

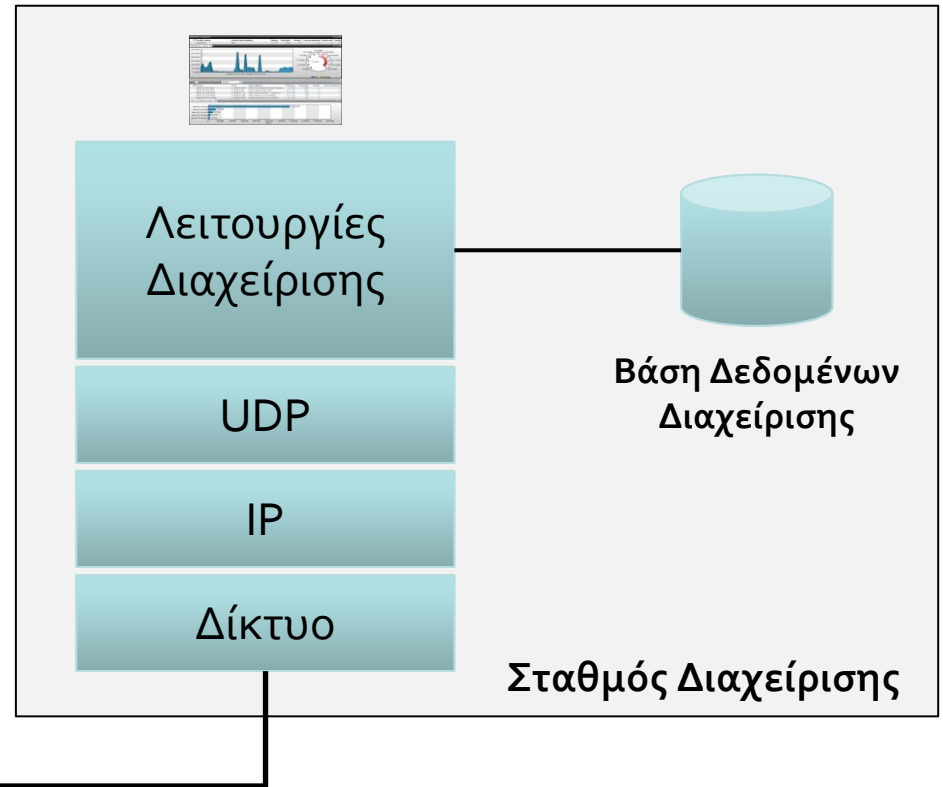
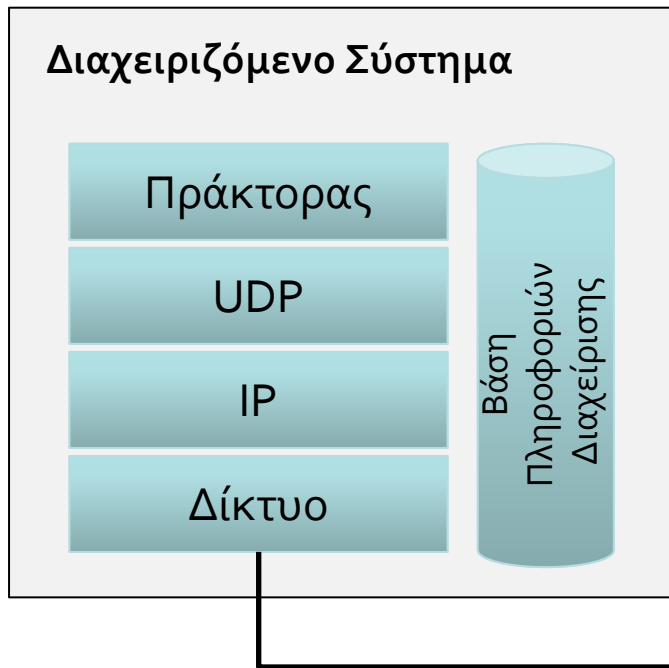


