Ασφάλεια Δικτύων και Επικοινωνιών

(Network and Communication Security)

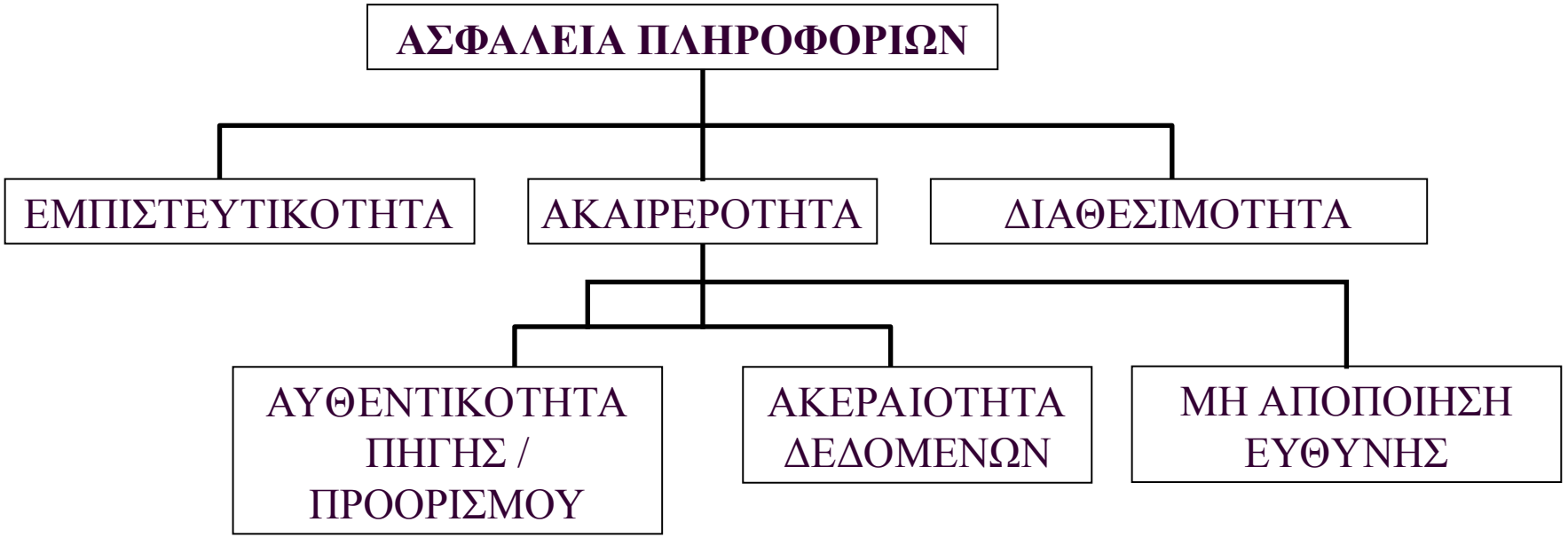
1. *Πρωτόκολλα δικτύων και πρότυπα ασφάλειας*
2. *Ασφάλεια στο Επίπεδο Δικτύου* (IPSec)
3. Εφαρμογή IPSec

Αν.Καθ. Παναγιώτης Κοτζανικολάου

ΠΜΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΕΠΙΣΤΗΜΗ ΔΕΔΟΜΕΝΩΝ

1. Εισαγωγή – Πρότυπα Ασφάλειας Δικτύων

Ασφάλεια Πληροφορίας



Ασφάλεια Υπολογιστικών Συστημάτων

- Η προστασία των **πληροφοριακών αγαθών** ή **παγίων** (*information assets*) από απειλές ασφάλειας.
  - **Απειλή ασφάλειας** (security threat): κάθε γεγονός που μπορεί να βλάψει ένα αγαθό.
  - **Επίθεση ασφάλειας** (security attack): Η εκδήλωση μίας απειλής
  - **Συνέπεια** (impact): η έκταση της απώλειας που θα προκληθεί στο αγαθό ή στον ιδιοκτήτη του αγαθού, εφόσον η απειλή πραγματοποιηθεί.
  - **Αδυναμία ασφάλειας** (vulnerability): κάθε χαρακτηριστικό το οποίο κάνει ένα αγαθό περισσότερο ευάλωτο σε μία ή περισσότερες απειλές.
  - **Επικινδυνότητα ή κίνδυνος** (security risk). Συνδυασμός των συνεπειών, απειλών και αδυναμιών

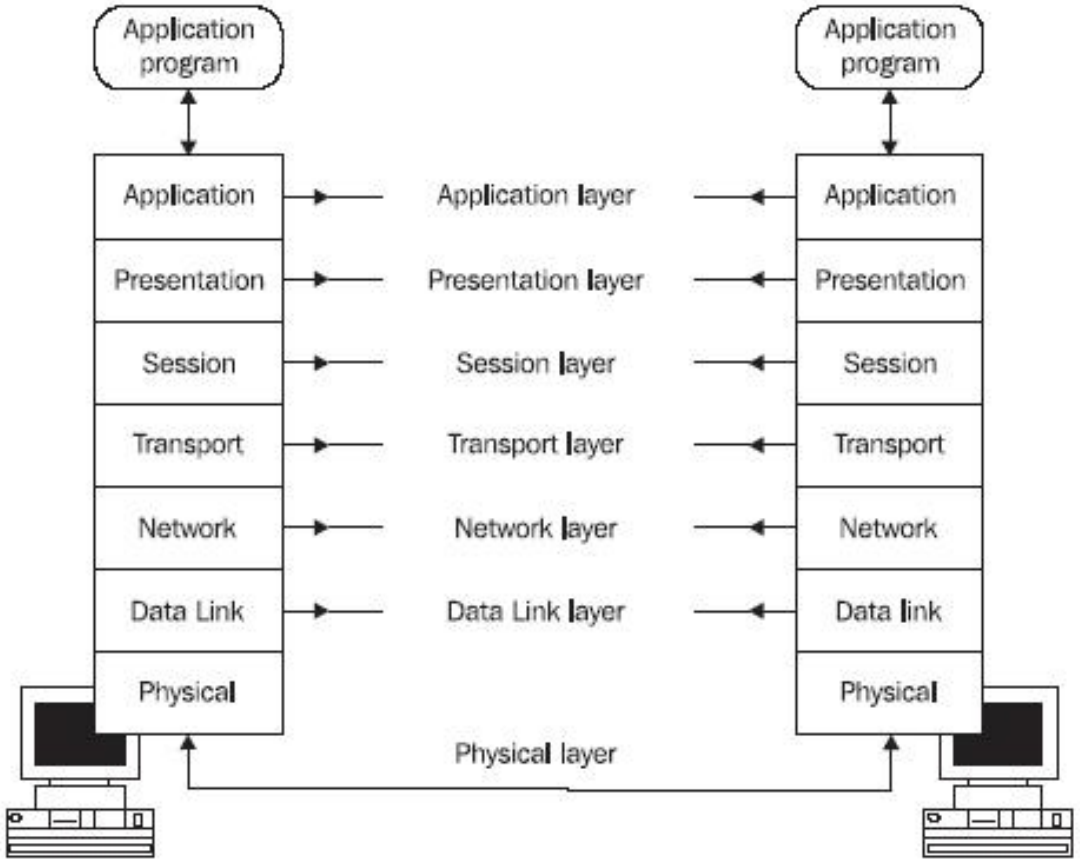
Δίκτυο Υπολογιστών

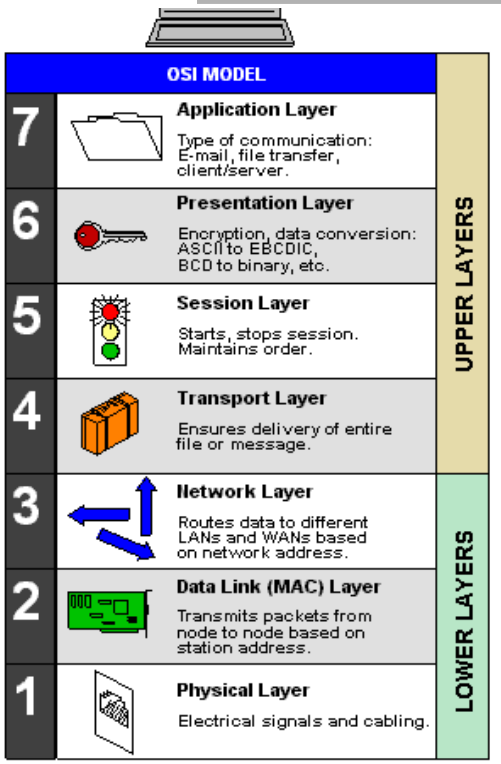
- **Δίκτυο υπολογιστών (computer network)**: κάθε συλλογή διασυνδεδεμένων υπολογιστών.
- **Χρήστης (user):** μια ανθρώπινη οντότητα υπεύθυνη για τις ενέργειές της σε ένα δίκτυο υπολογιστών.
- **Οικοδεσπότης ή ξενιστής (host):** μία προσπελάσιμη οντότητα μέσα σε ένα δίκτυο υπολογιστών. Κάθε οικοδεσπότης έχει έναν μοναδικό διεύθυνση μέσα σε ένα δίκτυο.
- **Διεργασία (process):** ένα στιγμιότυπο ενός εκτελέσιμου προγράμματος.
  - Η *διεργασία πελάτη* είναι εκείνη η διεργασία η οποία είναι υπεύθυνη να υποβάλλει αιτήματα χρήσης μιας δικτυακής υπηρεσίας.
  - Η *διεργασία εξυπηρετητή* είναι η διεργασία η οποία είναι υπεύθυνη να παρέχει μια δικτυακή υπηρεσία, παραδείγματος χάριν, μία διεργασία η οποία τρέχει διαρκώς στο παρασκήνιο.

Μοντέλα Αναφοράς Δικτύων

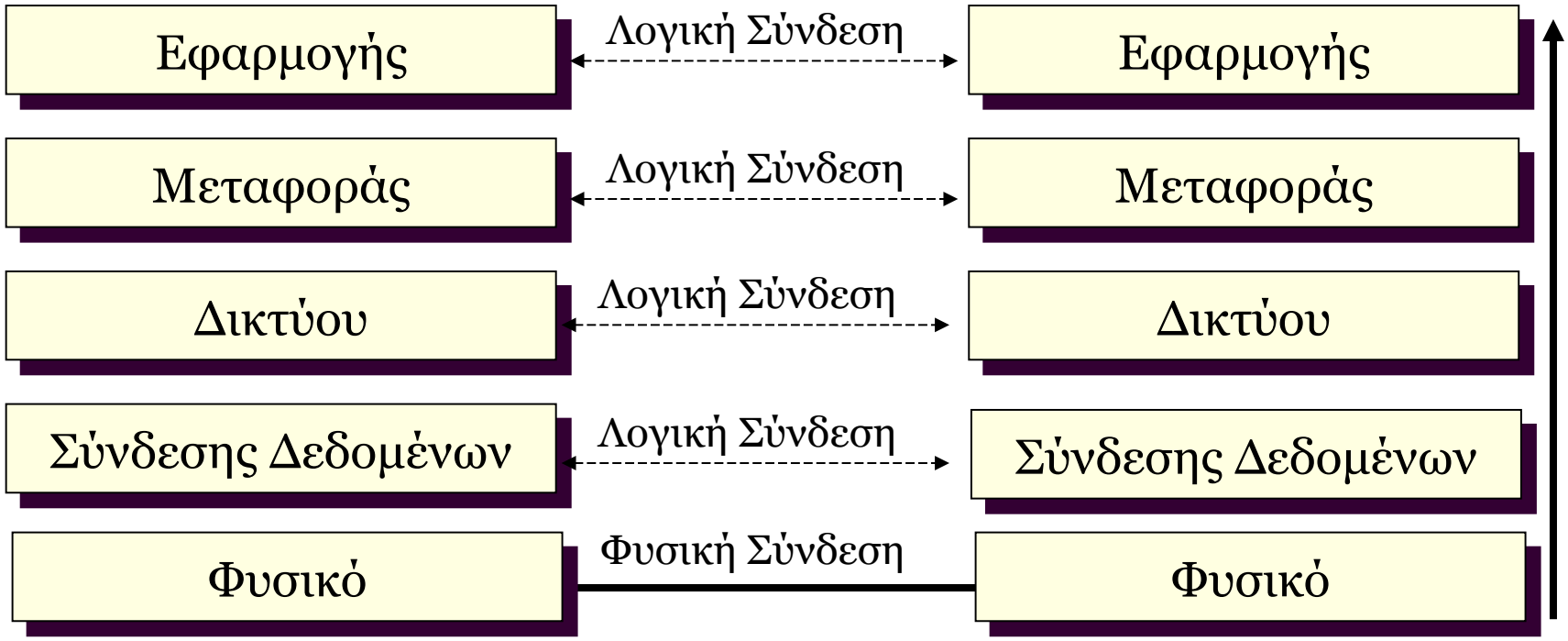
- Ομαδοποιούν ομοειδείς λειτουργίες σε αφηρημένα επίπεδα, γνωστά ως **στρώματα ή επίπεδα (layers)**
- Αφαιρετική προσέγγιση:
  - απλοποιεί την επικοινωνία
  - ορίζει διακριτές ενέργειες σε κάθε δικτυακό επίπεδο
- Κάθε επίπεδο επιτελεί συγκεκριμένες λειτουργίες, βάσει συγκεκριμένων κανόνων (πρωτοκόλλων επικοινωνίας)
- Τα πρωτόκολλα κάθε επιπέδου σε έναν κόμβο του δικτύου (host), μπορούν να επικοινωνήσουν με τα αντίστοιχα πρωτόκολλα *του ίδιου επιπέδου* σε έναν άλλο δικτυακό κόμβο.
- Στον ίδιο κόμβο, οι λειτουργίες κάθε επιπέδου διαθέτουν διεπαφές επικοινωνίας (interfaces) με τα επίπεδα που βρίσκονται ακριβώς πάνω και κάτω από το συγκεκριμένο επίπεδο.

