1) Γιατί το TCP λέγεται ότι είναι συνδεσμικό;

Το TCP λέγεται ότι είναι συνδεσμικό επειδή πριν μπορέσει να αρχίσει μια διεργασία εφαρμογής να στέλνει δεδομένα σε μια άλλη, οι δύο διεργασίες πρέπει να κάνουν χειραψία μεταξύ τους, δηλαδή πρέπει να στείλουν κάποια προκαταρκτικά τμήματα η μία στην άλλη για να καθορίσουν τις παραμέτρους της επικείμενης μεταφοράς δεδομένων. Ως τμήμα του καθορισμού της σύνδεσης TCP και οι δύο πλευρές της σύνδεσης θα αρχικοποιήσουν πολλές μεταβλητές κατάστασης TCP που σχετίζονται με τη σύνδεση TCP.

2) Τι και γιατί κάνει η διαδικασία ταχείας επαναμετάδοσης (Fast retransmit) στο πρωτόκολλο TCP;

Εάν ο αποστολέας δεχθεί τρία διπλότυπα ACK για τα ίδια δεδομένα, εκλαμβάνει αυτήν την λήψη ως μια ένδειξη ότι το τμήμα, που ακολουθεί εκείνο το τμήμα για το οποίο έχει γίνει επιβεβαίωση τρεις φορές, έχει χαθεί. Στη περίπτωση που ληφθούν τρία διπλότυπα ACK, το TCP κάνει μια ταχεία επαναμετάδοση, επαναμεταδίδοντας το ελλείπον τμήμα πριν λήξει ο χρονομετρητής αυτού του τμήματος.

3) Ποια πεδία του IP δεδομενογράμματος/πακέτου εξετάζει ο υπολογιστής προορισμού για να καθορίσει ότι δύο από τα δεδομενογράμματα που λαμβάνει είναι ή όχι συνεχόμενα τεμάχια του μεγαλύτερου δεδομενογράμματος; Πώς καταλαβαίνει ότι είναι του ίδιου αρχικού πακέτου; Πώς είναι απολύτως σίγουρος ότι έχει λάβει και το τελευταίο τεμάχιο του αρχικού δεδομενογράμματος;

i. Ο υπολογιστής προορισμού, προκειμένου να καθορίσει αν δύο δεδομενογράμματα είναι συνεχόμενα τεμάχια ενός αρχικού μεγαλύτερου δεδομενογράμματος ή όχι, εξετάζει τρία πεδία του δεδομενογράμματος IP: το πεδίο ταυτότητας, ένδειξης και μετατόπισης κατάτμησης.

ii. Όταν δημιουργείτε ένα δεδομενόγραμμα, ο υπολογιστής αποστολής σφραγίζει το δεδομενόγραμμα με έναν αριθμό ταυτότητας, όπως και με τις διευθύνσεις προέλευσης και προορισμού. Τυπικά, ο υπολογιστής προσαυξάνει τον αριθμό ταυτότητας κατά ένα, για κάθε δεδομενόγραμμα που στέλνει. Όταν ένας δρομολογητής πρέπει να κατατμήσει ένα δεδομενόγραμμα, κάθε προκύπτον δεδομενόγραμμα σφραγίζεται με την διεύθυνση προέλευσης, την διεύθυνση προορισμού και τον αριθμό ταυτότητας του αρχικού δεδομενογράμματος. Όταν ο προορισμός δεχθεί μια σειρά δεδομενογραμμάτων από τον ίδιο υπολογιστή, μπορεί να εξετάσει τους αριθμούς ταυτότητας των δεδομενογραμμάτων, για να καθορίσει ποια από τα δεδομενογράμματα είναι τεμάχια του ίδιου μεγαλύτερου δεδομενογράμματος.

iii. Επειδή το IP είναι μία αναξιόπιστη υπηρεσία, ένα η περισσότερα τεμάχια μπορεί να μην φθάσουν ποτέ στον προορισμό. Για να είναι ο υπολογιστής προορισμού απολύτως σίγουρος ότι έχει λάβει το τελευταίο τεμάχιο του αρχικού δεδομενογράμματος, το τελευταίο τεμάχιο έχει ένα bit σημαία με τιμή 0, ενώ όλα τα άλλα τεμάχια έχουν σε αυτό το bit σημαία την τιμή 1.

4**) Περιγράψτε εν συντομία την αρχιτεκτονική client-server και την αρχιτεκτονική ομοτίμων.**

i. Σε μία αρχιτεκτονική client-server, υπάρχει ένας πάντα ενεργός υπολογιστής, που καλείται εξυπηρετητής, ο οποίος εξυπηρετεί αιτήσεις για υπηρεσίες από πολλούς άλλους υπολογιστές, που καλούνται πελάτες.

ii. Σε μία αρχιτεκτονική ομοτίμων, υπάρχει μικρή ή και καμία στήριξη σε αποκλειστικούς εξυπηρέτες σε κέντρα δεδομένων. Αντιθέτως, η εφαρμογή εκμεταλλεύεται την απευθείας επικοινωνία ανάμεσα σε ζεύγη κατά διαλείμματα συνδεδεμένων υπολογιστών που καλούνται ομότιμοι. Οι ομότιμοι δεν ανήκουν στον πάροχο της υπηρεσίας, αλλά είναι επιτραπέζιοι ή φορητοί υπολογιστές, που ελέγχονται από χρήστες και μάλιστα οι περισσότεροι από αυτούς βρίσκονται σε σπίτια, πανεπιστήμια και γραφεία. Επειδή οι ομότιμοι επικοινωνούν χωρίς να περνούν από έναν αποκλειστικό εξυπηρετητή αρχιτεκτονική καλείται αρχιτεκτονική ομοτίμων.

iii.

5) Πότε ο πελάτης web και ο εξυπηρετητής Web χρησιμοποιούν παραμένουσες συνδέσεις (persistent connections) και πότε μη παραμένουσες συνδέσεις (non-persistent connections).