**Πανεπιστήμιο Πελοποννήσου**  
**Τμήμα Επιστήμης και Τεχνολογίας Τηλεπικοινωνιών**

**Διαχείριση και Ασφάλεια Δικτύων**

**Το Πρωτόκολλο SNMP**

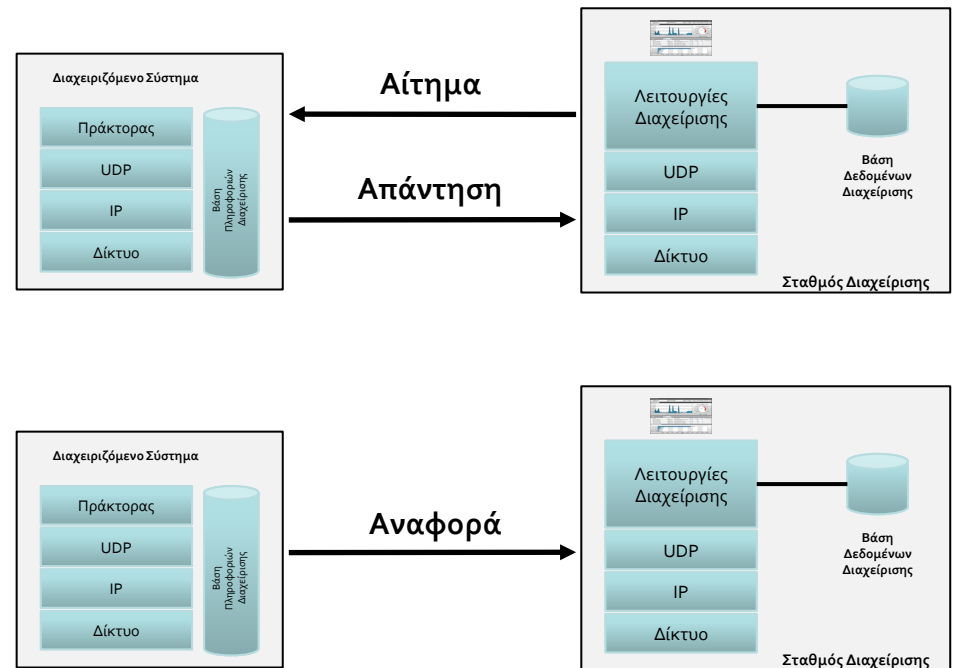
# Διαχειριστής και διαχειριζόμενος



# Μοντέλο λειτουργίας

- Ακολουθείται το μοντέλο πελάτη – εξυπηρετητή (client – server) ή αλλιώς...  
διαχειριστή – πράκτορα (manager – agent)