Μοντέλο ISO/OSI

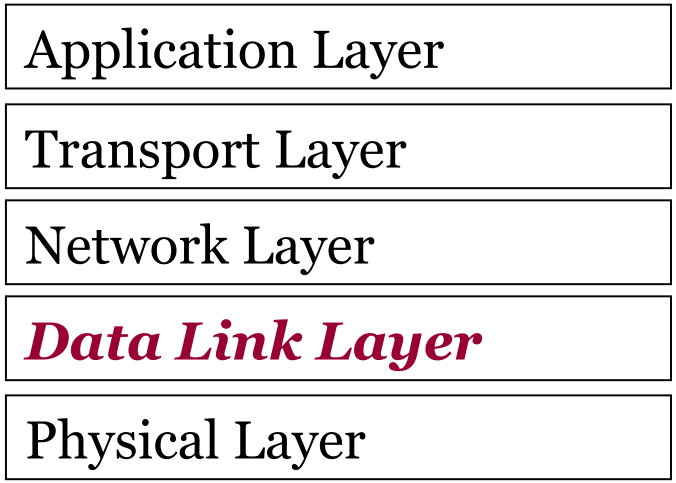




Μοντέλο Αναφοράς TCP/IP



Επίπεδο Σύνδεσης Δεδομένων



Μεταφορά μεταξύ δύο γειτονικών κόμβων

- **Επίπεδο Σύνδεσης Δεδομένων** (ή Πρόσβασης στο Δίκτυο – Network Access).
- Υπεύθυνο για την εγκατάσταση, υποστήριξη και κατάργηση συνδέσεων μεταξύ δύο οντοτήτων επιπέδου δικτύου.
- Ασχολείται κυρίως με
  - Κανόνες πρόσβασης στο δίκτυο
  - Ανίχνευση ή/και διόρθωση λαθών που μπορούν να συμβούν στο φυσικό επίπεδο.

Επίπεδο Σύνδεσης Δεδομένων

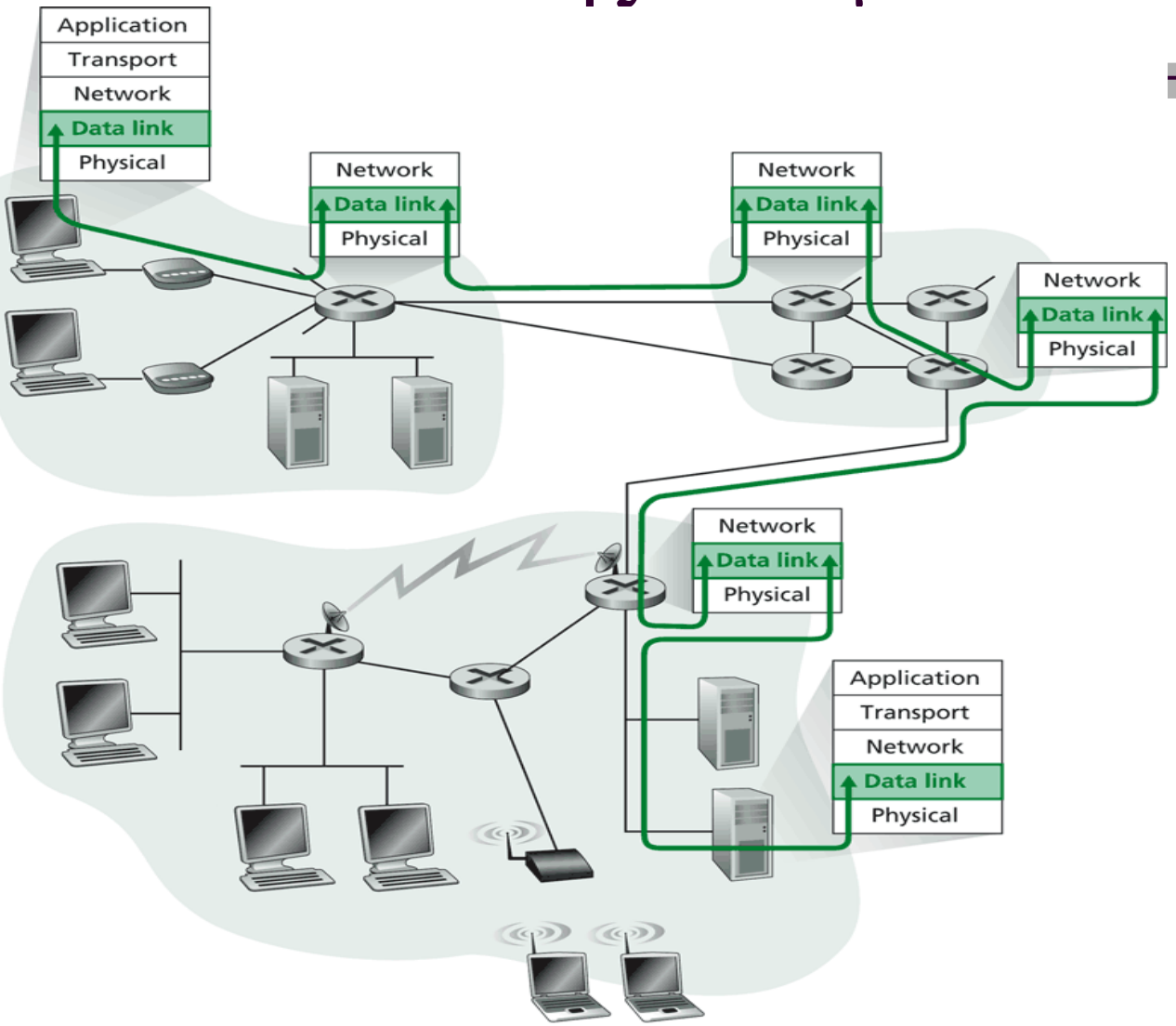
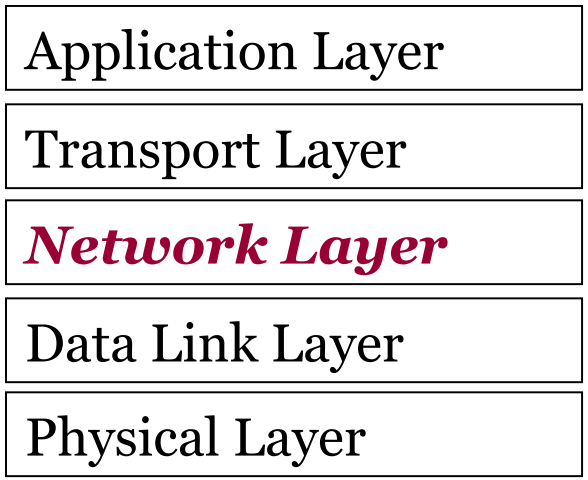


Figure 5.1 ♦ The link layer

Επίπεδο Δικτύου



Μεταφορά μεταξύ δύο ακραίων κόμβων

- **Επίπεδο Δικτύου** (ή Επίπεδο Internet). Είναι υπεύθυνο κυρίως για τη δρομολόγηση (routing) των δεδομένων που αποστέλλονται μεταξύ δύο οντοτήτων του επιπέδου μεταφοράς, αξιοποιώντας το υποδίκτυο (subnet) που τυχόν παρεμβάλλεται.
- «Υλοποιείται» στους ακραίους (end systems) κόμβους και στους δρομολογητές (routers) του δικτύου

Επίπεδο Δικτύου

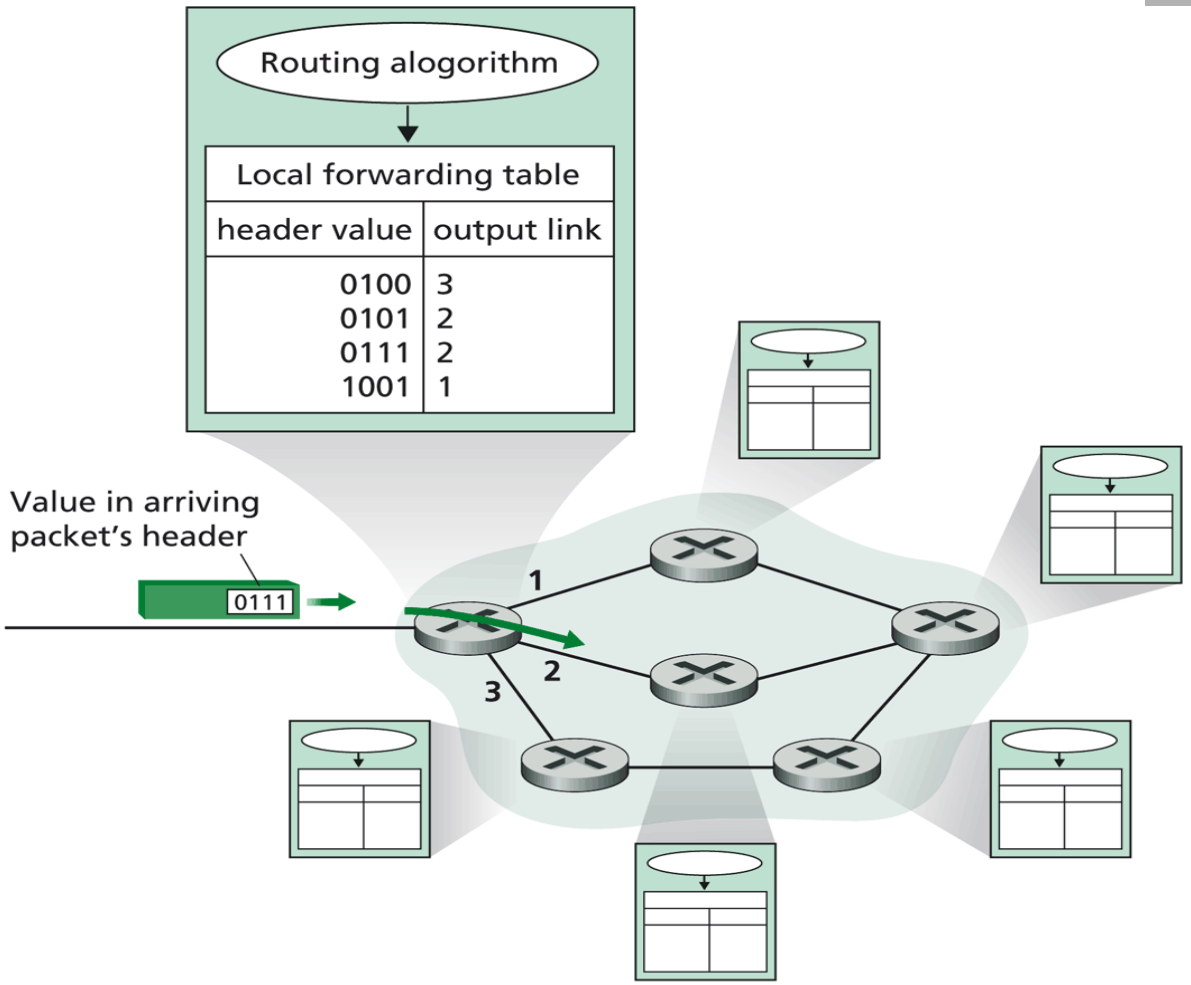
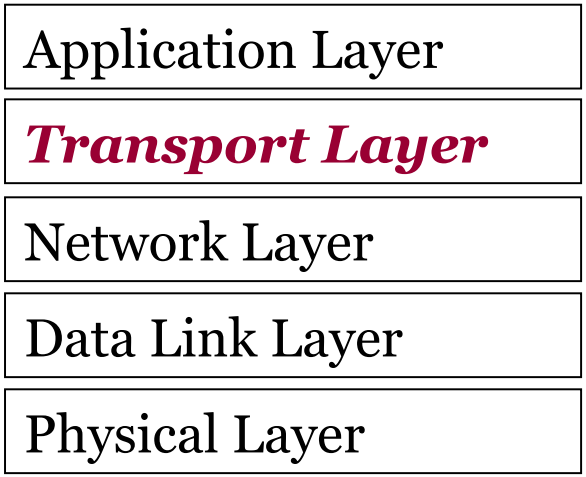


Figure 4.2 ♦ Routing algorithms determine values in forwarding tables

Επίπεδο μεταφοράς



Μεταφορά μεταξύ δύο εφαρμογών

- **Επίπεδο Μεταφοράς**. Είναι υπεύθυνο για τη μεταφορά δεδομένων μεταξύ δύο οντοτήτων επιπέδου εφαρμογής.
  - Καθορίζει τους κανόνες βάσει των οποίων εξασφαλίζεται η ορθή λήψη δεδομένων.
  - Στον παραλήπτη, είναι υπεύθυνο για τη προώθηση των εισερχόμενων δεδομένων στη κατάλληλη διεργασία
- Εκτελείται στους «ακραίους» κόμβους (end systems)

Επίπεδο μεταφοράς

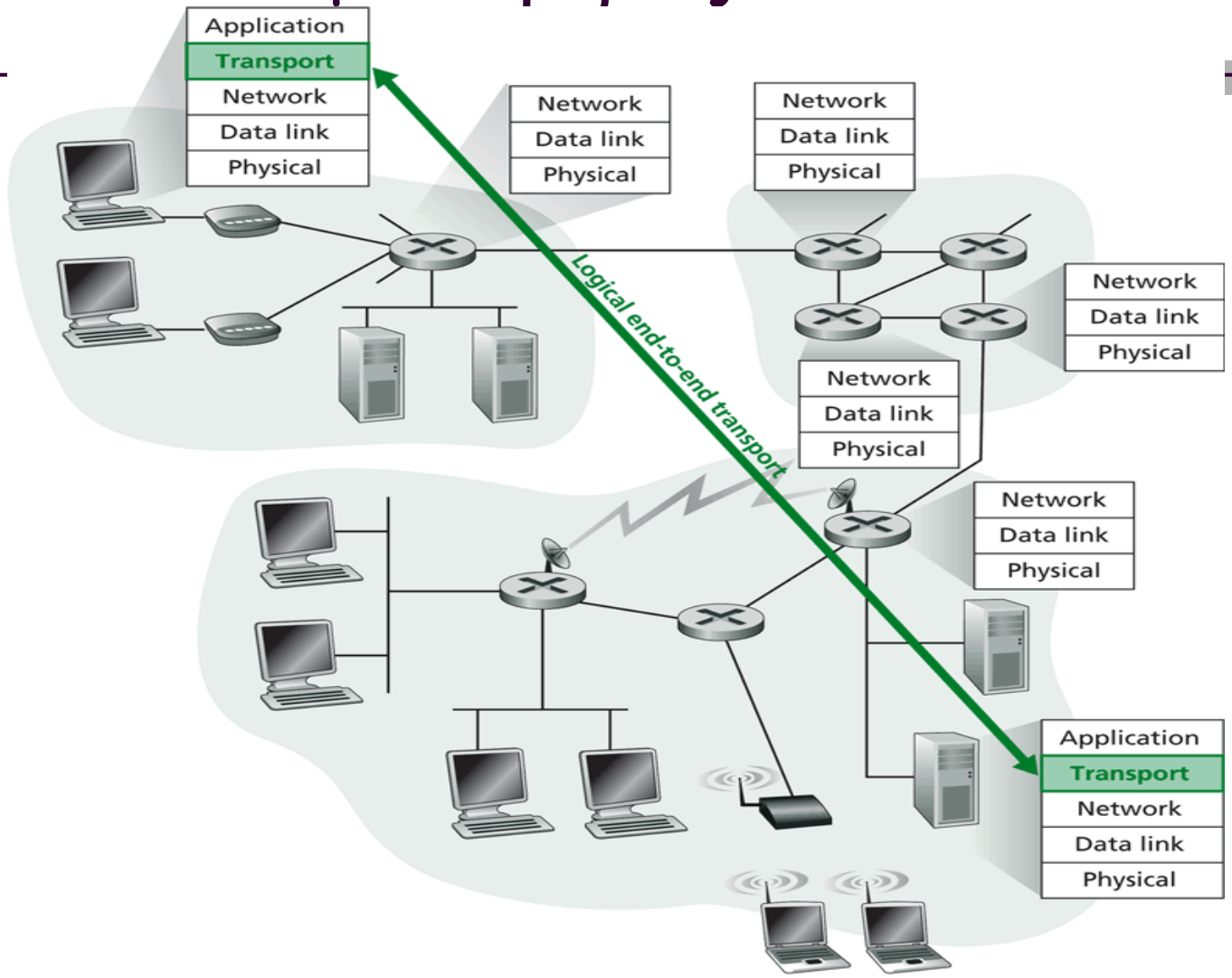
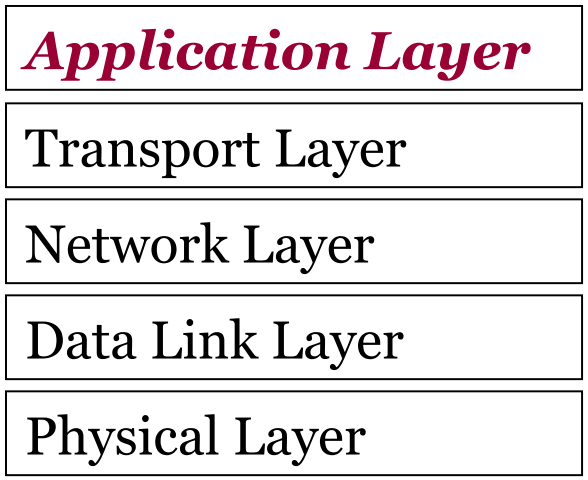


Figure 3.1 ♦ The transport layer provides logical rather than physical communication between application processes.