Όταν γίνεται μια αλληλεπίδραση client-server επάνω στο TCP ο προγραμματιστής εφαρμογών πρέπει να πάρει μια σημαντική απόφαση. Πρέπει κάθε ζεύγος αίτησης-απόκρισης να στέλνεται πάνω σε μία ξεχωριστή σύνδεση TCP ή όλες οι αιτήσεις και οι αντίστοιχες αποκρίσεις να στέλνονται πάνω στην ίδια σύνδεση TCP. Κατά τη πρώτη προσέγγιση η εφαρμογή λέγεται ότι χρησιμοποιεί μη παραμένουσες συνδέσεις ενώ κατά τη δεύτερη παραμένουσες συνδέσεις.

6) Αναφέρεται μια σημαντική ομοιότητα και μια σημαντική διαφορά στη λειτουργία των πρωτοκόλλων SMTP & HTTP.

<u>Ομοιότητες</u> :

- Και τα δύο πρωτόκολλα χρησιμοποιούνται για μεταφορά αρχείων από έναν υπολογιστή σε έναν άλλο.
- Όταν μεταφέρουν τα αρχεία , και τα δύο πρωτοκόλλα χρησιμοποιούν παραμένουσες συνδέσεις.

<u>Διαφορές :</u>

- Το **HTTP** μεταφέρει αρχεία από έναν server WEB σε έναν client Web , ενώ το **SMTP** μεταφέρει αρχεία από έναν server ταχυδρομείου σε έναν άλλο server Ταχυδρομείου.

- Το **HTTP** είναι κυρίως ένα πρωτόκολλο προσέλκυσής (pull protocol) ενώ το **SMTP** είναι κυρίως ένα πρωτόκολλο προώθησης (push protocol) .

- Το **SMTP** απαιτεί κάθε μήνυμα περιλαμβανόμενου και του σώματος κάθε μηνύματος να είναι ASCII -7bit .Εάν το μήνυμα περιέχει χαρακτήρες που δεν είναι ASCII -7bit ή περιέχει δυαδικά δεδομένα τότε το μήνυμα πρέπει να κωδικοποιηθεί σε ASCII -7bit . Τα δεδομένα HTTP δεν έχουν αυτό το πρόβλημα.

7) Το μοντέλο υπηρεσίας IP είναι μια υπηρεσία παράδοσης βέλτιστης προσπάθειας . Τι σημαίνει αυτό?

Αυτό σημαίνει ότι το IP κάνει την καλύτερη προσπάθεια για να παραδώσει τμήματα ανάμεσα σε επικοινωνούντες υπολογιστές, αλλά δε δίνει καμία εγγύηση. Ειδικότερα δεν εγγυάται παράδοση τμήματος , δεν εγγυάται παράδοση τμημάτων με τη σωστή σειρά και δεν εγγυάται την ακεραιότητα των δεδομένων μέσα στα τμήματα. Γι' αυτούς τους λόγους το IP λέγεται πως είναι μια αναξιόπιστη υπηρεσία.

8) Για ποιους λόγους μια εφαρμογή θα επέλεγε το UDP και όχι το TCP πρωτόκολλο?

Α) Καλύτερος έλεγχος επιπέδου εφαρμογής σε ότι αφορά στο ποια δεδομένα στέλνονται και πότε

Β) Μη εγκαθίδρυση σύνδεσης.

Γ) Ανύπαρκτη κατάσταση σύνδεσης

Δ) Μικρή καθυστέρηση κεφαλίδας πακέτου .

9) Αναφέρεται τη χρήση του πεδίου <<ΑΘΡΟΙΣΜΑ ΕΛΕΓΧΟΥ>> στην κεφαλίδα του IP πακέτου σε σχέση με την χρήση του πεδίου <<ΑΘΡΟΙΣΜΑ ΕΛΕΓΧΟΥ>> στην κεφαλίδα του TCP πακέτου. Γιατί χρησιμοποιούνται δύο <<ΑΘΡΟΙΣΜΑΤΑ ΕΛΕΓΧΟΥ>>?

i. Το άθροισμα ελέγχου κεφαλίδας υπολογίζεται λαμβάνοντας 2 byte μέσα στην κεφαλίδα ως έναν αριθμό και αθροίζοντας αυτούς τους αριθμούς χρησιμοποιώντας αριθμητική 1-συμπλίρωμα.

ii. Το TCP/UDP στην πλευρά αποστολής βρίσκει το 1-συμπλίρωμα του αθροίσματος όλων των λέξεων 16-bit μέσα στο τμήμα και εάν βρεθεί κάποια υπερχείλιση κατά την διάρκεια υπολογισμού του αθροίσματος , αυτή προστίθεται στο λιγότερο σημαντικό bit. Το αποτέλεσμα αυτό τοποθετείται στο πεδίο αθροίσματος ελέγχου του τμήματος TCP/UDP.

iii. Στο επίπεδο IP γίνεται έλεγχος αθροίσματος μόνο της κεφαλίδας IP ενώ το άθροισμα ελέγχου TCP/UDP υπολογίζεται σε όλο το τμήμα TCP ή UDP. Επίσης, το TCP/UDP και το IP δεν χρειάζεται να ανήκουν και τα δύο στην ίδια στοίβα

πρωτοκόλλων. Το TCP μπορεί κατ' αρχήν να εκτελείται επάνω από ένα διαφορετικό πρωτόκολλο. (πχ το ATM) και το IP μπορεί να μεταφέρει δεδομένα που δεν θα περνούν στο TCP/UDP.

10) Τι ορίζει ένα πρωτόκολλο στην δικτύωση υπολογιστών?

Ένα πρωτόκολλο ορίζει την μορφή και την σειρά των τμημάτων που ανταλλάσσονται ανάμεσα σε δύο ή περισσότερες επικοινωνούσες οντότητες, όπως και τις ενέργειες που λαμβάνουν χώρα κατά την διάρκεια της μετάδοσης ή της λήψης ενός μηνύματος ή άλλου συμβάντος.

