Get, GetNext, Set ve Trap komutları aracılığıyla olmaktadır.
- ***Get***, Ağ yönetim sistemi tarafından bir ya da daha fazla nesne bilgisi almak için kullanılır. Eğer yönetilen aygıt üzerinde çalışan ajan, istenen verilerin hepsini cevaplayamıyor ise ağ yönetim sistemine bir cevap yollamaz.
- ***Getnext işlemi*** tabloda yada ajan listesindeki bir sonraki değeri almak için kullanılır.
- ***Set işlemi*** ile yönetilen aygıtın MIB içerisindeki değerleri değiştirilebilir.
- ***Trap işlemi*** ise ağ yönetim sistemine, yönetilen aygıt tarafından oluşan değişiklikleri bildirmek için kullanılır.

Basit Ağ Yönetim Protokolü (SNMP Sürümleri-SNMPv2c)

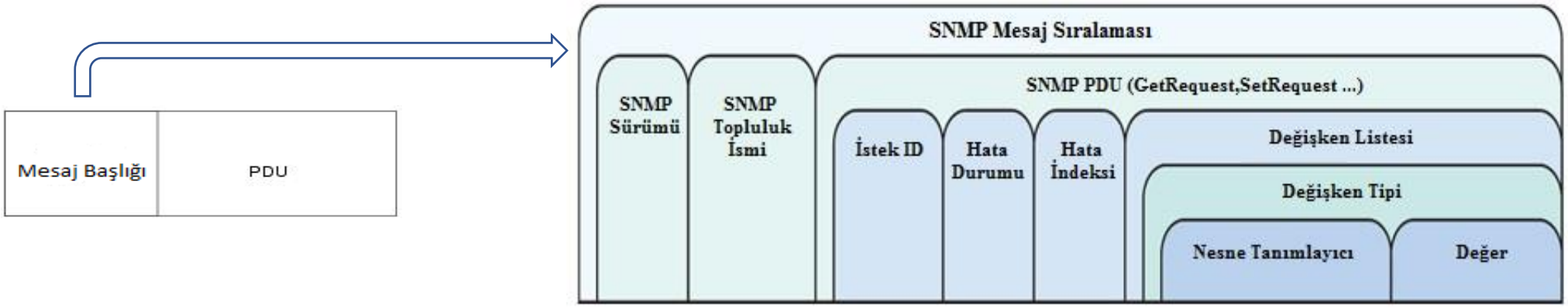
- SNMPv2'ye, SNMPv1'in evrimleştirilmiş hali diyebiliriz.
- Get, GetNext ve Set işlemleri SNMPv1 ile aynı olmasına rağmen SNMPv2'de trap işlemi biraz daha farklıdır. SNMPv2, v1'e göre iki yeni protokol işlemi daha içermektedir.
- ***GetBulk işlemi*** ile ağ yönetim sistemine büyük miktarda veri yollamak mümkündür. Eğer istenen veri bir paket boyutundan daha fazla ise ajan tarafından ard arda birkaç paket yollanır.
- ***Inform işlemi*** ise bir ağ yönetim sisteminin trap mesajlarını ağdaki başka bir ağ yönetim sistemine yollayabilmesi için kullanılır.
- SNMPv1'den farklı olarak eğer ajan yazılımı istenen değerlerin hepsini karşılayamıyorsa sisteme geri cevap döndürmemek yerine sadece sağlayabildiği mesajları gönderir.

Basit Ağ Yönetim Protokolü (SNMP Sürümleri-SNMPv3)

- SNMPv3 önceki sürümlere göre güvenlik açısından daha gelişmiş olan bir sürümüdür.
- SNMPv3'te güvenlik düzeyi kavramı ortaya çıkmıştır. Bu düzeyler;
  - **noAuthNoPriv (Kimlik denetimi ve şifreleme yok)**; v1 ve v2c'ye karşılık gelen güvenlik düzeyidir. Sadece kullanıcı adı bazlı şifreleme işlemleri yapar. Bu yapısından dolayı güvenli değildir.
  - **authNoPriv (Kimlik denetimi var, şifreleme yok)**; kimlik denetimini kullanıcı adı ve şifre bazlı yapmasının yanı sıra MD5 veya SHA algoritmalarını kullanarak veri bütünlüğü de sağlar.
  - **authPriv (Kimlik denetimi ve şifreleme var)**; DES, 3DES ya da AES algoritmasını kullanarak sadece aynı anahtara sahip alıcıların çözebileceği bir şekilde veriyi şifreler.