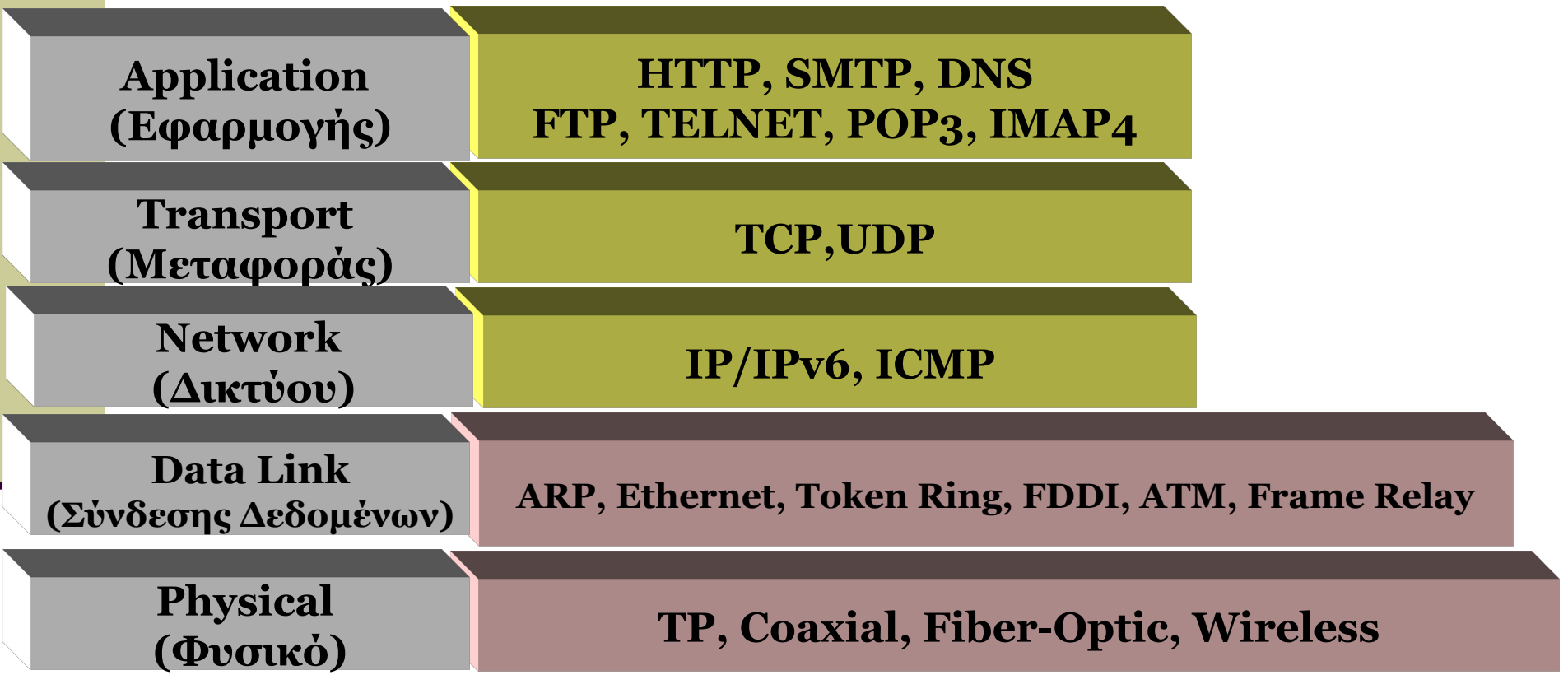
Επίπεδο εφαρμογής



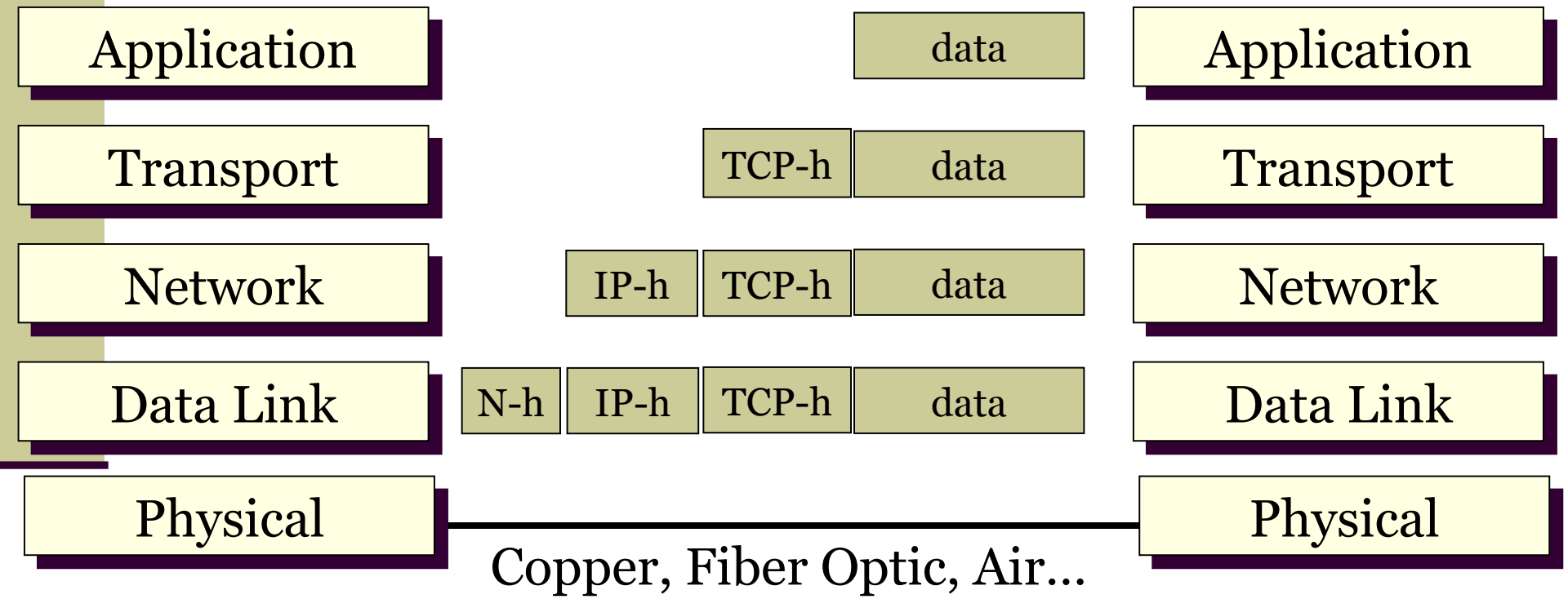
Δημιουργία δεδομένων προς μεταφορά

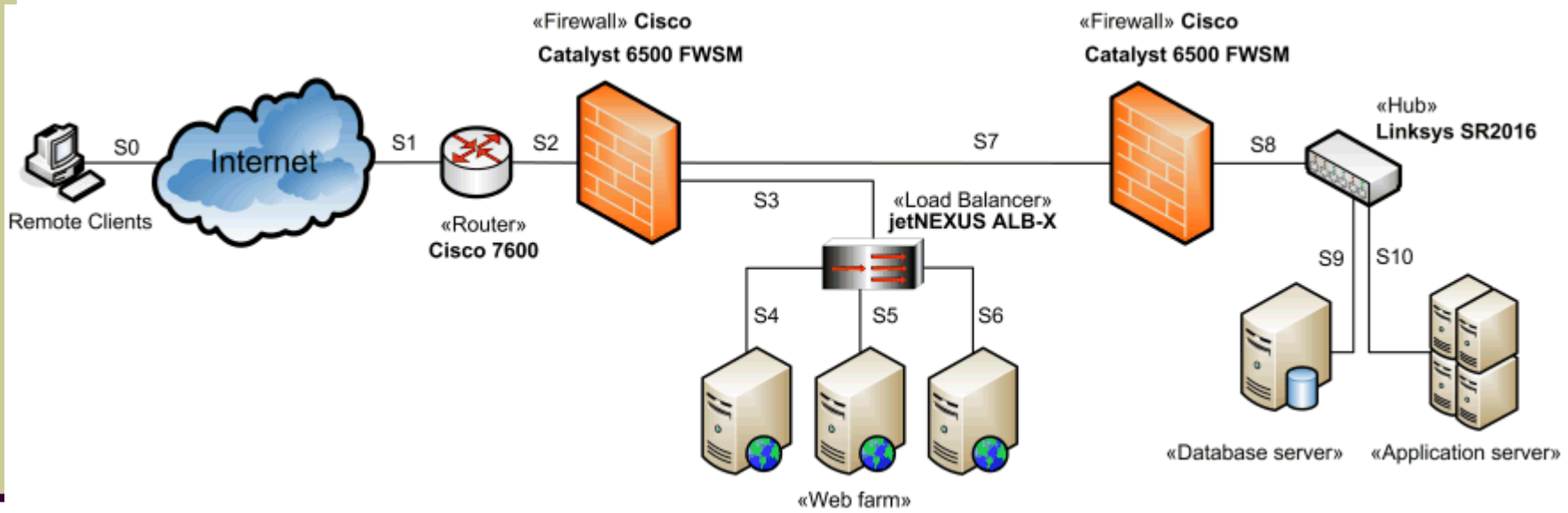
- **Επίπεδο Εφαρμογής**. Το επίπεδο αυτό περιέχει ένα πλήθος πρωτοκόλλων και εφαρμογών, οι οποίες χρησιμοποιούνται συνήθως από τους χρήστες δικτύων.
- Μεταξύ άλλων:
  - η αίτηση & λήψη σελίδων web
  - ηλεκτρονική αλληλογραφία
  - ανταλλαγή αρχείων
  - chat, …

Πρωτόκολλα διαφόρων επιπέδων στο μοντέλο TCP/IP



Χρήση επικεφαλίδων (headers) στα επίπεδα του TCP/IP




«Firewall» Cisco
Catalyst 6500 FWSM
«Firewall» Cisco
Catalyst 6500 FWSM
«Hub»
Linksys SR2016
S0
Internet
S1
S2
S7
S8
Remote Clients
«Router»
Cisco 7600
S3
«Load Balancer»
jetNEXUS ALB-X
S9
S10
S4
S5
S6
«Database server»
«Application server»
«Web farm»

Ασφάλεια στο μοντέλο ISO /OSI

- Με βάση τα διεθνή πρότυπα ασφάλειας δικτύων (ISO/IEC 7498-2 [2], ITU-T X.800 [3]) οι στόχοι ασφάλειας σε κάθε επίπεδο δικτύου επιτυγχάνονται μέσω:
  - ***πολιτικών ασφάλειας*** (security policies): το σύνολο κριτηρίων το οποίο ορίζει την παροχή υπηρεσιών ασφάλειας
  - ***υπηρεσιών ασφάλειας*** (security services): υπηρεσία η οποία παρέχεται από ένα επίπεδο δικτύου, προκειμένου να εξασφαλιστεί η επαρκής προστασία των συστημάτων ή των μεταδιδόμενων δεδομένων
- Μία υπηρεσία ασφάλειας υλοποιείται με τη βοήθεια κατάλληλων ***μηχανισμών ασφάλειας*** (security mechanisms)
  - μηχανισμοί που μπορούν να χρησιμοποιηθούν για να επιβάλουν τεχνικά την εφαρμογή μια υπηρεσίας ασφάλειας

Υπηρεσίες Ασφάλειας (1/4)

1. **Αυθεντικοποίηση (Authentication)**
   1. Αυθεντικοποίηση οντότητας (peer entity authentication)**:** μία οντότητα αποδεικνύει την εγκυρότητα της ταυτότητάς της.
   2. Αυθεντικοποίηση πηγής δεδομένων (data origin authentication)**:** μία οντότητα αποδεικνύει την εγκυρότητα της πηγής των δεδομένων.

2. **Έλεγχος πρόσβασης (Access Control).** Προστατεύει τα πληροφοριακά αγαθά που είναι διαθέσιμα μέσω του δικτύου από μη εξουσιοδοτημένη πρόσβαση.
   1. Πολιτικές κανόνων (rule-based policies) ή
   2. Πολιτικές ταυτότητας (identity-based policies).

Υπηρεσίες Ασφάλειας (2/4)

3. **Εμπιστευτικότητα Δεδομένων (Data Confidentiality)**.
   Προστατεύει τα δεδομένα από την αποκάλυψή τους σε μη εξουσιοδοτημένες οντότητες.
   1. Εμπιστευτικότητα σύνδεσης (connection confidentiality), όταν η υπηρεσία παρέχεται σε όλα τα επίπεδα (layers) της επικοινωνίας,
   2. Εμπιστευτικότητα χωρίς σύνδεση (connectionless confidentiality), όταν η εμπιστευτικότητα παρέχεται μόνο σε ένα επίπεδο,
   3. Επιλεκτική εμπιστευτικότητα (selective field confidentiality), όταν προστατεύει μόνο ορισμένα πεδία των δεδομένων, και
   4. Εμπιστευτικότητα κυκλοφοριακής ροής (traffic flow confidentiality), όταν προστατεύει την πληροφορία που ενδεχομένως θα μπορούσε να εξαχθεί από την παρατήρηση της κυκλοφοριακής ροής των δεδομένων.