11) Αναφέρατε και περιγράψτε εν συντομία τις υπηρεσίες που περιλαμβάνει το μοντέλο υπηρεσίας TCP.

i. Η πλέον θεμελιώδης αρμοδιότητα του TCP είναι να επεκτείνει την υπηρεσία παράδοσης IP ανάμεσα σε δύο τερματικά συστήματα, σε μία υπηρεσία παράδοσης ανάμεσα σε δύο διεργασίες που εκτελούνται στα δύο τερματικά συστήματα. Η επέκταση της παράδοσης από υπολογιστή σε υπολογιστή σε παράδοση από διεργασία σε διεργασία καλείται πολυπλεξία και αποπολυπλεξία επιπέδου μεταφοράς.

ii. Το μοντέλο TCP παρέχει αρκετές πρόσθετες υπηρεσίες σε εφαρμογές. Πρώτο και κύριο , παρέχει αξιόπιστη μεταφορά δεδομένων. Χρησιμοποιώντας έλεγχο ροής, αριθμούς ακολουθίας , επιβεβαιώσεις και χρονομετρητές , το TCP εξασφαλίζει ότι τα δεδομένα παραδίδονται από τη διεργασία αποστολής στη διεργασία λήψης σωστά και με την ορθή σειρά.

iii. Το TCP παρέχει επίσης έλεγχο συμφόρησης. Ο έλεγχος συμφόρησης του TCP απαγορεύει σε οποιοδήποτε σύνδεση TCP να πλημμυρίσει τις ζεύξεις και τους μεταγωγείς ανάμεσα σε επικοινωνούντες υπολογιστές με υπερβολική ποσότητα κίνησης. Το TCP προσπαθεί να δώσει σε κάθε σύνδεση που διασχίζει μια ζεύξη δικτύου με συμφόρηση, ίσο εύρος ζώνης αυτής της ζεύξης.

12) Τί κάνει η υπηρεσία ελέγχου συμφόρησης (congestion control) στο TCP/IP stack ? Τι προσπαθεί να πετύχει? Αναφέρατε ένα πρωτόκολλο που παρέχει υπηρεσία ελέγχου συμφόρησης και ένα που δεν παρέχει.

Η υπηρεσία ελέγχου συμφόρησης του **TCP** απαγορεύει σε οποιαδήποτε σύνδεση TCP να πλημμυρίσει τις ζεύξεις και τους μεταγωγείς ανάμεσα σε επικοινωνούντες υπολογιστές με υπερβολική ποσότητα κίνησης. Το TCP προσπαθεί να δώσει σε κάθε σύνδεση που διασχίζει μια ζεύξη δικτύου με συμφόρηση, ίσο εύρος ζώνης αυτής της

ζεύξης . Ένα πρωτόκολλο που παρέχει η υπηρεσία ελέγχου συμφόρησης είναι το TCP και ένα που δεν παρέχει είναι το UDP.

13)Ποιος είναι ο χρόνος διαδρομής (RTT) στο TCP πρωτόκολλο και ποιος ο χρόνος αναμετάδοσης(time out) ?

i. Το δείγμα RTT που συμβολίζεται ως SampleRTT, για ένα τμήμα είναι ο χρόνος από την στιγμή που στέλνεται το τμήμα (δηλαδή παραδίδεται στο IP) μέχρι να ληφθεί μία επιβεβαίωση για το τμήμα.

ii. Ο χρόνος αναμετάδοσης πρέπει να είναι μεγαλύτερος από το χρόνο διαδρομής μετ' επιστροφής (RTT), αλλιώς θα γίνονται άχρηστες αναμεταδώσεις.

14) Πώς λειτουργεί η αργή εκκίνηση (slow start) στο TCP πρωτόκολλο πως η αποφυγή συμφόρησης?

1) Όταν εκκινήσει μια σύνδεση TCP , η τιμή της cwnd αρχικοποιείται σε μια μικρή τιμή τογ 1 MSS, γεγονός που έχει ως αποτέλεσμα έναν αρχικό ρυθμό αποστολής περίπου MSS/RTT. Αφού το διαθέσιμο εύρος ζώνης της σύνδεσης στον αποστολέα TCP μπορεί να είναι πολύ μεγαλύτερο από το MSS/RTT, ο αποστολέας TCP θα θέλει να βρει την ποσότητα του διαθέσιμου εύρος ζώνης γρήγορα. Έτσι κατά την κατάσταση αργή εκκίνηση, η τιμή της cwnd στο 1 MSS και αυξάνεται κατά 1 MSS κάθε φορά ένα μεταδοθέν τμήμα επιβεβαιώνεται.

2) Όταν γίνεται είσοδος στην κατάσταση αποφυγής συμφόρησης η τιμή της cwnd είναι περίπου το μισό της τιμής που είχε όταν παρατηρήθηκε συμφόρηση , για πρώτη φορά. Έτσι αντί να διπλασιάσει την τιμή της cwnd σε κάθε RTT το TCP υιοθετεί μια πιο συντηρητική προσέγγιση και αυξάνει την τιμή της cwnd κατά ένα μόνο MSS ανά RTT.

15)Ποια είναι η λειτουργία του πεδίου <<Πρωτόκολλο>> στα πεδία της κεφαλίδας του IP πακέτου/δεδομενογράμματος?

Αυτό το πεδίο χρησιμοποιείται μόνο όταν ένα δεδομενόγραμμα IP φτάσει στον τελικό προορισμό του. Η τιμή αυτού του πεδίου δηλώνει το συγκεκριμένο πρωτόκολλο επίπεδο μεταφοράς στο οποίο το τμήμα δεδομένων αυτού του δεδομενογράμματος IP πρέπει να παραδοθεί.