- Δύο τρόποι συλλογής πληροφοριών:
  - Ερώτηση & απάντηση
  - Αναφορά γεγονότων

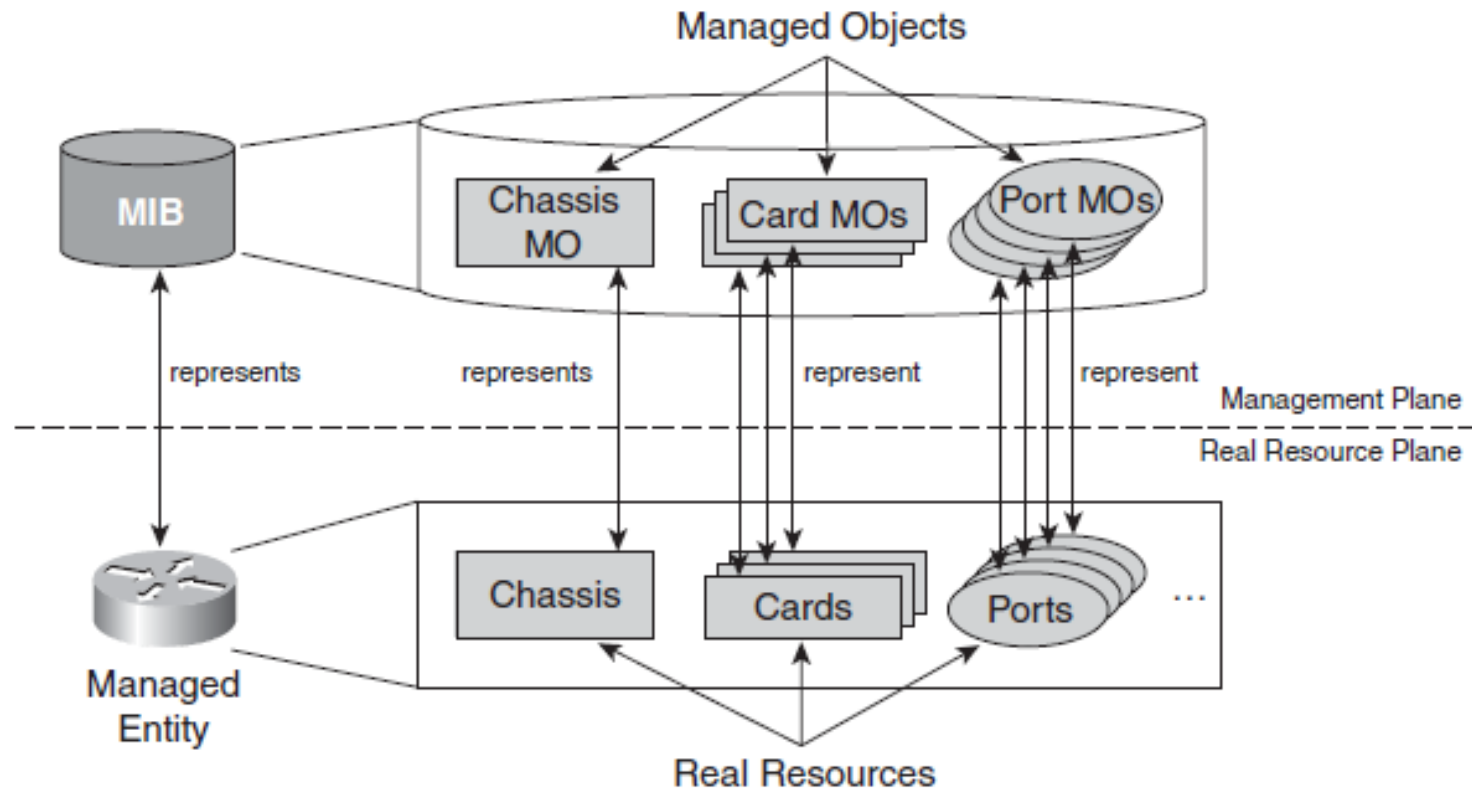


# Βάση πληροφοριών διαχείρισης

- Management Information Base (MIB)
- Ορίζει τη «σημασιολογική γλώσσα» ούτως ώστε οι διαχειριστές και οι διαχειριζόμενοι να μπορούν να συνεννοηθούν
- Αποτελεί μία αφαιρετική απεικόνιση των διαχειριζόμενων αντικειμένων
  - Παρέχει το «σχήμα» της οργάνωσης της πληροφορίας
  - ... αλλά, η MIB **ΔΕΝ** αποθηκεύει η ίδια δεδομένα!
- Σύνταξη βάσει της Δομής Πληροφοριών Διαχείρισης (Structure of Management Information – SMI)
- Μολονότι εξετάζουμε τις MIBs στο πλαίσιο του SNMP και σε σχέση με το SNMP, στην πραγματικότητα οι MIBs αποτελούν γενική προσέγγιση