Υπηρεσίες Ασφάλειας (3/4)

4. **Ακεραιότητα δεδομένων (Data Integrity).** Εξασφαλίζει ότι κατά τη διάρκεια της μετάδοσής τους τα δεδομένα δεν έχουν τροποποιηθεί από μη εξουσιοδοτημένες οντότητες.
    1. Ακεραιότητα σύνδεσης με αποκατάσταση (connection integrity with recovery): παρέχει την ακεραιότητα των δεδομένων και επίσης ανιχνεύει πιθανή τροποποίηση, εισαγωγή, διαγραφή, και επανάληψη των δεδομένων.
    2. Ακεραιότητα σύνδεσης χωρίς αποκατάσταση (connection integrity without recovery): σε αντίθεση με την προηγούμενη περίπτωση, δεν προσπαθεί την αποκατάσταση της ακεραιότητας.
    3. Επιλεκτική ακεραιότητα σύνδεσης (connection field integrity): παρέχει ακεραιότητα για μόνο σε ορισμένα πεδία δεδομένων σε μια σύνδεση.

Υπηρεσίες Ασφάλειας (4/4)

5. **Μη αποποίηση (non-repudiation).** Εξασφαλίζει ότι μία οντότητα δεν μπορεί να αρνηθεί τη μετάδοση ή η παραλαβή ενός μηνύματος.
    1. Μη αποποίηση με απόδειξη προέλευσης (non-repudiation with proof of origin): παρέχεται στον παραλήπτη των δεδομένων μία απόδειξη της προέλευσής τους. Ο αποστολέας δεν μπορεί να αρνηθεί αργότερα ότι απέστειλε τα συγκεκριμένα δεδομένα.
    2. Μη αποποίηση με απόδειξη παράδοσης (non-repudiation with proof of delivery): παρέχεται στον αποστολέα των δεδομένων μία απόδειξη της παράδοσής τους. Ο παραλήπτης δεν μπορεί αργότερα να αρνηθεί την λήψη των συγκεκριμένων δεδομένων.

Σχέση Επιπέδων Δικτύου – Υπηρεσιών Ασφάλειας

Service	1	2	3	4	5	6	7
Peer entity authentication			X	X			X
Data origin authentication			X	X			X
Access control service			X	X			X
Connection confidentiality	X	X	X	X		X	X
Connectionless confidentiality		X	X	X		X	X
Selective field confidentiality						X	X
Traffic flow confidentiality	X		X				X
Connection integrity with recovery				X			X
Connection integrity without recovery			X	X			X
Selective field connection integrity							X
Connectionless integrity			X	X			X
Selective field connectionless integrity							X
Nonrepudiation of origin							X
Nonrepudiation of delivery							X

Μηχανισμοί Ασφάλειας (1/6)

1. **Μηχανισμοί Κρυπτογράφησης (Encipherment Mechanisms)**
   - Παρέχουν τις υπηρεσίες εμπιστευτικότητας δεδομένων, μετασχηματίζοντας τα δεδομένα σε μη αναγνώσιμες μορφές.
   - Συμμετρικοί αλγόριθμοι (AES, Twofish, 3DES, RC5,...)
   - Ασύμμετροι αλγόριθμοι (RSA, ElGamal, EC,...)
   - Χρησιμοποιούνται και ως συστατικό στοιχείο άλλων μηχανισμών ασφάλειας (πρωτοκόλλων). Ενδεικτικά:
     - SSL, TLS, IPSec, VPN

Μηχανισμοί Ασφάλειας (2/6)

2. **Ψηφιακές υπογραφές (Digital signatures)**
   - Είναι το ηλεκτρονικό αντίστοιχο των συνηθισμένων υπογραφών στα ηλεκτρονικά δεδομένα.
   - Κατασκευάζονται χρησιμοποιώντας κατάλληλους αλγόριθμους ασύμμετρης κρυπτογράφησης.
   - Η αποκρυπτογράφηση των δεδομένων με το ιδιωτικό το κλειδί μιας οντότητας αντιστοιχεί στη διαδικασία υπογραφής των δεδομένων.
   - Παρέχουν αυθεντικοποίηση ταυτότητας και αυθεντικοποίηση πηγής δεδομένων, ακεραιότητα δεδομένων, και υπηρεσίες μη αποποίησης.
   - Παραδείγματα αλγορίθμων: RSA, ElGamal, DSA

Μηχανισμοί Ασφάλειας (3/6)

3. **Μηχανισμοί Ελέγχου Πρόσβασης (Access Control Mechanisms)**
   - Παρέχουν την αντίστοιχη υπηρεσία ελέγχου πρόσβασης.
   - Χρησιμοποιούν τις υπηρεσίες αυθεντικοποίησης οντότητας για να καθοριστούν και να επιβάλουν τα δικαιώματα πρόσβασης της οντότητας.
   - Παραδείγματα μηχανισμών:
     - Τείχη προστασίας (firewalls)
     - Λίστες ελέγχου πρόσβασης (Access Control Lists)
     - Προνόμια πρόσβασης ΛΣ

Μηχανισμοί Ασφάλειας (4/6)

4. **Μηχανισμοί Ακεραιότητας Δεδομένων (Integrity Mechanisms)**
   - Παρέχουν τις αντίστοιχες υπηρεσίες ακεραιότητας δεδομένων.
   - Παραδείγματα μηχανισμών:
     - Συναρτήσεις κατακερματισμού (hash functions)
     - Κώδικες αυθεντικοποίησης μηνύματος (Message Authentication Codes)
     - Ψηφιακές υπογραφές (digital signatures)
5. **Μηχανισμοί Αυθεντικοποίησης (Authentication Mechanisms)**
   - Παρέχουν την αντίστοιχη υπηρεσία αυθεντικοποίησης
   - Επιβεβαιώνουν την ταυτότητα μίας οντότητας
   - Παραδείγματα μηχανισμών:
     - Κωδικοί πρόσβασης
     - Ψηφιακές υπογραφές
     - Βιομετρικά χαρακτηριστικά

Μηχανισμοί Ασφάλειας (5/6)

6. **Μηχανισμοί Προστασίας Κίνησης (Traffic Padding Mechanisms)**
   - Παρέχουν προστασία από επιθέσεις ανάλυσης κίνησης.
   - Απαιτείται συνήθως συνεργασία με την υπηρεσία εμπιστευτικότητας για κρυπτογράφηση της επικοινωνίας.

7. **Μηχανισμοί Ελέγχου Δρομολόγησης (Routing Control Mechanisms)**
   - Επιτρέπουν την επιλογή μίας συγκεκριμένης διαδρομής (route) των δεδομένων.
   - Δυναμικά (ad hoc) ή μέσω στατικών (προσχεδιασμένων) διαδρομών
   - Παράδειγμα μηχανισμών: χρήση ετικετών ασφαλείας (security labels)

Μηχανισμοί Ασφάλειας (6/6)

8. **Μηχανισμοί «Συμβολαιογράφου» (Notarization Mechanisms)**
   - Παρέχουν υπηρεσίες:
     - ακεραιότητας δεδομένων (data integrity)
     - Αποδείξεις αποστολής και παράδοσης (non-repudiation of origin/delivery)
     - Χρονοσήμανσης δεδομένων (time-stamping)
   - Βασίζονται συνήθως σε συνδυασμό άλλων μηχανισμών (ψηφιακές υπογραφές, κρυπτογράφηση κτλ)

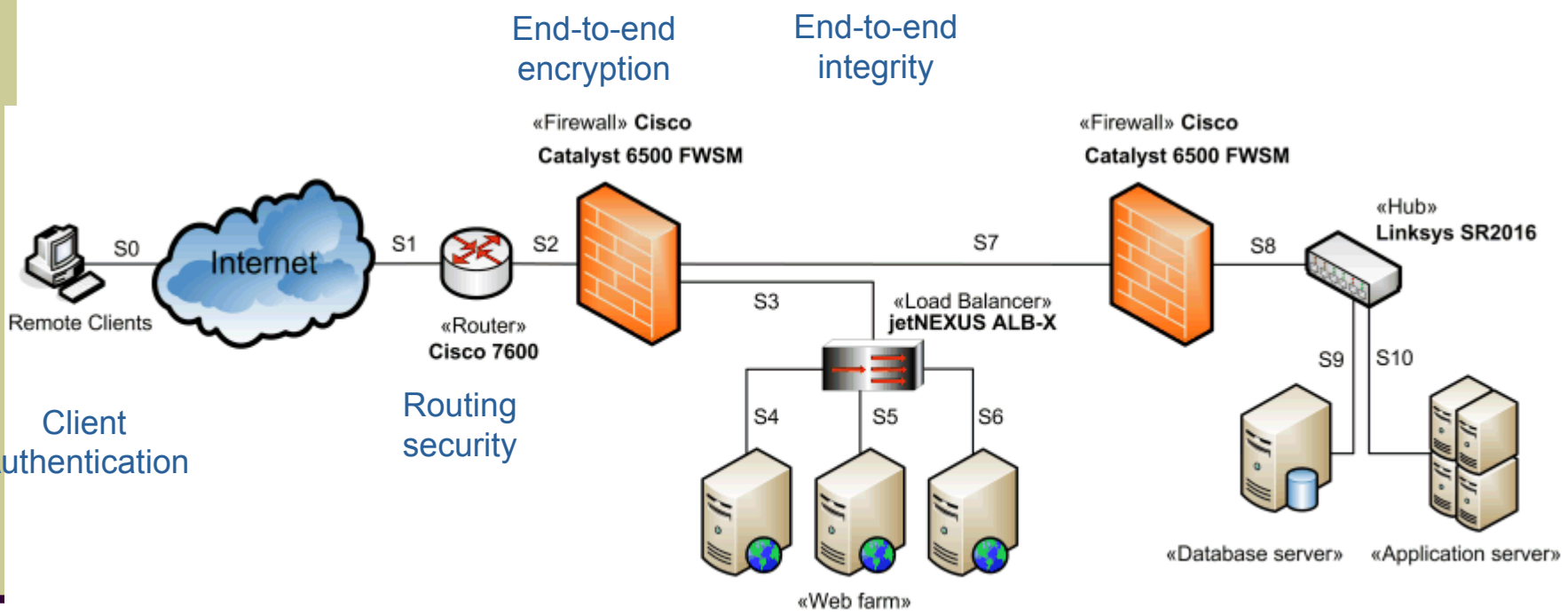
Σχέση υπηρεσιών - μηχανισμών ασφάλειας

Service	Encipherment	Digital Signature	Access Control	Data Integrity	Authentication Exchange	Traffic Padding	Routing Control	Notarization
Peer entity authentication	X	X			X			
Data origin authentication	X	X						
Access control service			X					
Connection confidentiality	X						X	
Connectionless confidentiality	X						X	
Selective field confidentiality	X							
Traffic flow confidentiality	X					X	X	
Connection integrity with recovery	X			X				
Connection integrity without recovery	X			X				
Selective field connection integrity	X			X				
Connectionless integrity	X	X		X				
Selective field connectionless integrity	X	X		X				
Nonrepudiation of origin		X		X				X
Nonrepudiation of delivery		X		X				X

Επιθέσεις Ασφάλειας Δικτύων

- Επιθέσεις εξαπάτησης (spoofing attacks)
  - Π.χ. IP spoofing,
  - ARP spoofing
- Επιθέσεις εισβολής (intrusion attacks)
  - Π.χ. Buffer overflows
- Επιθέσεις κατάχρησης σύνδεσης (logon abuse attacks)
  - Επιθέσεις πειρατείας (hijacking attacks)
  - TCP sequence number attack
- Επιθέσεις άρνησης υπηρεσίας (Denial of Service attacks / Distributed DoS attacks)
  - Ping of Death
  - SYN attack
- Επιθέσεις επιπέδου εφαρμογής
  - Virus, Trojans
  - SQL injection/poisoning
  - Remote command execution
  - Cross site scripting

Υπηρεσίες Ασφάλειας Δικτυακών Υπηρεσιών



2. Ασφάλεια στο επίπεδο δικτύου – Το πρωτόκολλο IPSec

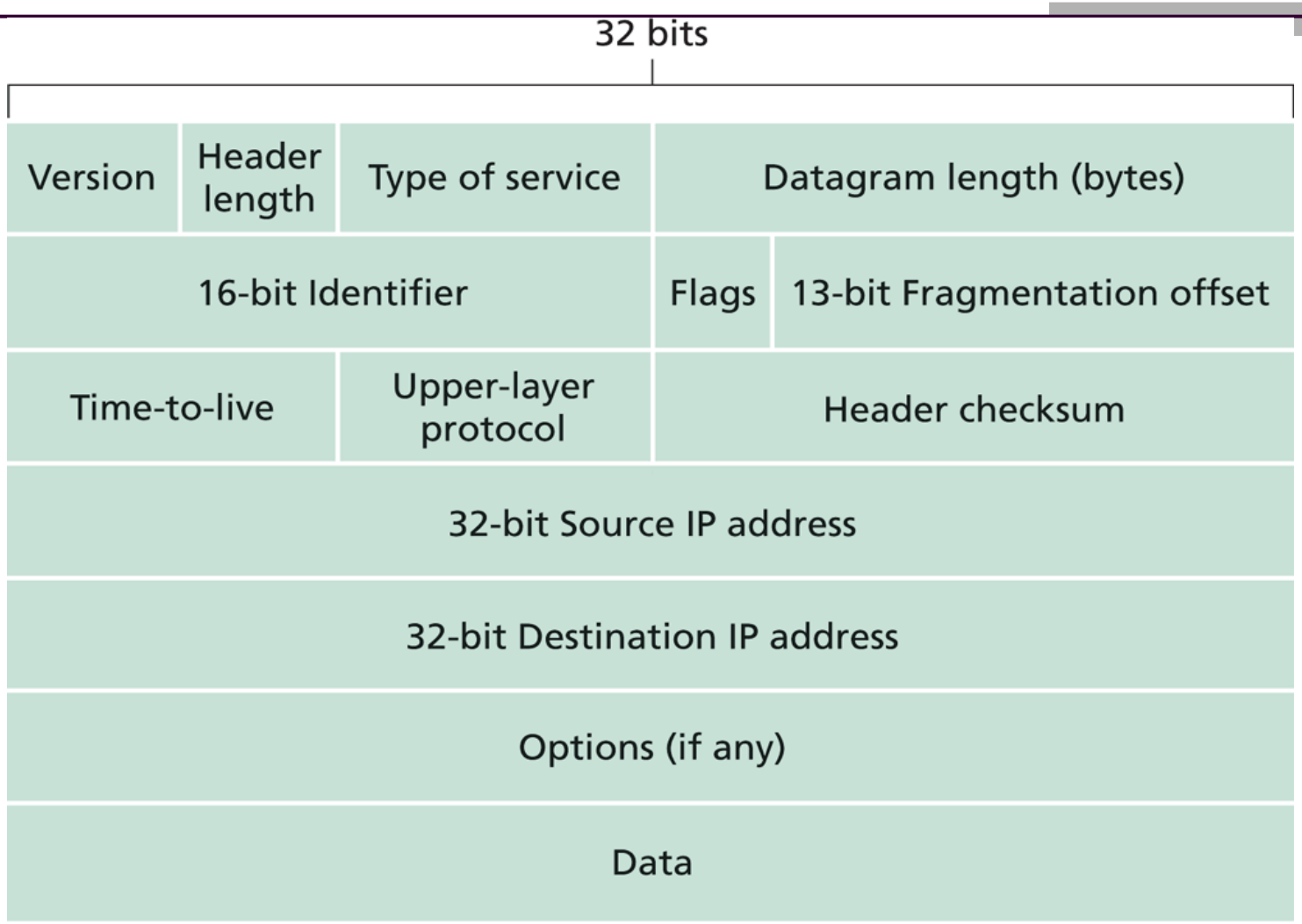
Επίπεδο Δικτύου και πρωτόκολλο IP

- Επίπεδο δικτύου (network layer):
  - Καθορίζει κανόνες επικοινωνίας μεταξύ των ακραίων κόμβων (end systems) και των δρομολογητών (routers) του δικτύου
- Πρωτόκολλο IP (Internet Protocol)
  - Χρησιμοποιείται στο επίπεδο δικτύου στο μοντέλο TCP/IP
  - Καθορίζει τη μορφή των πακέτων στο επίπεδο Δικτύου
  - Καθορίζει τη μορφή των διευθύνσεων των κόμβων (διεύθυνση IP)
  - Λαμβάνει αποφάσεις δρομολόγησης με βάση τις διευθύνσεις IP που βρίσκονται στις επικεφαλίδες IP (IP headers)