16) Τι ονομάζεται συνδεσμική υπηρεσία στο επίπεδο μεταφοράς? Τι προσπαθεί να πετύχει ο έλεγχος συμφόρησης στο επίπεδο μεταφοράς? Αναφέρετε αν τα πιο γνωστά επίπεδα μεταφοράς TCP και UDP υλοποιούν ή όχι συνδεσμική υπηρεσία και έλεγχο συμφόρησης.

i. Το TCP κάνει τον πελάτη και τον εξυπηρετητή να ανταλλάζουν πληροφορίες ελέγχου επιπέδου μεταφοράς μεταξύ τους πριν τα μηνύματα επιπέδου εφαρμογής αρχίσουν να ρέουν. Αυτή η αποκαλούμενη διαδικασία χειραψίας ,

προειδοποιεί τον πελάτη και τον εξυπηρετητή επιτρέποντας τους να προετοιμαστούν για μία ανταλλαγή πακέτων. Μετά τη φάση χειραψίας λέγεται ότι υπάρχει μια σύνδεση TCP.

ii. Ο έλεγχος συμφόρησης του TCP απαγορεύει σε οποιαδήποτε σύνδεση TCP να πλημμυρίσει τις ζεύξεις και τους μεταγωγής ανάμεσα σε επικοινωνούντες υπολογιστές με υπερβολική ποσότητα κίνησης.

iii. Το μοντέλο TCP υλοποιεί συνδεσμική υπηρεσία και έλεγχο συμφόρησης ενώ το μοντέλο UDP όχι.

17) Το πρωτόκολλο HTTP είναι ακαταστατικό πρωτόκολλο ή διατηρεί την κατάσταση(state) των χρηστών/συνδέσεων? Το πρωτόκολλο FTP είναι ακαταστατικό πρωτόκολλο ή διατηρεί την κατάσταση (state) των χρηστών/συνδέσεων? Πώς επηρεάζει την απόδοση της μεταφοράς αρχείων αν διατηρεί κατάσταση ή όχι το πρωτόκολλο?

i. Επειδή ένας εξυπηρετητής HTTP δεν κρατά πληροφορίες για τους πελάτες θεωρείται ένα ακαταστατικό πρωτόκολλο.

ii. Κατά τη διάρκεια μίας συνόδου , ο εξυπηρετητής FTP πρέπει να διατηρεί την κατάσταση (state) για τον χρήστη.

iii. Η παρακολούθηση αυτών των πληροφοριών κατάστασης για κάθε σύνοδο χρήστη περιορίζει σημαντικά τον συνολικό αριθμό συνόδων που μπορεί να διατηρεί το FTP ταυτόχρονα. Το HTTP , από την άλλη είναι ακαταστατικό δεν χρειάζεται να παρακολουθεί καμία κατάσταση χρήστη.

18) Τι δηλώνει ο αριθμός ακολουθίας (sequence number) σε ένα TCP τμήμα? Τι δηλώνει ο αριθμός επιβεβαίωσης (ack) σε ένα TCP τμήμα? Το TCP παρέχει συσσωρευτικές ή ανεξάρτητες επιβεβαιώσεις?

i. Το TCP θεωρεί τα δεδομένα ως ένα αδόμητο , αλλά διατεταγμένο ρεύμα bytes. Η χρήση από το των αριθμών ακολουθίας αντανακλά αυτήν την άποψη, κατά το ότι οι αριθμοί ακολουθίας αναφέρονται στο ρεύμα των μεταδιδόμενων byte κι όχι στην σειρά των μεταδιδόμενων τμημάτων. Ο αριθμός ακολουθίας για ένα τμήμα είναι λοιπόν ο αύξων αριθμός του πρώτου byte μέσα στο τμήμα απ' το συνολικό ρεύμα από byte.

ii. Το TCP είναι αμφίδρομο, οπότε ο υπολογιστής Α μπορεί να λαμβάνει δεδομένα από τον υπολογιστή Β , ενώ στέλνει δεδομένα στον υπολογιστή Β ως τμήμα της ίδιας σύνδεσης TCP . Καθ' ένα από τα τμήματα που φθάνουν από τον υπολογιστή Β έχει έναν αριθμό ακολουθίας για τα δεδομένα που ρέουν από τον

Β προς τον Α. Ο αριθμός επιβεβαίωσης που θέτει ο υπολογιστής Α στο τμήμα του είναι ο αριθμός ακολουθίας του επόμενου byte που περιμένει ο υπολογιστής Α από τον υπολογιστή Β.

Επειδή το TCP επιβεβαιώνει μόνο byte μέχρι το πρώτο ελλείπον byte στο ρεύμα, το λέγεται ότι παρέχει συσσωρευτικές επιβεβαιώσεις.

19) Αναφέρατε μια σημαντική ομοιότητα και σημαντική διαφορά στη λειτουργία των πρωτοκόλλων FTP & HTTP.

Ομοιότητες:

i. Τα HTTP kai FTP είναι και τα δύο πρωτόκολλα μεταφοράς αρχείων και έχουν πολλά κοινά χαρακτηριστικά , για παράδειγμα και τα δύο εκτελούνται επάνω από το TCP.

Διαφορές:

i. Η πιο χτυπητή διαφορά είναι ότι το FTP χρησιμοποιεί δύο παράλληλες συνδέσεις ΤΣΠ για μεταφορά ενός αρχείου, μια σύνδεση ελέγχου και μία σύνδεση δεδομένων. Η σύνδεση ελέγχου χρησιμοποιείται για αποστολή πληροφοριών ελέγχου ανάμεσα σε δύο υπολογιστές-πληροφοριών όπως όνομα χρήστη, συνθηματικό ,εντολές για αλλαγή ενός απομακρυσμένου καταλόγου και εντολές για τοποθέτηση και λήψη αρχείων. Η σύνδεση δεδομένων χρησιμοποιείται για να κάνει την πραγματική αποστολή ενός αρχείου.

ii. Επειδή το FTP χρησιμοποιεί μια ξεχωριστή σύνδεση ελέγχου , το FTP λέγεται ότι στέλνει τις πληροφορίες ελέγχου εξωζωνικά (out of bound) .Το HTTP στέλνει γραμμές κεφαλίδας αιτήσεων και αποκρίσεων μέσω της ίδιας σύνδεσης TCP , που μεταφέρει το ίδιο το μεταφερόμενο αρχείο . Γι’ αυτόν το λόγο το HTTP λέγεται ότι στέλνει τις πληροφορίες ελέγχου του ενδοζωνικά.

iii.

20) Τι προσδιορίζει το πεδίο Χρόνου Ζωής (TTL) σε ένα IP πακέτο? Τι εγγυάται?