# Η MIB ως αφαίρεση



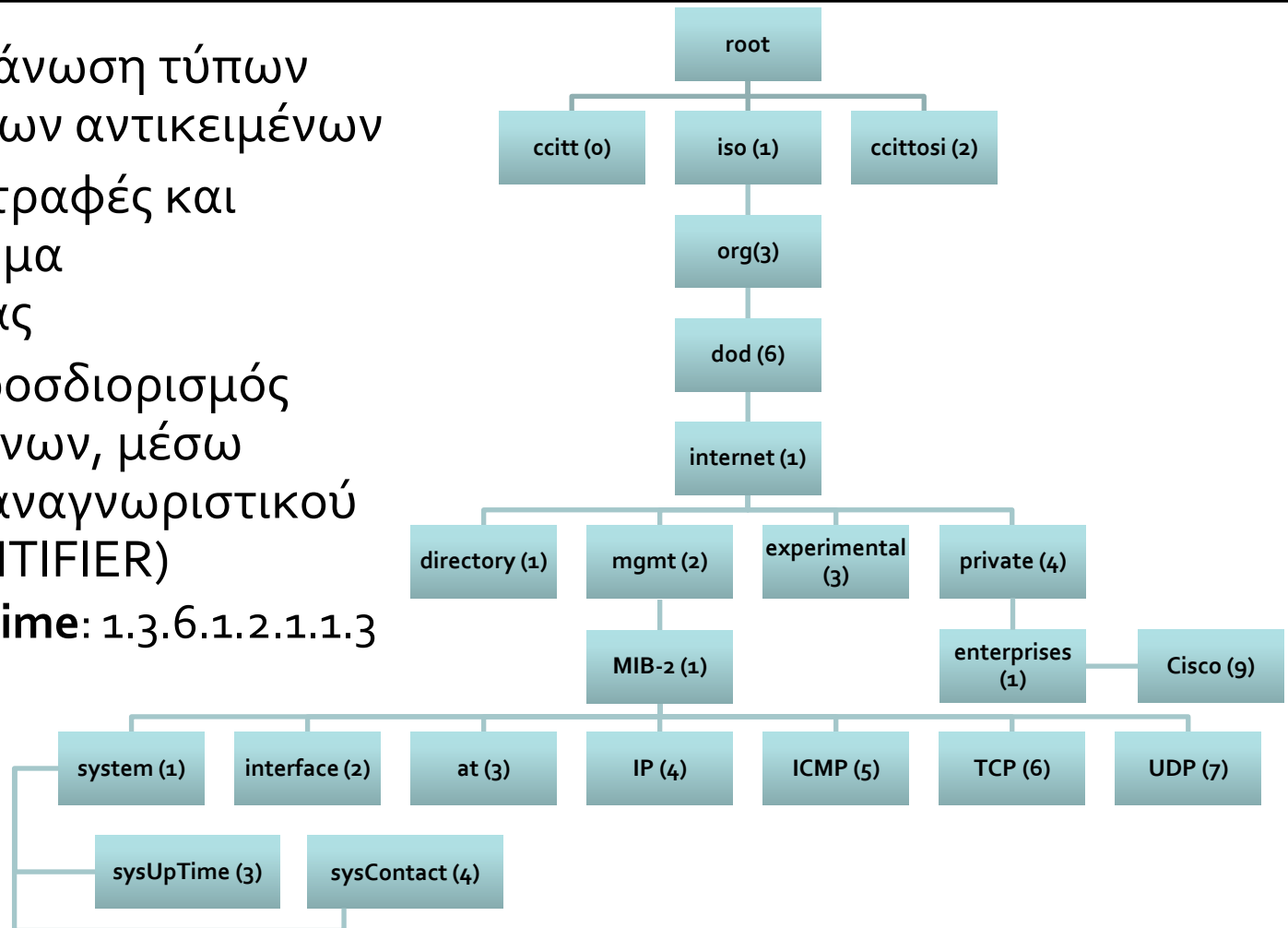
# Πληροφορίες διαχείρισης

- Πληροφορίες κατάστασης
  - π.χ., εάν κάποια ζεύξη είναι ενεργή ή όχι
- Πληροφορίες φυσικής διαμόρφωσης
  - π.χ., τι κάρτες διαθέτει μία συσκευή, ποιες είναι οι MAC διευθύνσεις των δικτυακών καρτών...
- Πληροφορίες λογικής διαμόρφωσης
  - π.χ., IP διευθύνσεις
- Ιστορικές πληροφορίες
  - π.χ., πόσα πακέτα πέρασαν τα τελευταία ~10', πόσα πακέτα χάθηκαν...