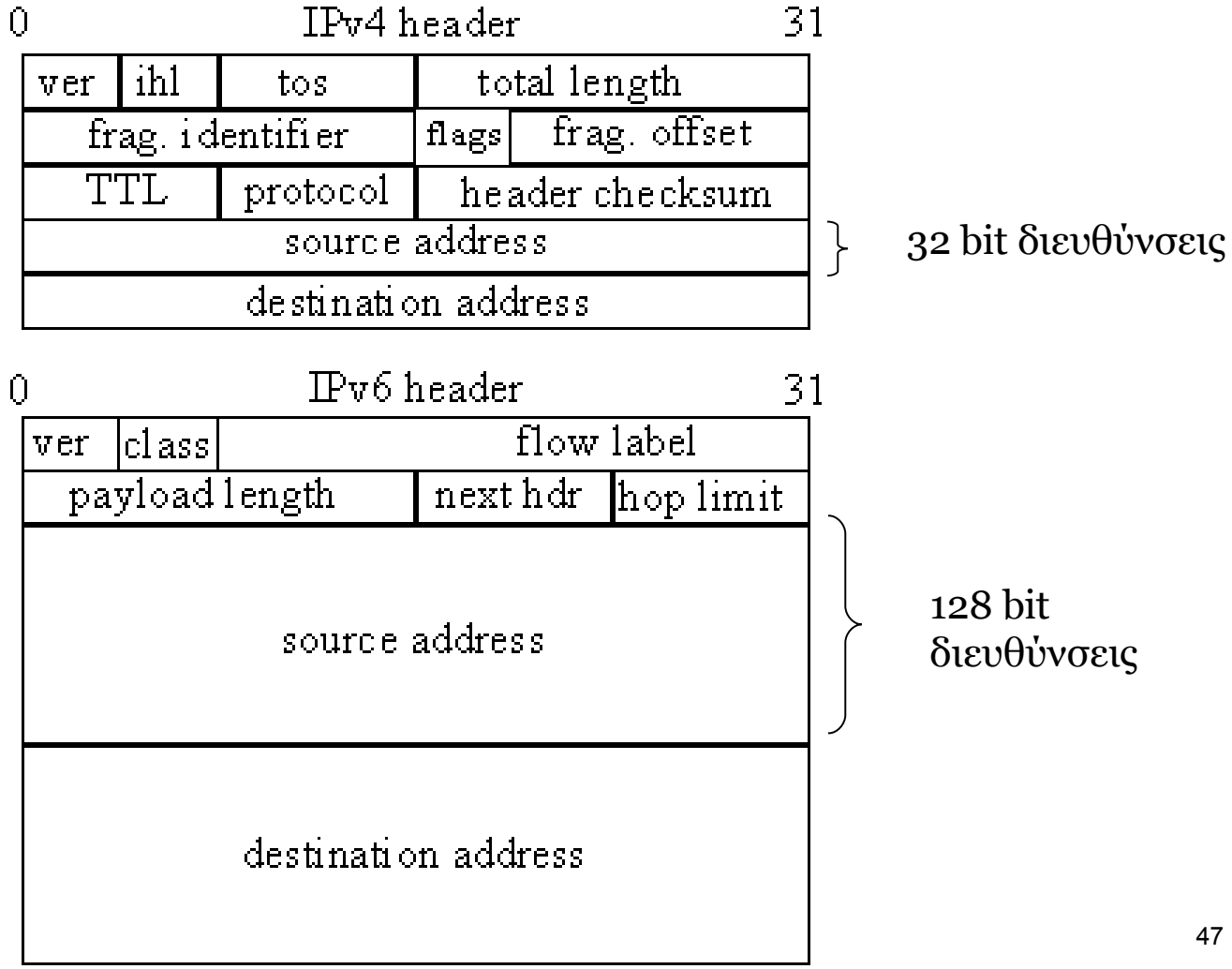
Διάσπαση σε πακέτα

- Όριο στην ποσότητα πληροφορίας που μπορεί να λάβει ο παραλήπτης
  - buffer size
- Όσο μεγαλύτερο είναι ένα πακέτο, τόσο υψηλότερη η πιθανότητα να επαναμεταδοθεί λόγω λάθους
  - Μόνο το πακέτο που έφθασε λάθος χρειάζεται να επαναμεταδοθεί
- Περισσότεροι από ένας κόμβοι «ανταγωνίζονται» για την πρόσβαση στο μέσο
  - Όσο μεγαλύτερο είναι το μέγεθος ενός πακέτου, τόσο περισσότερο απασχολεί ένας κόμβος το δίκτυο
- Μεταγωγή πακέτου (packet switch): Τα πακέτα μιας μετάδοσης μπορούν να ακολουθήσουν διαφορετικά δρομολόγια
  - Ευελιξία

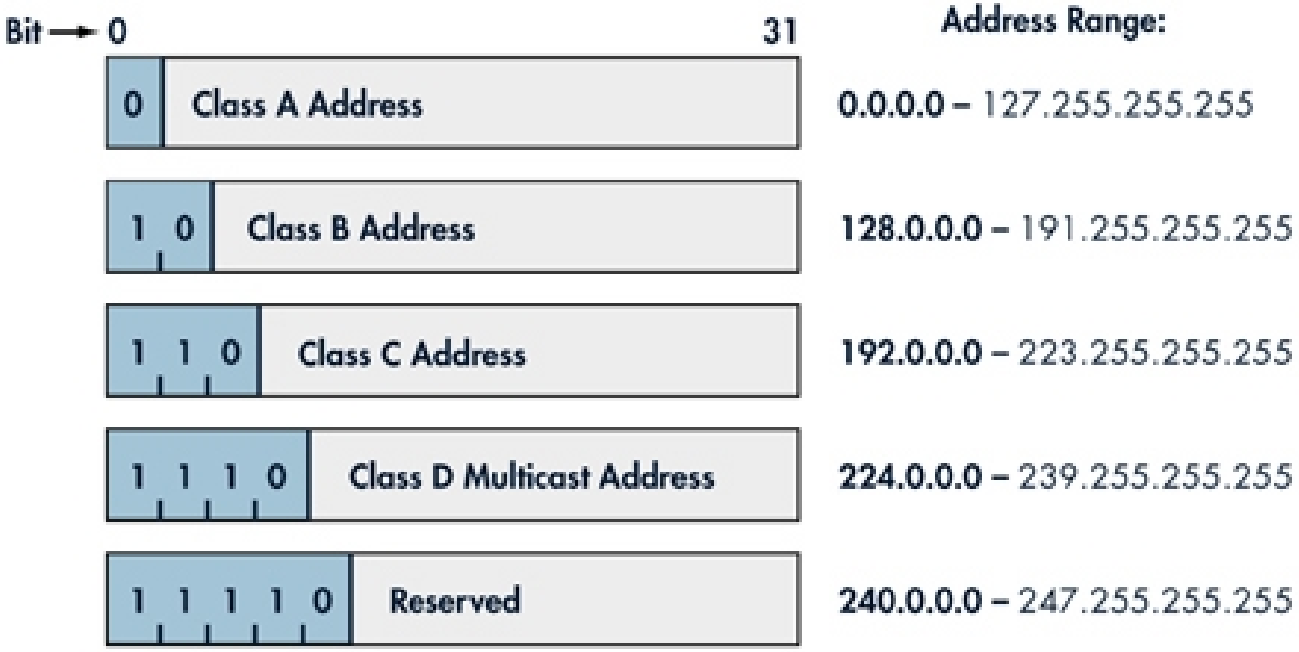
Επικεφαλίδα IP (IPv4)



Επικεφαλίδα IP (IPv6)



Κλάσεις IP και private IPs



Από	Μέχρι
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

Ιδιωτικές (private) διευθύνσεις IP

Προβλήματα στο IP

- Οποιοσδήποτε ενδιάμεσος κόμβος (hub, switch ή router) μπορεί να λειτουργήσει σαν ωτακουστής πακέτων (packet sniffer).
- Λειτουργία σε *promiscuous mode* (ο κόμβος ακούει οτιδήποτε περνά από το καλώδιο που είναι συνδεδεμένος)
  - Πολύτιμη λειτουργία για διαχειριστές δικτύων (για διαχείριση, ανίχνευση λαθών)
  - … αλλά και για hackers

Επιθέσεις Ασφάλειας στο IP

- *Packet Sniffing* (παρακολούθηση πακέτου):
  - Ο επιτιθέμενος «κρυφακούει» χωρίς να γίνει αντιληπτός την επικοινωνία (πακέτα) που ανταλλάσσεται
- *IP Spoofing* (πλαστογράφηση IP διεύθυνσης) :
  - Ο επιτιθέμενος μπορεί να τροποποιήσει την ταυτότητα (IP διεύθυνση) της πηγής.
- *Data modification* (τροποποίηση δεδομένων):
  - Ο επιτιθέμενος τροποποιεί δεδομένα, παρόλο που δεν μπορεί να έχει πρόσβαση ανάγνωσης σε αυτά
- *Replay Old Packets* (επανάληψη πακέτου):
  - Ο επιτιθέμενος επαναλαμβάνει την αποστολή παλαιών πακέτων

IP spoofing

- Κάθε πακέτο, περιέχει στο IP header τις IP διευθύνσεις αποστολέα και παραλήπτη
- Αλλαγή της διεύθυνσης του πραγματικού αποστολέα (source IP address) με μια άλλη IP διεύθυνση
  - τυχαία ή επιλεγμένη
  - υπαρκτή ή όχι
- Σκοπός επίθεσης
  - Παράκαμψη μηχανισμών αυθεντικοποίησης για την πρόσβαση σε υπηρεσία
  - Πρώτο βήμα για τη διενέργεια επιθέσεων προς τρίτους (DOS, DDOS attacks)

Το πρωτόκολλο IPSec

- Αντιμετωπίζει τις επιθέσεις στο επίπεδο δικτύου (network layer) και ειδικότερα στο πρωτόκολλο IP
- Παρέχει υπηρεσίες:
  - Εμπιστευτικότητας (encryption)
  - Αυθεντικοποίησης (authentication)
- Οι υπηρεσίες ασφάλειας που προσφέρει είναι *διαφανείς (transparent)* για τα πιο πάνω επίπεδα

Υπηρεσίες Ασφάλειας του IPSec

- Εμπιστευτικότητα δεδομένων

  (data confidentiality)

- Ακεραιότητα δεδομένων

  (data integrity)

- Αυθεντικοποίηση πηγής

  (data-origin authentication)

- Προστασία από επιθέσεις επανάληψης

  (replay attack protection)

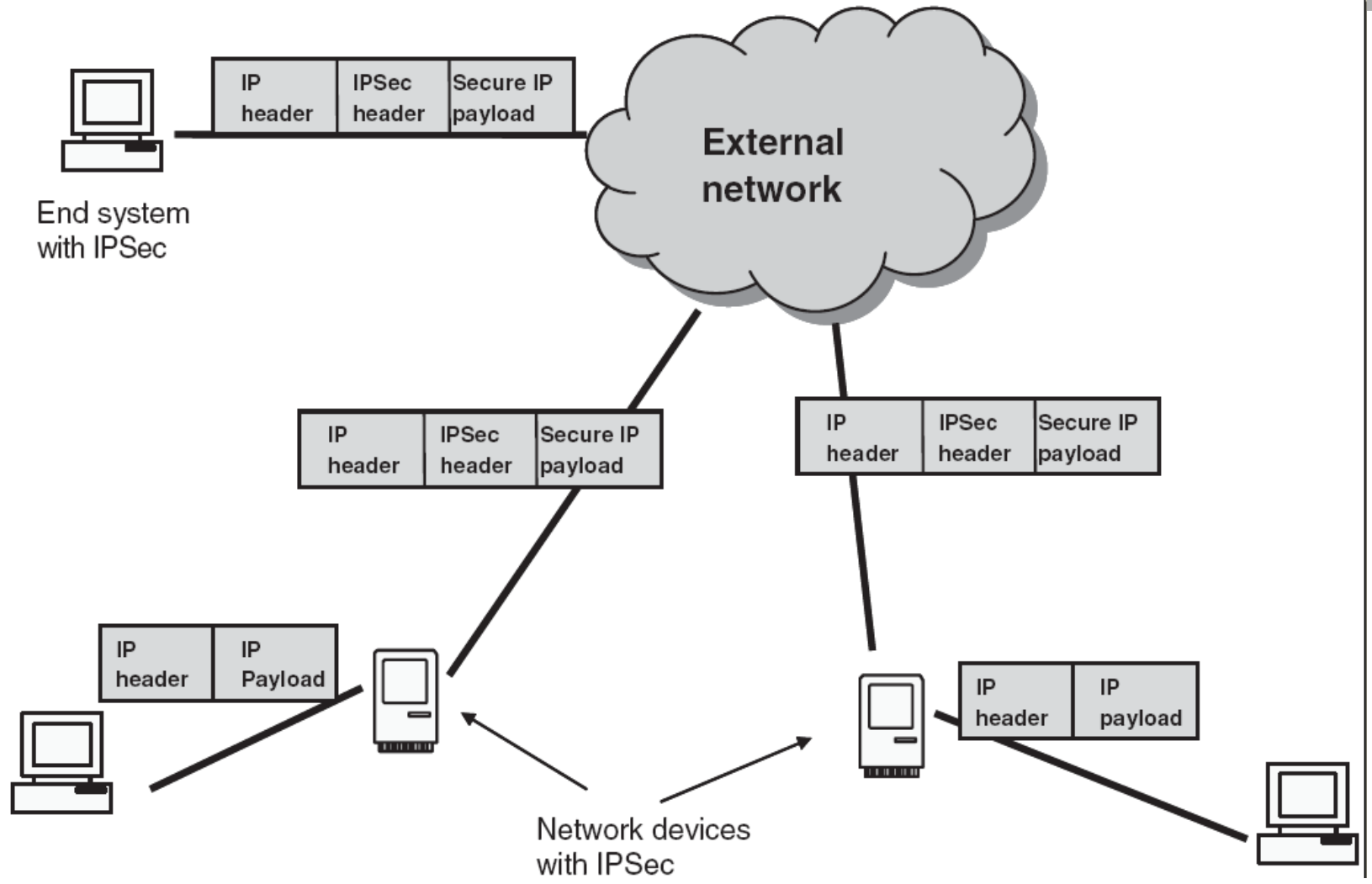
Βασικά συστατικά του IPSec

- Ένα μηχανισμό για αυθεντικοποίηση:
  - *Επικεφαλίδα Αυθεντικοποίησης (Authentication Header – **AH**)*
- Ένα μηχανισμό που συνδυάζει αυθεντικοποίηση και κρυπτογράφηση:
  - *Ενθυλάκωση Ασφάλειας Φορτίου (Encapsulating Security Payload – **ESP**)*
- *Συσχετισμούς Ασφάλειας (Security Associations – SA)*: αναπαριστούν την συμφωνία μεταξύ δύο οντοτήτων (τα κρυπτογραφικά κλειδιά)
- Μία *Υποδομή Διαχείρισης Κλειδιών*: χρησιμοποιείται για την ανταλλαγή/δημιουργία κοινών κλειδιών (SA)