Το πεδίο χρόνου ζωής time to live περιλαμβάνεται για να διασφαλίσει ότι τα δεδομενογράμματα δεν κυκλοφορούν για πάντα μέσα στο δίκτυο. Αυτό το πεδίο μειώνεται κατά ένα κάθε φορά που γίνεται επεξεργασία του δεδομενογράμματος από έναν δρομολογητή. Εάν το πεδίο TTL φτάσει στο 0, το δεδομενόγραμμα πρέπει να απορριφθεί.

21) Για ποιους σκοπούς χρησιμοποιεί το HTTP τα cookies; Γιατί αμφισβητείται η χρήση τους; Αναφέρεται ένα παράδειγμα.

i. Είναι συχνά επιθυμητό για έναν ιστότοπο να αναγνωρίζει χρήστες, είτε επειδή ο εξυπηρετητής επιθυμεί να περιορίσει την προσπέλαση χρηστών ή επειδή θέλει να παρέχει περιεχόμενο ως μία συνάρτηση της ταυτότητας του χρήστη.
ii. Αν και τα cookies συχνά απλοποιούν τις αγορές στο διαδίκτυο για τον χρήστη, παραμένουν άκρως αμφισβητήσιμα, επειδή μπορούν να θεωρηθούν ως παραβίαση της ιδιωτικότητα. Χρησιμοποιώντας έναν συνδυασμό cookies και πληροφοριών λογαριασμού, που παρέχονται από τον χρήστη, ένας ιστότοπος μπορεί να μάθει πολλά πράγματα για έναν χρήστη και πιθανώς να πωλήσει αυτές τις γνώσεις της σε κάποιον άλλο.

22) Το TCP παρέχει αξιόπιστη μεταφορά δεδομένων .Τι εξασφαλίζει η αξιόπιστη μεταφορά δεδομένων και τι χρησιμοποιεί?

Το TCP δημιουργεί μια υπηρεσία αξιόπιστης μεταφοράς δεδομένων επάνω από την αναξιόπιστη υπηρεσία βέλτιστής προσπάθειας του IP. Η υπηρεσία αξιόπιστης μεταφοράς δεδομένων του TCP εξασφαλίζει ότι το ρεύμα δεδομένων που διαβάζει μία διεργασία από τον ενταμιευτή λήψης του TCP είναι αναλλοίωτο , χωρίς κενά, χωρίς διπλά αντίγραφα και με τη σωστή σειρά, δηλαδή το ρεύμα δεδομένων είναι ακριβώς το ίδιο ρεύμα δεδομένων που στάλθηκε από το τερματικό σύστημα στην άλλη πλευρά της σύνδεσης. Η υπηρεσία αξιόπιστης μεταφοράς δεδομένων του TCP χρησιμοποιεί μόνο λέξεις χρόνου ώστε να επανακάμψει από χαμένα τμήματα κατόπιν παρουσιάζουμε μια πληρέστερη περιγραφή , που χρησιμοποιεί διπλότυπες επιβεβαιώσεις εκτός των λήξεων χρόνου.

25) Το Traceroute υλοποιείται με μηνύματα ICMP. Ποιος είναι ο σκοπός του Traceroute; Πώς λειτουργεί;

Το Traceroute χρησιμοποιείται για να μετρήσουμε την καθυστέρηση από άκρο σε άκρο σε ένα δίκτυο υπολογιστών. Υποθέστε πως υπάρχουν N-1 δρομολογητές ανάμεσα στην προέλευση και στον προορισμό. Τότε η προέλευση θα στείλει N ειδικά πακέτα μέσα στο δίκτυο, με κάθε πακέτο να έχει την διεύθυνση του τελικού του προορισμού. Όταν ο N-οστός δρομολογητής λάβει το N-οστό πακέτο, ο δρομολογητής δεν προωθεί το πακέτο στον προορισμό του, αλλά αντίθετα στέλνει ένα μήνυμα πίσω στην προέλευση. Επίσης, όταν ο υπολογιστής προορισμού λάβει το N-οστό πακέτο, και αυτός επίσης στέλνει ένα μήνυμα πίσω στην προέλευση. Η προέλευση καταγράφει τον χρόνο που διέρρευσε από την ώρα που στέλνει ένα πακέτο ως την ώρα που λαμβάνει το αντίστοιχο μήνυμα επιστροφής, επίσης καταγράφει το όνομα και την διεύθυνση του δρομολογητή που επιστρέφει το μήνυμα. Το Traceroute επαναλαμβάνει το πείραμα 3 φορές, οπότε στην πραγματικότητα στέλνει 3xN πακέτα προς τον πρόσημο.

Ποιες είναι οι τρείς διαφορές ανάμεσα στο HTTP και SMTP;

1. Το HTTP είναι πρωτόκολλο προσέλκυσης ενώ το SMTP είναι προώθησης

2. Το HTTP είναι stateless.

3. Το HTTP μεταφέρει αρχεία αναμεσά στον Web Server και τον client ενώ το SMTP μεταφέρει email από τους mail Servers

Ποια πεδία του IP δεδομενογράμματος/πακέτου εξετάζει ο υπολογιστής προορισμού και πως καθορίζει ότι δύο δεδομενογράμματα που καθορίσθηκε ότι ανήκουν στο ίδιο μεγαλύτερο δεδομενογράμμα είναι ή όχι συνεχόμενα τεμάχια του μεγαλύτερου δεδομενογράμματος;

Τα πεδία που ελέγχει είναι ο αριθμός ταυτότητας identification number, ο αριθμός ένδειξης(Flags) και ο αριθμός μετατόπισης κατάτμησης (fragment offset) στο δεδομενόγραμμα IP. Όταν τα πεδία IP source και identifier είναι ίδια, σημαίνει ότι τα δυο datagrams ανήκουν στο ίδιο αρχικό.

Τι είναι το παράθυρο λήψης (receive window) στο TCP πρωτόκολλο; Τι είναι το παράθυρο συμφόρησης (congestion window); Πιο παράθυρο χρησιμοποιεί ο αποστολέας TCP;

Το παράθυρο λήψης είναι ένα buffer εισερχόμενων δεδομένων τα οποία δεν έχουν επεξεργαστεί ακόμα από την εφαρμογή. Το μέγεθος του παραθύρου ανακοινώνει τον αριθμό των bytes που είναι ελευθέρα στο buffer εισερχομένων. Το παράθυρο συμφόρησης εφαρμόστηκε για να αποφευχθεί η υπέρβαση ορισμένων δρομολογητών στη μέση της διαδρομής δικτύου. Ο αποστολέας με κάθε τμήμα δεδομένων που στέλνει, αυξάνει ελαφρώς το παράθυρο συμφόρησης.