# Οργάνωση MIB

- Δενδρική οργάνωση τύπων διαχειριζόμενων αντικειμένων
- Αντικειμενοστραφές και ιεραρχικό σχήμα ονοματοδοσίας
- Μοναδικός προσδιορισμός των αντικειμένων, μέσω αριθμητικού αναγνωριστικού (OBJECT IDENTIFIER)
  - π.χ. **sysUpTime**: 1.3.6.1.2.1.1.3



# Σύνταξη αντικειμένων διαχείρισης

- Με βάση τη Structure of Management Information (SMI)
  - Version 1 (SMIv1) [RFC 1155, 1990]
  - Version 2 (SMIv2) [RFC 2578, 1999]
- Γενική δομή:

**<όνομα> OBJECT-TYPE**

**SYNTAX**

<τύπος αντικειμένου>

**ACCESS**

<τύπος πρόσβασης>

**STATUS**

<κατάσταση του  
αντικειμένου>

**DESCRIPTION**

<περιγραφικό κείμενο>

**::= {<θέση αντικειμένου>}**





# Παράδειγμα: ipForwDatagrams

## ipForwDatagrams OBJECT-TYPE

SYNTAX Counter

ACCESS read-only

STATUS mandatory

### DESCRIPTION

"The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route option processing was successful."

::= { ip 6 }

root

iso (1)

org(3)

dod (6)

internet (1)

mgmt (2)

MIB-2 (1)

IP (4)

ipForwDatagrams (6)



# Στιγμιότυπα αντικειμένων

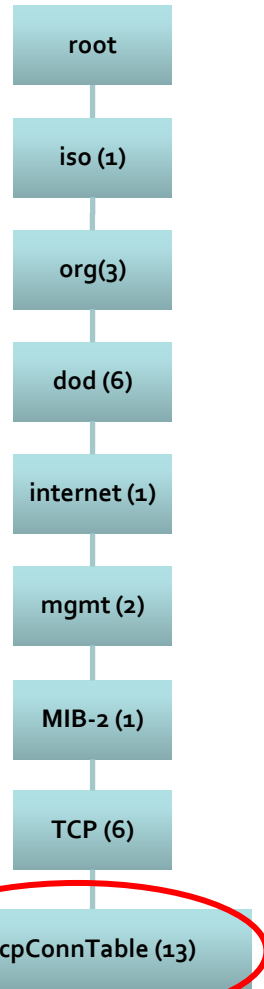
- Στιγμιότυπα (instances): τα “πραγματικά” αντικείμενα πίσω από τις αφαιρέσεις
- Δύο τύποι αντικειμένων:
  - Μονόμετρα ή βαθμωτά (scalars): ένα στιγμιότυπο ανά αντικείμενο  
π.χ., ο αριθμός των ενεργών TCP συνδέσεων
  - Στήλης (columnar): πολλαπλά στιγμιότυπα ανά αντικείμενο  
π.χ., οι ενεργές TCP συνδέσεις



# Παράδειγμα: tcpConnTable

```
tcpConnTable OBJECT-TYPE
    SYNTAX SEQUENCE OF TcpConnEntry
    ACCESS not-accessible
    STATUS mandatory
    DESCRIPTION
        "A table containing TCP connection-specific
        information."
    ::= { TCP 13 }
```

```
tcpConnEntry OBJECT-TYPE
    SYNTAX TcpConnEntry
    ACCESS not-accessible
    STATUS mandatory
    DESCRIPTION
        "Information about a particular current TCP
        connection. An object of this type is transient,
        in that it ceases to exist when (or soon after)
        the connection makes the transition to the CLOSED
        state."
    INDEX { tcpConnLocalAddress,
            tcpConnLocalPort,
            tcpConnRemAddress,
            tcpConnRemPort }
    ::= { tcpConnTable 1 }
```



# Αναγνωριστικά στιγμιοτύπων

- Για μονόμετρα αντικείμενα: προσθέτουμε το 0 , π.χ.:
  - Αντικείμενο **sysUpTime**: 1.3.6.1.2.1.3
  - Στιγμιότυπο **sysUpTime**: 1.3.6.1.2.1.3.0
- Για αντικείμενα στήλης:  
λίγο πιο πολύπλοκο!