Basit Ağ Yönetim Protokolü (SNMP Paket Yapıları)

- SNMP, paket yapısı açısından genel itibariyle iki yapıdan oluşur: Mesaj başlığı ve PDU
- **SNMP Mesaj Başlığı;**
- SNMP mesaj başlığı da 2 alan içerir: Sürüm numarası ve topluluk (community) ismi
- **Sürüm numarası**: Kullanılan SNMP sürümünü tanımlar**.**
- **Topluluk ismi:** Ağ yönetim sistemleri için erişim alanı tanımlar. Topluluk isimleri doğrulama (authentication) mekanizması gibi çalışır.



Basit Ağ Yönetim Protokolü (SNMP Paket Yapıları-devam)

Alan	Tanımı	Boyutu
Snmp Mesajı Sıralaması	Snmp sürümünü, topluluk ismini ve Snmp PDU'sunu belirten Snmp mesaj sırasını belirtir.	2 byte
Snmp Sürümü	Hangi sürümün kullanıldığını belirtir. Şekil 2.11 ve 2.12'de gösterilmiştir.	3 byte
Snmp Topluluk İsmi	Snmp cihazlarına güvenlik ekleyebilmek ve onlara kolay erişebilmek için tanımlanan "octet string"dir. Şekil 2.11 ve 2.12'de gösterilmiştir.	8 byte
Snmp PDU	Snmp mesajının ana bölümünü oluşturur. Farklı protokol veri birimlerini (PDU) tanımlar. Aşağıda PDU çeşitleri ve nasıl bir çerçeve yapısı kullanıldığı ve nasıl bir işlev sunduğu ayrıca anlatılacaktır	2 byte
İstek ID	Belirli Snmp isteklerini tanımlar. Bu index, Snmp yöneticisine uygun isteğe dönen cevapı eşletirme izni verir, Snmp ajan yazılımdan dönen cevabın yansıması gibidir.	3 byte
Hata Durumu	Snmp yöneticisinden gönderilen isteğe 0x00 değeri atanır. Sistemde bir hata varsa Snmp ajanı bu alanı değiştirir. 0x00—Hata yok 0x01—Dönen cevap aktarım için büyük. 0x02—İstenen nesne bulunamadı. 0x03—istekteki veri tipi, Snmp ajanındaki veri tipiyle eşleşmiyor. 0x04—Snmp yöneticisi sadece okuma parametresi atadı. 0x05—Genel Hata	3 byte
Hata İndeksi	Hata olursa, hataya neden olan nesne işaretlenir, diğer taraftan hata indeksi 0x00	3 byte
Değişken Listesi	Bu alanda SNMP PDU çeşidine göre veya uygulama alanına göre farklı değişkenler alabilir.	2 byte
Değişken Tipi	İki alandan oluşur. OID ve OID'nin değeri	2 byte
Nesne Tanımlayıcı (OID)	Snmp ajanındaki parametreleri ifade eder.	12 byte
Değer	SetRequest PDU – Değer, Snmp ajanındaki belirtilen OID'ye atanır. GetRequestPDU – Değeri boştur, dönen verinin izi gibi davranır. GetResponsePDU – Snmp ajanından belirtilen OID'den dönen değerdir.	2 byte

Basit Ağ Yönetim Protokolü (SNMP Paket Yapıları-devam)

- SNMP protokol veri birimi çerçeve yapısı (PDU çeşidine göre farklılık gösterebilir);

- PDU Çeşitleri;
  - GetRequest PDU
  - GetNextRequest PDU
  - SetRequest PDU
  - GetResponse PDU
  - Trap PDU

Basit Ağ Yönetim Protokolü (PDU Çeşitleri)