Τι είναι διπλότυπο ACK στο TCP πρωτόκολλο; Γιατί υπάρχουν διπλότυπα ACK; Με πιο σκεπτικό η διαδικασία ταχείας αναμετάδοσης (fast retransmit) κάνει αναμετάδοση πριν λήξει ο χρονομετρητής στο πρωτόκολλο TCP;

Το διπλότυπο ACK στο TCP, εμφανίζεται όταν χαθεί η επιβεβαίωση πακέτου πριν φτάσει η λήξη του χρόνου. Ένα διπλότυπο ACK είναι ένα ACK το οποίο κάνει επιβεβαίωση λήψης για για ένα πακέτο που ο αποστολέας έχει ήδη λάβει επιβεβαίωση. Για τη ταχεία αναμετάδοση, επειδή ο αποστολέας στέλνει συχνά ένα μεγάλο αριθμό τμημάτων απανωτά, εάν χαθεί ένα τμήμα κατά πάσα πιθανότητα θα υπάρχουν πολλά διπλότυπα ACK. Στη περίπτωση που βρεθούν τρία απανωτά διπλότυπα ACK, το TCP κάνει μια ταχεία μετάδοση μεταδίδοντας ξανά το τμήμα που λείπει πριν λήξη ο χρόνος του τμήματος.

Σ/Λ

1. Το TCP Reno αποφεύγει τους χαμηλούς ρυθμούς μετάδοσης της αργής εκκίνησης χάρη στο μηχανισμό «ταχείας επαναμετάδοσης». [ΛΑΘΟΣ, ο μηχανισμός λέγεται ταχεία ανάκαμψη]

2. Γενικά όταν μία μετάδοση TCP και μία μετάδοση UDP χρησιμοποιούν από κοινού ένα σχετικά μικρό εύρος ζώνης, τότε το UDP θα κάνει κατάχρηση του διαθέσιμου εύρους εις βάρος του TCP. [Σωστό, το TCP είναι connection-oriented-service και έχει μηχανισμό ελέγχου συμφόρησης. Το UDP δεν έχει πολλές υπηρεσίες και είναι και connectionless. Θα κάνει καταχρηση γιατί θα στέλνει δεδομένα συνεχώς καθώς δεν παρέχει έλεγχος συμφόρησης.]

3. **Το TCP σχεδιάστηκε για να υποστηρίξει μεταδόσεις σε σταθερά και ασύρματα δίκτυα.** [ΛΑΘΟΣ, σχεδιάστηκε για διαδικτυακές λειτουργίες]

4. **Η «ταχεία ανάκαμψη» οδηγεί γενικά σε υψηλότερη μέση τιμή του παραθύρου συμφόρησης.** [ΣΩΣΤΟ, γιατί η μέση τιμή του congestion window παίρνει υψηλότερη τιμή και στην συνέχεια αυξάνεται αντί να ξεκινήσει από την αρχή]

Ποια πεδία του IP δεδομενογράμματος/πακέτου εξετάζει ο υπολογιστής προορισμού και πως καθορίζει ότι δύο από τα δεδομενογράμματα που λαμβάνει είναι τεμάχια του ίδιου μεγαλύτερου δεδομενογράμματος;

Τα πεδία που θα εξεταστούν είναι ο αριθμός ταυτότητας, ένδειξης και μετατόπισης κατάτμησης στο δεδομενόγραμμα Για να είναι σίγουρος ο υπολογιστής προορισμού ότι έχει λάβει το τελευταίο τεμάχιο του αρχικού δεδομενογράμματος, καταλαβαίνει ότι το flag του τελευταίου bit έχει τιμή 0, ενώ όλα τα άλλα τεμάχια θα έχουν το flag = 1. Για να καταλάβει αν λείπει ένα τεμάχιο και για να γίνει η σύνθεση με σωστή σειρά το πεδίο μετατόπισης κατάτμησης χρησιμοποιείται για να καθορίσει που μπαίνει κάθε τεμάχιο μέσα στο αρχικό δεδομενόγραμμα IP

Το TCP παρέχει αξιόπιστη μεταφορά δεδομένων (reliable data transfer). Τι εξασφαλίζει η αξιόπιστη μεταφορά δεδομένων και τι χρησιμοποιεί;

(1)Με αυτόν τον τρόπο την αξιόπιστη μεταφορά δεδομένων το TCP εξασφαλίζει ότι τα δεδομένα αποστέλλονται σωστά και με σωστή σειρά. Δηλαδή δεν υπάρχει αλλοίωση στα δεδομένα και δεν έχουν φτάσει με λάθος σειρά. Οι τρόποι που γίνετε αυτό είναι με ελέγχους ροής, αριθμούς ακολουθίας, χρονομετρητές και επιβεβαιώσεις.

(2 ακριβώς από βιβλίο) Το TCP δημιουργεί μία υπηρεσία αξιόπιστης μεταφοράς δεδομένων πάνω από την αναξιόπιστη υπηρεσία βέλτιστης προσπάθειας του IP. Η υπηρεσία αξιόπιστης μεταφοράς δεδομένων του TCP εξασφαλίζει ότι το ρεύμα δεδομένων που διαβάζει μία διεργασία από τον ενταμιευτή λήψης της του TCP είναι αναλλοίωτο, χωρίς κενά, χωρίς διπλά αντίγραφα και με την σωστή σειρά. Δηλαδή το

ρεύμα byte είναι ακριβώς το ίδιο ρεύμα byte που στάλθηκε από το τερματικό σύστημα στην άλλη πλευρά της σύνδεσης. Το TCP χρησιμοποιεί χρονομετρητή επαναμετάδοσης.