Μηχανισμοί AH και ESP

- Κάθε μηχανισμός προσθέτει μία νέα επικεφαλίδα (header) σε κάθε IP πακέτο, μεταξύ του IP header και του TCP/UDP header
- Μόνο οι ενδιαφερόμενοι κόμβοι χρησιμοποιούν τις επικεφαλίδες AH και ESP
  - Συνεπώς οποιοσδήποτε δρομολογητής (router) χειρίζεται IPSec πακέτα σαν κανονικά IP πακέτα
- Οι μηχανισμοί AH και ESP εφαρμόζονται:
  - μεμονωμένα
  - ή σε συνδυασμό

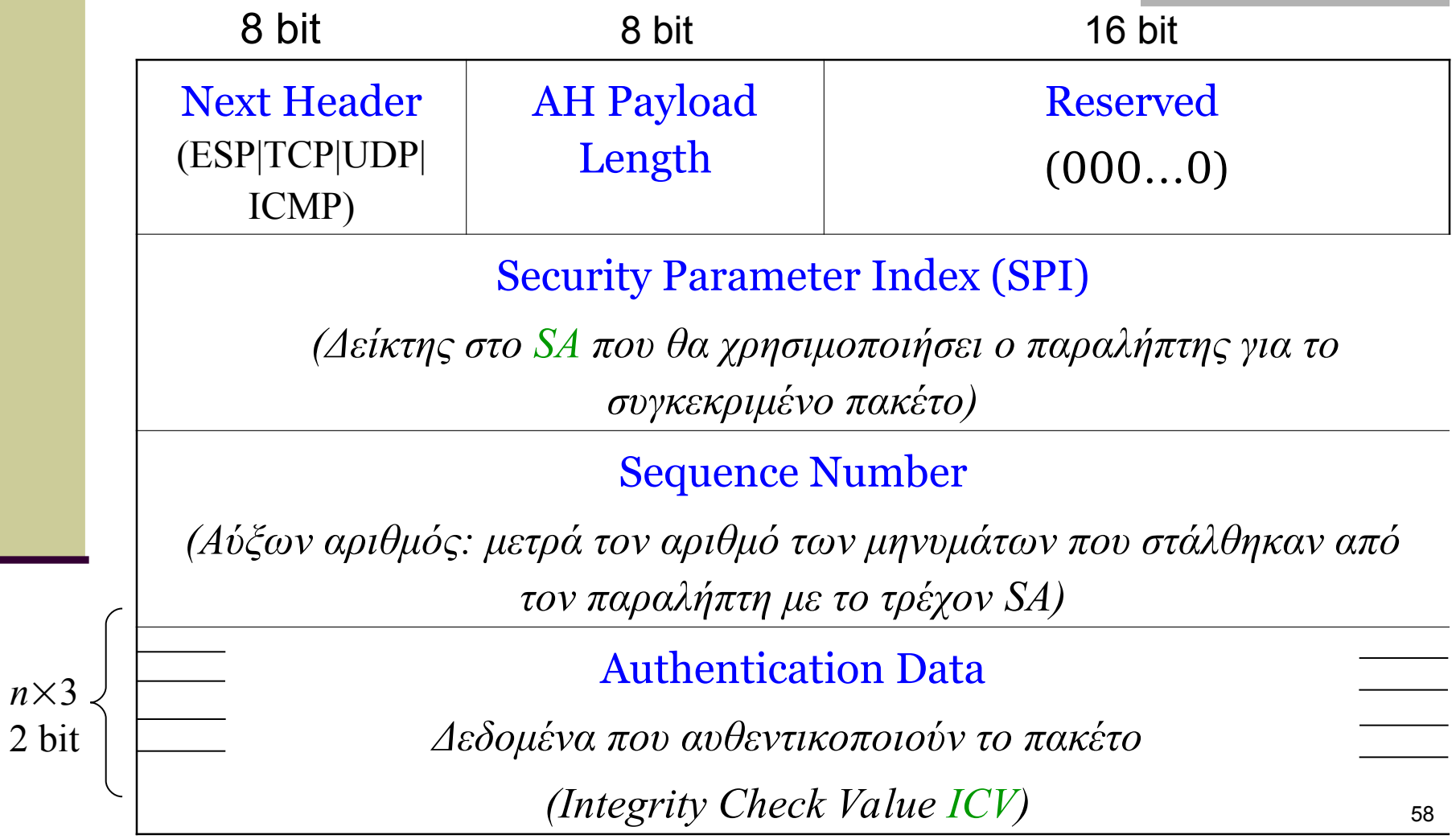
Παράδειγμα σεναρίου IPSec



Authentication Header - AH

- Παρέχει:
  - Αυθεντικοποίηση πηγής (data origin authentication)
    - Αποτρέπει επιθέσεις IP spoofing
  - Ακεραιότητα δεδομένων (data integrity)
    - Ανιχνεύει πιθανή τροποποίηση δεδομένων

Δομή επικεφαλίδας AH



Υπολογισμός και επαλήθευση Authentication Data

Α: Πηγή

Β: Προορισμός

(1) Υπολογισμός ICV:

ICV = $HMAC_K(IP_A, IP_B, \ldots, AH, TCP\text{-}header)$

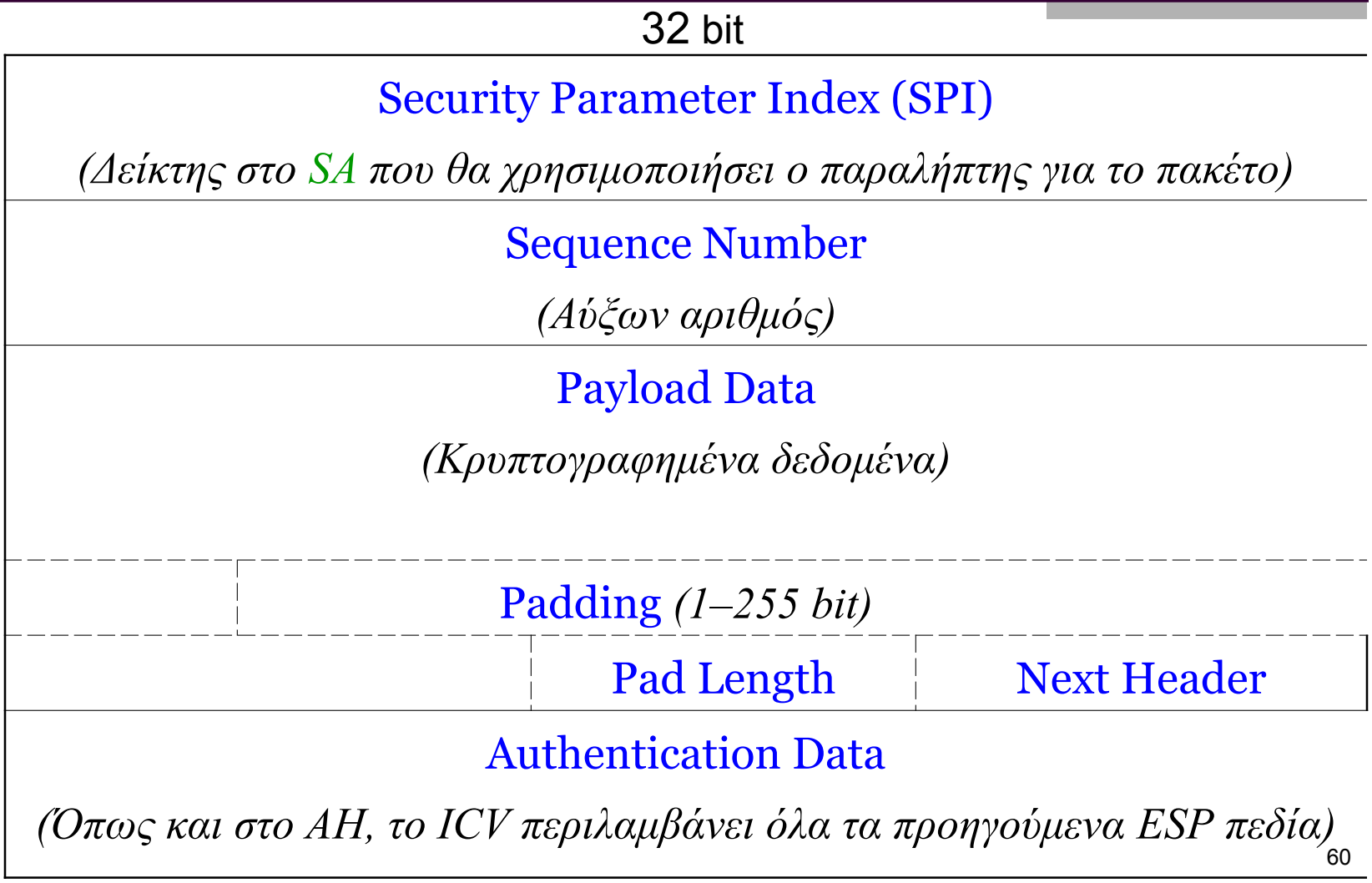
= $Hash(K, IP_A, IP_B, \ldots, AH, TCP\text{-}header)$

(2) Αποστολή πακέτου (με την επικεφαλίδα AH)

(3) Εξαγωγή όλων των στοιχείων

(4) Υπολογισμός και επαλήθευση ICV με το κλειδί *K*

Δομή επικεφαλίδας ESP



Υπολογισμός κρυπτογραφημένων δεδομένων (Encrypted Payload Data)

- Κρυπτογράφηση των πεδίων:

  $ENCR_K$(*Payload Data*, *Padding*, *Pad Length, Next Header*)

- Αλγόριθμοι κρυπτογράφησης
  - DES, 3-DES, IDEA, 3-IDEA, CAST, Blowfish, AES
- Εφόσον απαιτούνται δεδομένα συγχρονισμού της κρυπτογράφησης (Initialization Vector – IV), περιλαμβάνονται στην αρχή του Payload Data
- Αλγόριθμοι αυθεντικοποίησης
  - MD5, SHA-1

Encapsulating Security Payload - ESP

- Παρέχει:
  - Εμπιστευτικότητα δεδομένων (data confidentiality)
    - Αποτρέπει επιθέσεις packet sniffing
  - Εμπιστευτικότητα κυκλοφοριακής ροής (traffic flow confidentiality)
    - Απόκρυψη πραγματικού μήκους μηνύματος
- Μπορεί να παρέχει και τις υπηρεσίες του AH (προαιρετικά)
  - Αυθεντικοποίηση πηγής
  - Ακεραιότητα δεδομένων

Ανταλλαγή κλειδιών κρυπτογράφησης και αυθεντικοποίησης

- Απαιτείται να γνωρίζουν και οι δύο κόμβοι τα κλειδιά Κ και Κ'
- Αυτό γίνεται με τη βοήθεια
  - Των Συσχετισμών Ασφάλειας (Security Associations – SA)
    - αναπαριστούν την συμφωνία μεταξύ δύο οντοτήτων (τα κρυπτογραφικά κλειδιά)
  - Του πρωτοκόλλου Ανταλλαγής Κλειδιών (Internet Key Exchange – IKE):
    - χρησιμοποιείται για την ανταλλαγή κοινών κλειδιών (SA) μεταξύ των κόμβων

Συσχετισμοί Ασφάλειας (SA)

- Αφορά μία συμφωνία μεταξύ δύο κόμβων για συγκεκριμένες υπηρεσίες ασφάλειας
  - Ορίζει κοινές παραμέτρους ασφάλειας
- Είναι μίας κατεύθυνσης
  - ένα SA για εξερχόμενη κίνηση και
  - ένα SA για εισερχόμενη κίνηση
- Δύο κόμβοι μπορούν να χρησιμοποιήσουν πολλά SA για μία επικοινωνία
- Όλα τα SA που χρησιμοποιεί ένας κόμβος αποθηκεύονται σε μία βάση
  - Security Association Database – SAD

Περιεχόμενο SA

- Διευθύνσεις
  - Source IP, Destination IP
- Δεδομένα Αυθεντικοποίησης
  - Authentication Algorithm, **Authentication Key (K)**
- Δεδομένα κρυπτογράφησης
  - Encryption Algorithm, **Encryption Key (K')**
- Μετρητές για προστασία
  - Προστασία από επανάληψη (replay attacks)
  - Προστασία από υπερχείλιση (overflow attacks)
- Χρόνος ζωής του SA
- Σημαία κατάστασης επικεφαλίδας IPSec
  - Κατάσταση μετάδοσης (Transport mode)
  - Κατάσταση διόδου (Tunneling mode)