- **GetRequest PDU:** Ağ yönetim sisteminin nesne tanımlayıcıları (OID) çekmek için ajan yazılımına gönderdiği PDU çeşididir.
- **GetNextRequest PDU:** Belirtilen sonraki OID değerini almak için ağ yönetim sisteminden, ajan yazılıma gönderilen PDU çeşididir.
- **SetRequest PDU:** Ağ yönetim sisteminden, ajana OID değerleri atamak için kullanılır.
- **GetResponse PDU:** Ajandan, ağ yönetim sistemine gönderilen cevaplardır.
- **Trap PDU:** Ajandan, ağ yönetim sisteminin seçili olan modülüne gönderilen bildirimlerdir. Cihazda hata varsa, hata bildirimin sadece ağ yönetim sisteminin hata yönetim modülüne gönderilmesi gibi.

Basit Ağ Yönetim Protokolü (SNMP Paket Yapıları-devam)

- ***SNMPv1 için;***
- Get/GetNext/Set PDU ayynı paket yapısına sahip oldukları için aynı PDU çerçeve yapısında gösterilmiştir.

Get/GetNext/Set PDU

PDU Tipi	İstek ID	0	0	Değişken Listesi

Response PDU

PDU Tipi	İstek ID	Hata Durumu	Hata İndeksi	Değişken Listesi

Trap PDU

PDU Tipi	Cihaz Tipi	Ajan Adresi	Genel trap	Özel trap	Geçen Süre	Değişken Listesi

Değişken Listesi

İsim1	Değer1	İsim2	Değer2	.....	İsimx	Değerx

Basit Ağ Yönetim Protokolü (SNMP Paket Yapıları-devam)

- ***SNMPv2c için;***

- SNMPv1'deki PDU çeşitlerine ek olarak SNMPv2c'nin desteklemiş olduğu PDU çeşitleri şu şekildedir:

GetBulk PDU

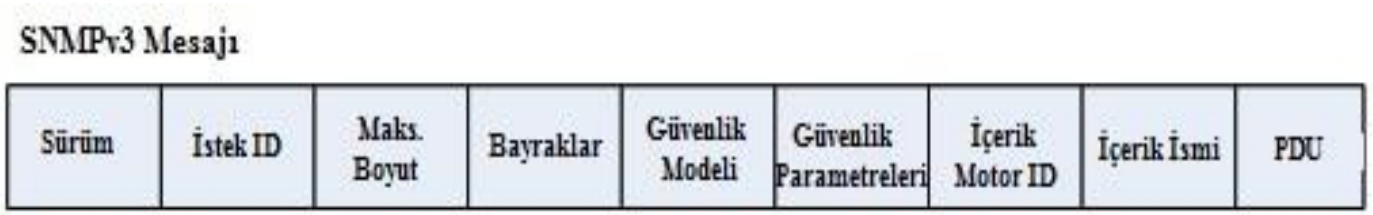
PDU Tipi	İstek ID	Tekralayıcı Yok	Maksimum Tekrar	Değişken Listesi

Trap PDU (SNMPv2c)

				Değişken Listesi				
PDU Tipi	İstek ID	0	0	sysUp Time.0	Değer1	snmpTrap OID.0	Değer2	.....

Basit Ağ Yönetim Protokolü (SNMP Paket Yapıları-devam)

- ***SNMPv3 için;***
- SNMPv3'ün paket yapısı diğer sürümlere göre değişiklik göstermektedir. Güvenlik mekanizması nedeniyle paket yapısına güvenlik modeli, güvenlik parametreleri gibi yeni alanlar eklenir.