π.χ.: 1.3.6.1.2.6.13.1.1.  
167.8.15.92.227.  
176.15.53.216.228

1.3.6.1.2.6.13.1

tcpConnEntry

1	2	3	4	5
tcpConn State (1)	tcpConn LocAddr (2)	tcpConn LocPort (3)	tcpConn RmtAddr (4)	tcpConn RmtPort (5)
167.8.15.92.227. 176.15.53.216	estab	167.8.15.92	227	176.15.53.216 228
167.8.15.92.235. 176.15.53.218	estab	167.8.15.92	235	176.15.53.218 240
167.8.15.92.236. 178.67.124.15	closing	167.8.15.92	236	178.67.124.15 196
167.8.15.92.244. 181.33.16.4	estab	167.8.15.92	244	181.33.16.4 227



# Βασικοί τύποι δεδομένων

- INTEGER
- Integer32
- Unsigned32
- OCTET STRING
- Gauge32
- OBJECT IDENTIFIER
- IpAddress
- Counter32
- Counter64
- BITS
- Opaque
- TimeTicks
- SEQUENCE



# Δικαιώματα πρόσβασης

## SNMPv1

- read-only
- read-write
- write-only
- not-accessible

## SNMPv2

- read-only
- read-write
- read-create
- accessible-for-notify
- not-accessible



# Βασικά μηνύματα SNMP

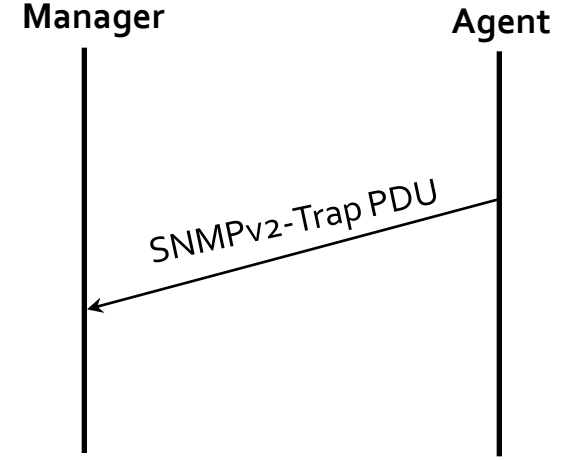
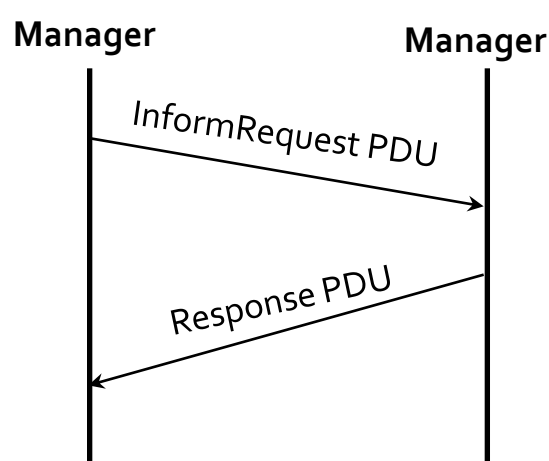
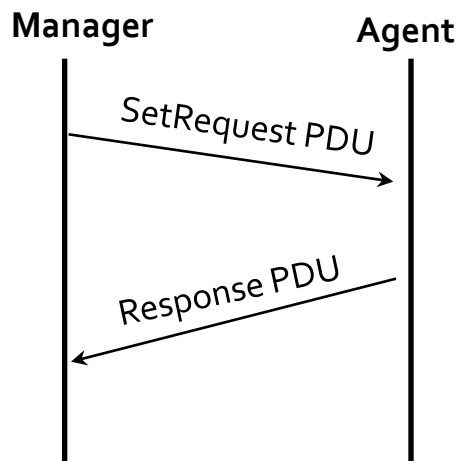
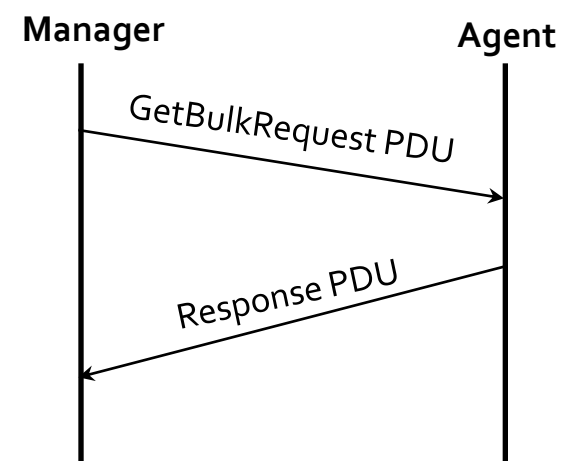
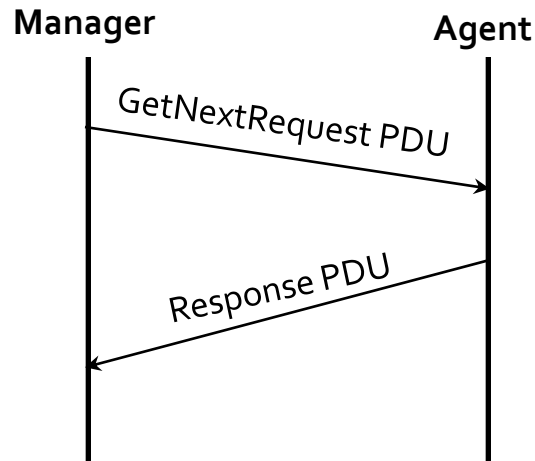
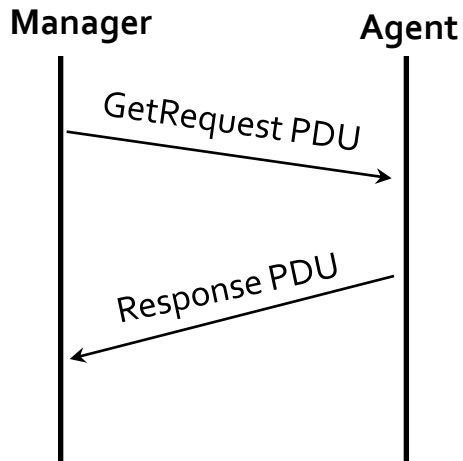
- GetRequest
- GetNextRequest
- GetBulkRequest (v2+)
- SetRequest
- GetResponse
- InformRequest (v2+)
- Trap