Τι είναι διπλότυπο ACK στο TCP πρωτόκολλο; Γιατί υπάρχουν διπλότυπα ACK;Τι κάνει η διαδικασία ταχείας επαναμετάδοσης (fast retransmit) στο πρωτόκολλο TCP και με ποιο σκεπτικό;

Το διπλότυπο ACK στο TCP πρωτόκολλο εμφανίζεται όταν χαθεί η επιβεβαίωση πακέτου πριν συμβεί το συμβάν λήξης χρόνου. Ένα διπλότυπο ACK είναι ένα ACK το οποίο κάνει επιβεβαίωση λήψης για ένα πακέτο για το οποίο ο αποστολέας έχει λάβει μια προηγούμενη επιβεβαίωση. Όσον αφορά την ταχεία αναμετάδοση, επειδή ο αποστολέας στέλνει συχνά ένα μεγάλο αριθμό τμημάτων το ένα πίσω από το άλλο, εάν χαθεί ένα τμήμα, κατά πάσα πιθανότητα θα υπάρχουν πολλά διπλά ACK , το ένα πίσω από το άλλο. Εάν ο αποστολέας TCP δεχθεί τρία διπλότυπα ACK για τα ίδια δεδομένα, εκλαμβάνει αυτήν την λήψη ως μία ένδειξη ότι το τμήμα, που ακολουθεί εκείνο το τμήμα για το οποίο έχει γίνει επιβεβαίωση 3 φορές, έχει χαθεί. Στην περίπτωση που ληφθούν αυτά τα 3 διπλότυπα ACK το TCP κάνει μία ταχεία μετάδοση, επαναμεταδίδοντας το ελλείπον τμήμα πριν λήξει ο χρονομετρητής αυτού του τμήματος.

Στα πρωτόκολλα Πολλαπλής Προσπέλασης με Ανίχνευση Φέροντος (CSMA), αφού όλοι οι κόμβοι κάνουν ανίχνευση φέροντος, γιατί γίνονται συγκρούσεις; Τι συμβαίνει αν οι κόμβοι δεν κάνουν ανίχνευση σύγκρουσης και τι συμβαίνει αν κάνουν ανίχνευση σύγκρουσης και σε ποια από τις δύο περιπτώσεις έχουμε καλύτερη απόδοση;

Συγκρούσεις στο CSMA έχουμε λόγω της καθυστέρησης διάδοσης καναλιού. Δηλαδή τον χρόνο που χρειάζεται ένα σήμα για να διαδοθεί από έναν κόμβο σε έναν άλλον. Αν για παράδειγμα ένας κόμβος Α δει ότι δεν υπάρχει μετάδοση από τους υπόλοιπους , ξεκινάει να στέλνει. Παράλληλα αν ένας κόμβος Β δεν προλάβει να εντοπίσει το μήνυμα που έχει ξεκινήσει ήδη να αποστέλλει ο Α , τότε ξεκινάει να στέλνει και αυτό , με αποτέλεσμα να υπάρξουν παρεμβολές στο πακέτο του Α.

Αν οι κόμβοι δεν κάνουν ανίχνευση σύγκρουσης τότε ο κόμβος- αποστολέας έχει τελειώσει με το πλαίσιο του

Σε περίπτωση που υπάρξει σύγκρουση , χρησιμοποιείται ο αλγόριθμος δυαδικής εκθετικής υποχώρησης. Δηλαδή, περιμένει ένα διάστημα μέχρι να ξαναστείλει, το οποίο αυξάνεται κάθε φορά που εντοπίζεται σύγκρουση

-Τι συμβαίνει όταν ένα πακέτο χαθεί στο TCP; Πώς δρα ο παραλήπτης;

Το πρωτόκολλο ελέγχου μετάδοσης (TCP) ανιχνεύει την απώλεια πακέτων, και εκτελεί αναμετάδοση για το κάθε πακέτο το οποίο δεν στάλθηκε, είτε έπειτα από μία ειδοποίηση, είτε μετά από συγκεκριμένο χρόνο. Το πως καθορίζεται το πότε θα σταματήσουν να στέλνονται τα πακέτα, εξαρτάται καθαρά από την υλοποίηση, αλλά μετά από έναν αόριστο αριθμό χαμένων πακέτων, ο κεντρικός υπολογιστής θεωρείται μη λειτουργικός. Ο τρόπος όπου καταλαβαίνει ο κεντρικός υπολογιστής ότι ένα πακέτο έχει χαθεί, είναι μέσω του παραλήπτη. Όταν ένας δέκτης TCP σηματοδοτεί ότι δεν έχει ληφθεί ένα πακέτο, ή εάν δεν λαμβάνεται καθόλου επιβεβαίωση, ο αποστολέας TCP υποθέτει ότι το πακέτο είχε χαθεί και στέλνει ξανά το πακέτο (δεν βρίσκω κάτι άλλο).

-Το CSMA/CD πως μοιάζει με ανθρώπινη συμπεριφορά;

Ως άνθρωποι έχουμε ανθρώπινα πρωτόκολλα, τα οποία μας επιτρέπουν όχι μόνο να φερόμαστε πιο πολιτισμένα, αλλά επίσης να μειώνουμε τον χρόνο που γίνονται οι συγκρούσεις με άλλους σε συζητήσεις και συνεπώς να αυξάνονται τα δεδομένα που ανταλλάσσουμε κατα την διάρκεια των συζητήσεων. Συγκεκριμένα, υπάρχουν δύο σημαντικοί κανόνες για ευγενική συζήτηση μεταξύ ανθρώπων:

- Άκου πριν να μιλήσεις. Εάν κάποιος άλλος μιλά, περίμενε μέχρι να τελειώσει. Στον κόσμο της δικτύωσης, αυτό καλείται ανίχνευση φέροντος (carrier sensing) - ένας κόμβος κάνει ακρόαση στο κανάλι πριν μεταδώσει. Εάν ένα πλαίσιο από έναν άλλο κόμβο μεταδίδεται αυτήν την στιγμή μέσα σε κανάλι, τότε ο κόμβος περιμένει μέχρι να ανιχνεύσει ‘ότι δεν υπάρχει μετάδοση για ένα μικρό χρονικό διάστημα και μετά αρχίζει την μετάδοση
- Εάν κάποιος άλλος αρχίσει να μιλά ταυτόχρονα, σταμάτα να μιλάς. Στον κόσμο της δικτύωσης αυτό καλείται ανίχνευση σύγκρουσης (collision detection) - ένας κόμβος που μεταδίδει κάνει ακρόαση στο κανάλι ενώ μεταδίδει. Εάν ανιχνεύσει ότι ένας άλλος κόμβος μεταδίδει ένα πλαίσιο και κάνει παρεμβολές, τότε σταματά να μεταδίδει και περιμένει ένα τυχαίο χρονικό διάστημα πριν να επαναλάβει τον κύκλο ανίχνευσης και μετάδοσης όταν το κανάλι είναι αδρανές.