Basit Ağ Yönetim Protokolü (SNMPv3 PDU Alanları)

Alan	Tanımı
Maksimum Boyut	Gönderilen maksimum mesaj boyutu
Bayraklar	0x0 - Doğrulama ve gizlilik yok 0x1 – Doğrulama var, gizlilik yok 0x3 – Doğrulama ve gizlilik var 0x4 – Bir tane PDU raporu gönderir.
Güvenlik Modeli	Güvenlik modelini ifade eder. 0 – Güvenlik modeli yok. 1-SNMPv1 güvenlik modeli 2-SNMPv2c güvenlik modeli 3-SNMPv3 güvenlik modeli
İçerik Motor ID	Her işlem için özgün bir SNMP girdisi tanımlar.
İçerik İsmi	İçerik ismi tanımlar. Her isim içeri motor ID ile eşleştirilmelidir.
Güvenlik Parametreleri	Yetkilendirme Motor ID: SNMP motorunu yetkilendirerek SNMP Motor ID'yi özeleştirir. Yetkilendirme Motor Çalışması: Yetkilendirilmiş Motor ID'sinin çalışmasını özeleştirir. Yetkilendirme Motor Zamanı: Bir zaman değeri atar. Kullanıcı Adı: Bir kullanıcı adı atar. Ağ yönetim sistemi ve ajan aynı isimde olmalı. Doğrulama Parametresi: Doğrulama mekanizması için bir anahtarlama kullanır. Gizlilik Parametresi: Gizlilik mekanizması için parametre kullanır. DES, AES gibi algoritmalar kullanılır.

Basit Ağ Yönetim Protokolü (SNMP Çalışma Mekanizması)

- SNMP'nin çalışma mekanizması istek gönderme ve isteğe cevap alma şeklindedir ve bunun için taşıma katmanında kullandığı protokol UDP'dir.
- Ağ yönetim sistemi, istekleri herhangi bir portundan, ajanın 161. portuna gönderir. Ajan geri bildirim için kendisine gelen istekleri 162. portundan gönderdiği cevaplarla sağlar.
- SNMP ajan yazılımı, cihazda herhangi fiziksel bir sorun oluştuğunda (cihaz üzerindeki fiziksel değerlere atanan değerlerin üzerine çıkıldığı zaman veya periyodik olarak veri gönderimi yapmak için ayarlandığı zaman) iletişimini kendi başlatır.
- SNMP sayesinde bir cihazdan bilgi alınabileceği gibi, cihazdaki bilgi değiştirilebilir ve cihazda yeni bir yapılandırma uygulanabilir. Örneğin cihaz baştan başlatılabilir, cihaza bir yapılandırma dosyası gönderilebilir ya da cihazdan alınabilir.

Basit Ağ Yönetim Protokolü (MIB Kavramı)

- MIB kavramı bir ağaç yapısına benzetilebilir. Ulaşılmak istenen değeri tutan değişkene OID (Object IDentifier, Nesne Tanımlayıcısı) adı verilir. MIB yapısındaki sıralamaya göre değer alır.
- Her kuruluşun, "**Internet Engineering Task Force *(IETF)*"** tarafından atanan bir değeri vardır, yani belirli bir yere kadar ağaç yapısı evrenseldir, ancak kurumların kendi kullanacakları yönetim nesneleri için bu kodu her kurum kendi tanımlar.
- Bu değişkenler ağacın dallarının en uç noktasında olup bir cihazla ilgili tek bir değeri tutabileceği gibi kendisinden sonra gelen bütün alt dalları ifade etmek için de kullanılabilir. Kökten ağaç dalına uzanan bu hiyerarşi birbirlerinden nokta ile ayrılmış sayı dizileriyle ifade edilir.

Basit Ağ Yönetim Protokolü (MIB Kavramı-devam)

- Şekil'de, OID değeri "1.3.6.1.2.1.1.5" olan "sysName" değeri ağaç yapısında gösterilmiştir.
- Buradaki ilk girdi de sysName.0 olarak adlandırılır. Yani komutta 1.3.6.1.2.1.1.5.0 yerine sysName.0 yazılırsa da aynı işlevi görür.
- Değişkenin başındaki ilk dört sayı, yani 1.3.6.1 standarttır. Bu noktadan sonra ulaşmak istediğimiz bilgiye göre alt dallara ilerlenir.
- Örneğin 1.3.6.1.2.1.1 dalı sistemle ilgili sistem adı, sistem tanımı, sistemin ayakta olduğu süre gibi değerleri tutar. Bunun alt dalı olan 1.3.6.1.2.1.1.5.0 değişkeni bunlardan biridir (sistem adı).