## Traps:

- coldStart
- warmStart
- linkDown
- linkUp
- authenticationFailure
- egpNeighborLoss
- enterpriseSpecific

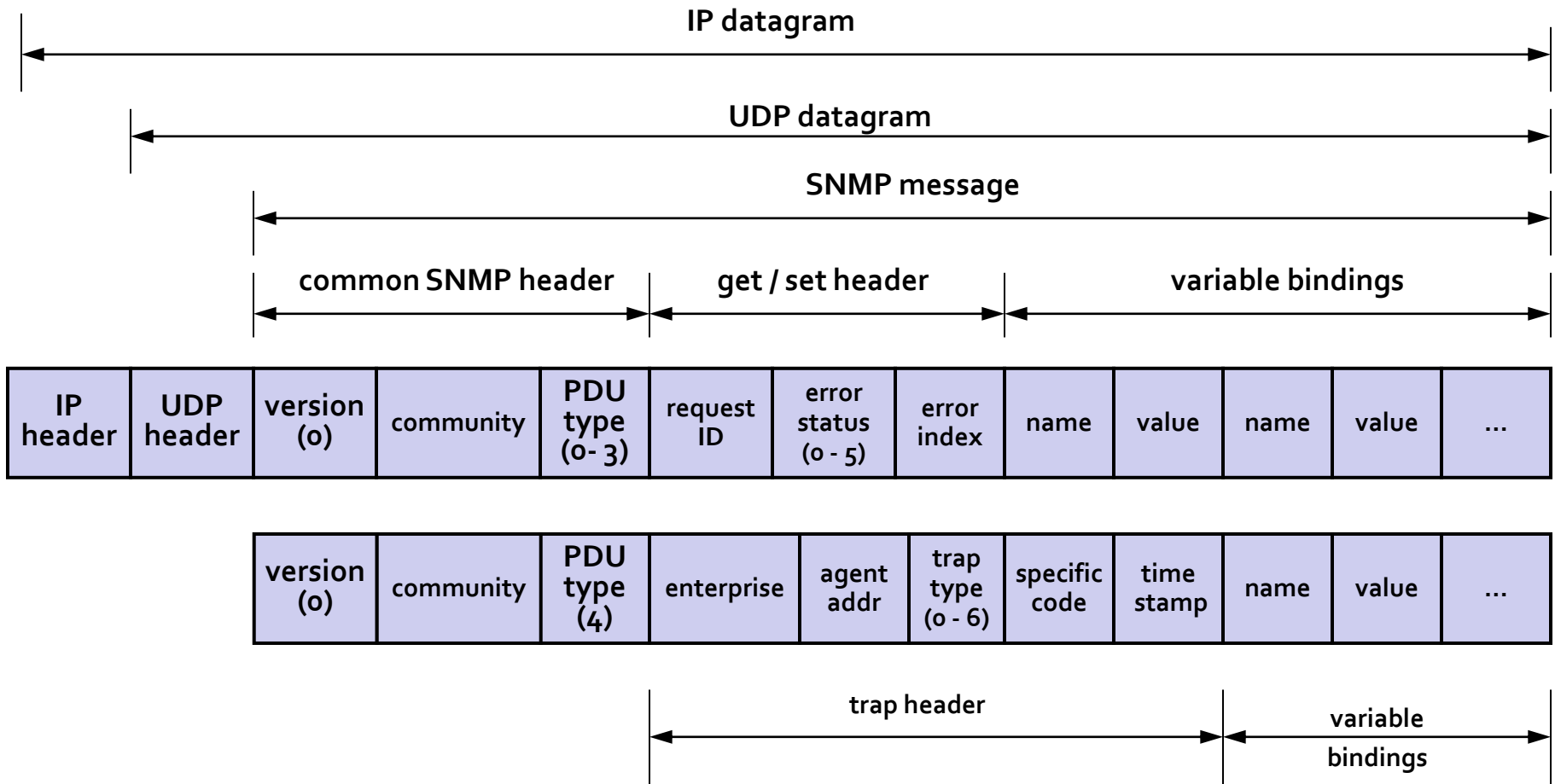


# Αλληλουχία μηνυμάτων





# Δομή μηνυμάτων SNMP



# Διαχείριση επιδόσεων

- Η διαδικασία μέτρησης της επίδοσης όλων των στοιχείων του δικτύου
- Επιτρέπει στο διαχειριστή:
  - να μπορεί να αντιμετωπίσει βραχυπρόθεσμα προβλήματα
  - να παρατηρήσει μακροπρόθεσμες τάσεις του δικτύου
- Η διαχείριση επιδόσεων απαιτεί την εξέταση στατιστικών μεγεθών σε ένα συγκεκριμένο χρονικό διάστημα, που μπορεί να κυμαίνεται από δευτερόλεπτα έως και μήνες
- Ο υπολογισμός της μεταβολής ενός στατιστικού μεγέθους από τη χρονική στιγμή  $t_0$  έως  $t_1$  δίνεται από τη σχέση

$$X(t_1) - X(t_0) / t_1 - t_0$$



# Παράδειγμα

- **ifInOctets:**  
Συνολικός αριθμός bytes που έλαβε μία φυσική σύνδεση
- **ifSpeed:**  
Χωρητικότητα σε Kbps μίας φυσικής σύνδεσης

- Χρησιμοποίηση (π.χ., σε σύνδεση Ethernet):

$$8 * ((\text{ifInOctets}(t_1) - \text{ifInOctets}(t_0)) / ((t_1 - t_0) * \text{ifSpeed}))$$