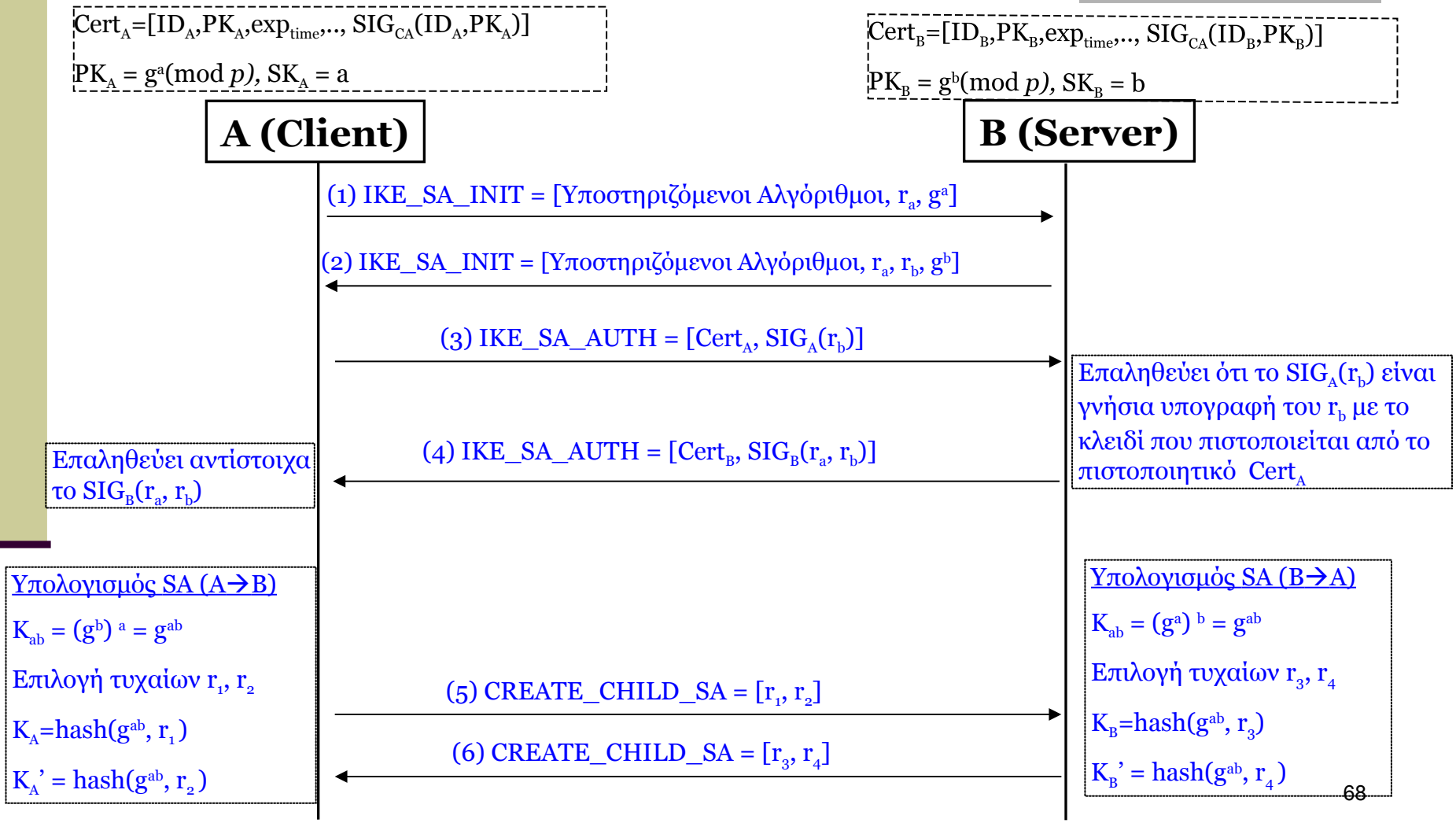
Δείκτης Παραμέτρων Ασφάλειας (Security Parameter Index)

- Βρίσκεται και στο AH και στο ESP
- Δημιουργείται από τον αποστολέα κάθε πακέτου
- Δείχνει στον παραλήπτη ποιο SA χρησιμοποίησε ο αποστολέας (ώστε να το αναζητήσει και ο παραλήπτης στη βάση του Security Association Database – SAD)

Υποδομή Διαχείρισης Κλειδιών (Internet Key Exchange – IKE)

- Η χρήση των μηχανισμών AH και ESP, προϋποθέτει την ύπαρξη των ίδιων SA μεταξύ των δύο κόμβων.
- Χρειάζεται μία υποδομή για την ανταλλαγή των κλειδιών (Internet Key Exchange)
  - Manually
  - Automated
    - Public Key Infrastructure(PKI) - Public Key Certificates
- Αλγόριθμοι ανταλλαγής κλειδιού
  - Diffie-Hellmann
  - RSA

Παράδειγμα ανταλλαγής κλειδιών: IKE με Authenticated Diffie-Hellman



Καταστάσεις λειτουργίας IPSec

- Κατάσταση μεταγωγής (Transport mode):
  - Εφαρμόζεται μόνο στο payload field (όχι στο source IP)
  - Απευθείας επικοινωνία δύ κόμβων (end-to-end)
- Κατάσταση Διόδου (Tunnel mode):
  - Εφαρμόζεται και στο payload field και στο source IP field)
  - Δημιουργείται νέο source Il
  - επικοινωνία μέσω IPSec enabled Gateway
  - Κατάλληλο για VPN

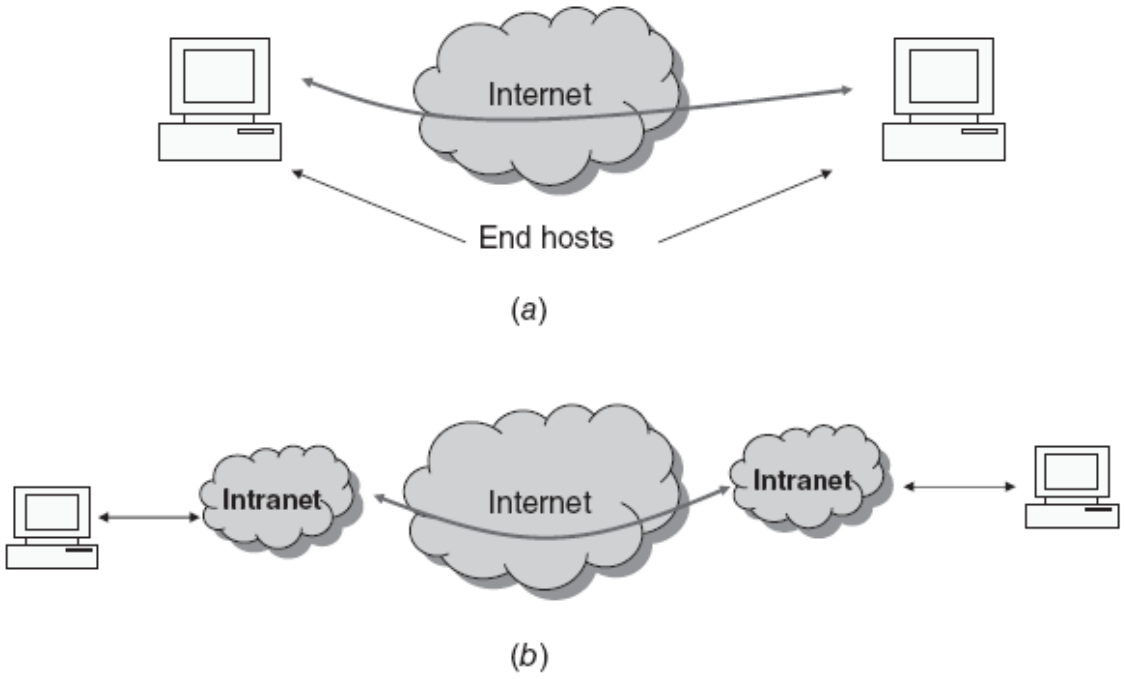
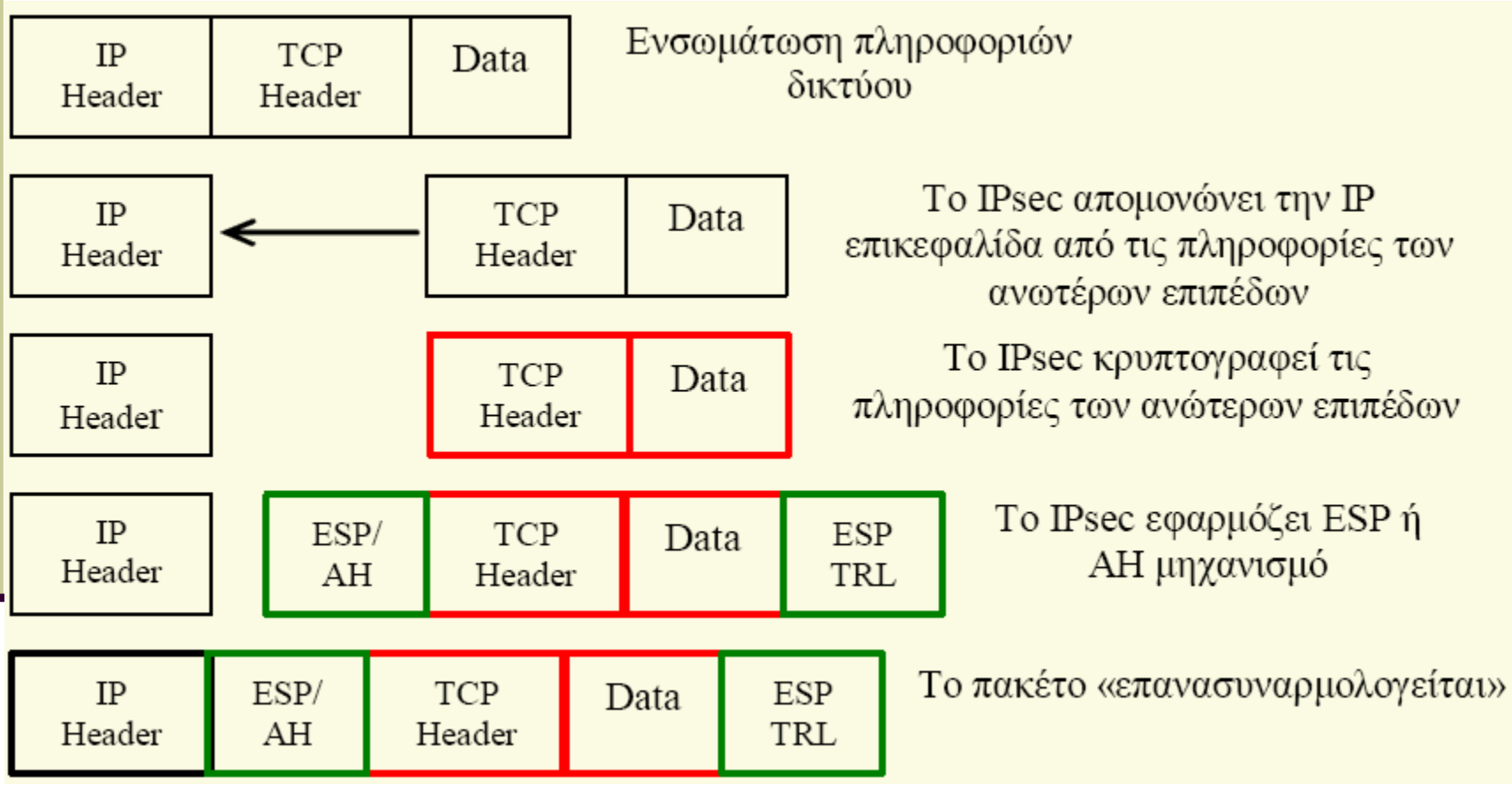
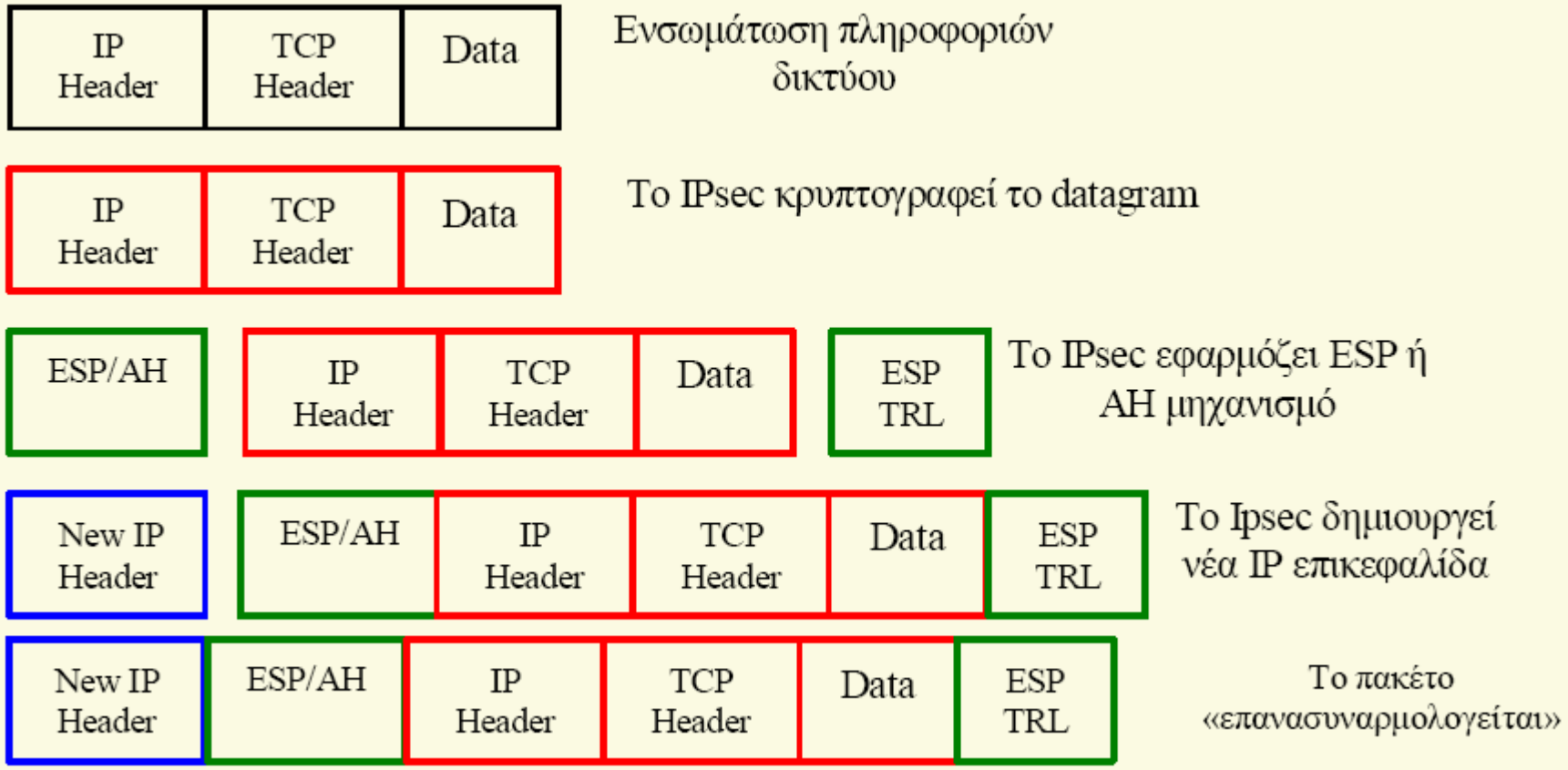


Figure 5.7 Applications of IPSec: (*a*) transport mode; (*b*) tunnel mode.

IPSec σε κατάσταση μεταγωγής (Transport mode)



IPSec σε κατάσταση διόδου (Tunnel mode)



Συμπεράσματα

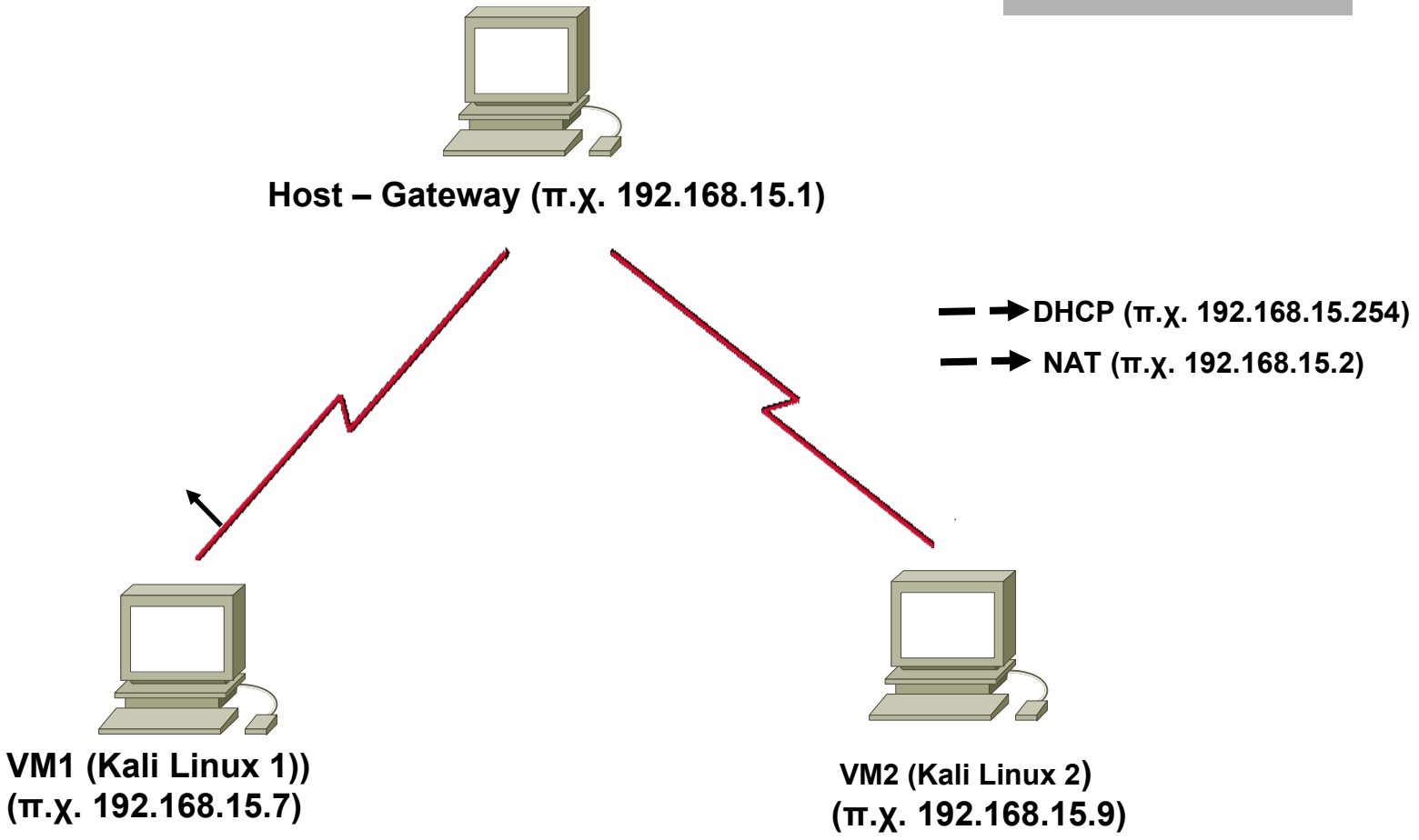
- Το IPSec προσφέρει υπηρεσίες ασφάλειας στο επίπεδο δικτύου
  - Αυθεντικοποίηση
  - Εμπιστευτικότητα
  - Ακεραιότητα
  - Προστασία από επεξεργασία κίνησης
- Έχει δύο μηχανισμούς ασφάλειας
  - Authentication Header - AH
  - Encapsulating Security Payload - ESP
- Για να εφαρμοστούν οι μηχανισμοί ασφάλειας, απαιτείται η κοινή γνώση Συσχετισμών Ασφάλειας (Security Associations – SA)
- Για την ανταλλαγή των SA χρειάζεται υποδομή ανταλλαγής κλειδιών (Internet Key Exchange)
- Δύο καταστάσεις λειτουργίας
  - Transport mode (μεταξύ απλών κόμβων)
  - Tunnel mode (δύο Gateway ή κόμβος – Gateway)
- Είναι διάφανο ως προς τα ανώτερα επίπεδα
- Προσθέτει επεξεργαστικό κόστος

4. Παράδειγμα υλοποίησης IPSec με τη χρήση του strongswan

Βήματα

1. Δημιουργία δύο Linux εικονικών μηχανημάτων σε virtualbox ή vmware
2. Εγκατάσταση strongswan (και στα δύο μέρη)
3. Δημιουργία και διαχείριση Κλειδιών
   - Δημιουργία δοκιμαστικής Αρχής Πιστοποίησης (σε ένα από τα δύο μέρη)
   - Δημιουργία κλειδιού/πιστοποιητικού ΑΠ
   - Δημιουργία κλειδιού/πιστοποιητικού για το αριστερό άκρο
   - Δημιουργία κλειδιού/πιστοποιητικού για το δεξί άκρο
   - Αντιγραφή/εγκατάσταση κλειδιών στα δύο άκρα
4. Διαμόρφωση αρχείων ipsec.conf και ipsec.secrets (και στα δύο άκρα)
5. Εκκίνηση / δοκιμή σύνδεσης

1) Εικονικό περιβάλλον με δύο κόμβους linux



Strongswan

- Το strongswan (http://www.strongwan.org/) είναι μία ανοικτή υλοποίηση του IPsec για το Linux με βάση την άδεια χρήσης GNU GPL v2.0
- Είναι απόγονος του FreeS/WAN
- Περιλαμβάνει υποστήριξη για transport/tunnel mode encryption
- Υποστηρίζει τις περισσότερες επεκτάσεις του IPSec όπως IKEv2, X.509 Ψηφιακά Πιστοποιητικά, NAT, opportunistic encryption
- Υποστηρίζει linux kernel 2.x, 3.x
- Παρέχει αναλυτική τεκμηρίωση και παραδείγματα (http://www.strongswan.org/documentation.html)

2) Εγκατάσταση IPSec (strongswan)

1ος τρόπος

Κατέβασμα κώδικα:

- wget http://download.strongswan.org/strongswan-x.x.x.tar.bz2

Αποσυμπίεση tarball

- tar xjvf strongswan-x.x.x.tar.bz2; cd strongswan-x.x.x

Διαμόρφωση

- ./configure --prefix=/usr --sysconfdir=/etc --<your-options>

Build, install

- make
- sudo make install

2ος τρόπος

- **apt-get install strongswan**

3) Δημιουργία και διαχείριση κλειδιών

1. Το strongswan περιλαμβάνει λειτουργίες Αρχής Πιστοποίησης (Certification Authority).
2. Για το παράδειγμά μας θα δημιουργήσουμε μία δοκιμαστική Αρχή Πιστοποίησης σε ένα από τα δύο εικονικά μηχανήματα.
3. Με τη βοήθεια της δοκιμαστικής ΑΠ θα δημιουργήσουμε και θα πιστοποιήσουμε τα κλειδιά των δύο άκρων της IPSec σύνδεσης.
4. Στη συνέχεια θα εγκαταστήσουμε τα απαραίτητα κλειδιά και στα δύο μέρη της σύνδεσης.
5. Τέλος θα εκκινήσουμε τη σύνδεση.

Δημιουργία δοκιμαστικής Αρχής Πιστοποίησης (Certification Authority)

Εκτελείται σε ένα VM το οποίο έχει και το ρόλο της Αρχής Πιστοποίησης

Περιγραφή	**Ενέργειες**
Δημιουργία φακέλου για τη ΑΠ	`cd /etc/ipsec.d`
	`mkdir myTestCA`
	`cd myTestCA`
Δημιουργία κλειδιού της ΑΠ (σε pem format)	`ipsec pki --gen --outform pem >myTestCAKey.pem`
Δημιουργία αυτο-υπογεγραμμένου πιστοποιητικού για την ΑΠ	`ipsec pki --self --in myTestCAKey.pem --dn "O=cs.unipi, CN=testCA" --ca --outform pem > myTestCACert.pem`
	`(για περαιτέρω βοήθεια: ipsec pki –self –help)`

Δημιουργία ζεύγους κλειδιών και πιστοποιητικού για το αριστερό άκρο

Εκτελείται σε ένα VM το οποίο έχει και το ρόλο της Αρχής Πιστοποίησης

Περιγραφή	**Ενέργειες**
Δημιουργία μυστικού κλειδιού αριστερού άκρου	`ipsec pki --gen --type rsa --size 2048 --outform pem >leftKey.pem`
Εξαγωγή δημόσιου κλειδιού και Δημιουργία/Υπογραφή πιστοποιητικού για το αριστερό άκρο, από την ΑΠ	`ipsec pki --pub --in leftKey.pem | ipsec pki --issue --cacert myTestCACert.pem --cakey myTestCAKey.pem --dn "O=cs.unipi, CN=left side" --flag ikeIntermediate --flag serverAuth --outform pem > leftCert.pem`
	`(για περαιτέρω βοήθεια: ipsec pki –issue –help)`

Δημιουργία ζεύγους κλειδιών και πιστοποιητικού για το δεξί άκρο

Εκτελείται σε ένα VM το οποίο έχει και το ρόλο της Αρχής Πιστοποίησης

Περιγραφή	**Ενέργειες**
Δημιουργία μυστικού κλειδιού δεξιού άκρου	`ipsec pki --gen --type rsa --size 2048 --outform pem > rightKey.pem`
Εξαγωγή δημόσιου κλειδιού και Δημιουργία/Υπογραφή πιστοποιητικού για το δεξί άκρο, από την ΑΠ	`ipsec pki --pub –in rightKey.pem | ipsec pki --issue --cacert myTestCACert.pem --cakey myTestCAKey.pem --dn "O=cs.unipi, CN=right side" --flag ikeIntermediate --flag serverAuth --outform pem > rightCert.pem`

Αντιγραφή κλειδιών και πιστοποιητικών στα δύο μέρη της σύνδεσης

Εκτελείται αντίστοιχα και από τα δύο μέρη της σύνδεσης

Αριστερό άκρο	**Δεξί άκρο**
Στο φάκελο `/etc/ipsec.d/private` αντιγράφουμε το ιδιωτικό κλειδί leftKey.pem	Στο φάκελο `/etc/ipsec.d/private` αντιγράφουμε το ιδιωτικό κλειδί rightKey.pem
Στο φάκελο /`etc/ipsec.d/certs` αντιγράφουμε το πιστοποιητικό leftCert.pem	Στο φάκελο `/etc/ipsec.d/certs` αντιγράφουμε το πιστοποιητικό rightCert.pem
Στο φάκελο `/etc/ipsec.d/cacerts` αντιγράφουμε το πιστοποιητικό της ΑΠ myTestCACert.pem	Στο φάκελο `/etc/ipsec.d/cacerts` αντιγράφουμε το πιστοποιητικό της ΑΠ myTestCACert.pem

4α) Διαμόρφωση αρχείου /etc/ipsec.conf

Εκτελείται αντίστοιχα και από τα δύο μέρη της σύνδεσης

Αριστερό άκρο	**Δεξί άκρο**
Στο αρχείο `/etc/ipsec.conf` προσθέτουμε την ακόλουθη σύνδεση	Στο αρχείο `/etc/ipsec.conf` προσθέτουμε την ακόλουθη σύνδεση

`conn <<connection name>>`
`  left=<<left ip address>>`
`  leftcert=leftCert.pem`
`  right=<<right ip address>>`
`  rightid="O=cs.unipi, CN=right side"`
`  keyexchange=ikev2`
`  auto=add`
	`conn <<connection name >>`
	`  left=<<left ip address>>`
	`  leftid="O=cs.unipi, CN=left side"`
	`  right=<<right ip address>>`
	`  rightcert=rightCert.pem`
	`  keyexchange=ikev2`
	`  auto=add`

4β) Διαμόρφωση αρχείου /etc/ipsec.secrets

Εκτελείται αντίστοιχα και από τα δύο μέρη της σύνδεσης

Αριστερό άκρο	**Δεξί άκρο**
Στο αρχείο `/etc/ipsec.secrets` προσθέτουμε ένα δείκτη προς το RSA ιδιωτικό κλειδί του αριστερού άκρου	Στο αρχείο `/etc/ipsec.secrets` προσθέτουμε ένα δείκτη προς το RSA ιδιωτικό κλειδί του δεξιού άκρου
`: RSA /etc/ipsec.d/private/leftKey.pem`	`: RSA /etc/ipsec.d/private/rightKey.pem`

5) Εκκίνηση σύνδεσης

Εκτελείται αντίστοιχα και από τα δύο μέρη της σύνδεσης

Αριστερό άκρο	**Δεξί άκρο**
`ipsec restart`	`ipsec restart`
`ipsec up <<connection name>>`	`ipsec up <<connection name>>`

Για τη δοκιμή της σύνδεσης χρησιμοποιείστε το wireshark

Βιβλιογραφία

1. IETF RFC 5996, Internet Key Exchange Protocol Version 2 (IKEv2), Sept. 2010, http://tools.ietf.org/html/rfc5996
2. IETF RFC 2409, Internet Key Exchange Protocol (IKE), Nov. 1998, http://tools.ietf.org/html/rfc2409
3. http://www.vocal.com/security/ikev2.html
4. Ασφάλεια δικτύων υπολογιστών, Δ. Γκρίτζαλης, Σ. Γκρίτζαλης, Σ. Κάτσικας, Εκδόσεις Παπασωτηρίου.
5. Strongswan, IPSec implementation, https://www. strongswan.org/
6. Internet Key Exchange Protocol Version 2, http://www.ietf.org/rfc/rfc5996.txt