1. Το UDP θεωρείται connectionless πρωτόκολλο διότι δεν εγγυάται την παράδοση των πακέτων. [Λάθος, θεωρείται connectionless διότι δεν προηγείται κάποια αρχική χειραψία.]

2. Τα παράθυρα συμφόρησης & λήψης (cwnd/rwnd) υπολογίζονται από τον παραλήπτη του TCP. [Λάθος. Το cwnd από τον αποστολέα. Το rwnd από τον παραλήπτη.]

3. Η επικεφαλίδα TCP διαθέτει πεδίο για την ενημέρωση σχετικά με το παράθυρο λήψης (rwnd).[Σωστό διότι είναι πεδίο που χρειάζεται για τον έλεγχος συμφόρησης]

4. Το TCP Reno αποφεύγει τους χαμηλούς ρυθμούς μετάδοσης της αργής εκκίνησης χάρη στο μηχανισμό «ταχείας επαναμετάδοσης». [Λάθος, ο μηχανισμός λέγεται ταχεία ανάκαμψη. Στην αρχή υπάρχει εκθετική αύξηση, μετά το ssthresh αυξάνεται γραμμικά. όταν υπάρχει συμφόρηση πέφτει σε μία μικρότερη τιμή από την οποία βρέθηκε η συμφόρηση και αυξάνεται ξανά γραμμικά]

5. Γενικά όταν μία μετάδοση TCP και μία μετάδοση UDP χρησιμοποιούν από κοινού ένα σχετικά μικρό εύρος ζώνης, τότε το UDP θα κάνει κατάχρηση του διαθέσιμου εύρους εις βάρος του TCP. [Σωστό. Το TCP είναι connection-oriented-service και έχει μηχανισμό ελέγχου συμφόρησης. Οπότε για να κάνει χρήση θα πρέπει να γίνει το handshake. Το UDP δεν έχει πολλές υπηρεσίες και είναι connectionless, δεν έχει εγγύηση ότι θα φτάσει το μήνυμα δηλαδή απλά στέλνει χωρίς να ξέρει αν θα φτάσει ή πως θα φτάσει. Είναι λογικό να κάνει κατάχρηση του εύρους ζώνης γιατί απλά θα στέλνει συνεχόμενα. Στο UDP δεν υπάρχει έλεγχος συμφόρησης.]

6. Το TCP σχεδιάστηκε για να υποστηρίξει μεταδόσεις σε σταθερά και ασύρματα δίκτυα. [Λάθος, Το TCP σχεδιάστηκε για να υποστηρίζει διαδικτυακές λειτουργίες]

7. Η «ταχεία ανάκαμψη» οδηγεί γενικά σε υψηλότερη μέση τιμή του παραθύρου συμφόρησης. [Σωστό, διότι η μέση τιμή του παραθύρου συμφόρησης παίρνει υψηλότερη τιμή (9*MSS) και στην συνέχεια αυξάνεται γραμμικά αντί να ξεκινήσει από την αρχική τιμή]

Πυρήνας του Δικτύου

Μεταγωγή πακέτου

Η μεταγωγή πακέτου (packet switching) είναι μια τεχνική που χρησιμοποιείται σε δίκτυα επικοινωνίας με σκοπό να προωθηθεί μια πληροφορία από ένα πομπό σε ένα δέκτη. Στην μεταγωγή πακέτου τα προς μετάδοση μηνύματα τεμαχίζονται σε πακέτα μικρού αριθμού bytes.

Μεταγωγή κυκλώματος

Η μεταγωγή κυκλώματος (circuit switching) είναι μια τεχνική που χρησιμοποιείται σε δίκτυα επικοινωνίας με σκοπό να προωθηθεί μια πληροφορία από ένα πομπό σε ένα δέκτη.

Στην μεταγωγή κυκλώματος για να επικοινωνήσουν δυο σταθμοί αποκαθίσταται μια αποκλειστική φυσική σύνδεση μεταξύ τους που διατηρείται σταθερή σε όλη την διάρκεια της επικοινωνίας. Αποτελείται από μια σειρά συνδέσεων μεταξύ των κόμβων του δικτύου.

Μεταγωγή Κυκλώματος vs Μεταγωγή Πακέτου

Μεταγωγή πακέτου: φθηνότερη, υποστηρίζει πιο πολλούς χρήστες στατιστικά, μεγαλύτερη διαθέσιμη ταχύτητα σε κάθε χρήστη, χρησιμοποιείται στο internet

Μεταγωγή κυκλώματος: Σταθερός ρυθμός μεταφοράς, δέσμευση πόρων κατά απαίτηση, χρησιμοποιείται στην τηλεφωνία

Τί ορίζει ένα πρωτόκολλο στη δικτύωση υπολογιστών;

Ως Πρωτόκολλο επικοινωνίας ορίζεται ένα σύνολο κανόνων συμφωνημένων και από τα δυο επικοινωνούντα μέρη και που εξυπηρετούν την μεταξύ τους ανταλλαγή πληροφοριών.

Επίπεδο Εφαρμογής

Τι ορίζει το πρωτόκολλο επιπέδου εφαρμογής;

- Τους τύπους των μηνυμάτων που ανταλλάσσονται (απόκρισης, απάντησης)
- Την σύνταξη των μηνυμάτων (πεδία)
- Την σημασιολογία/σημασία πληροφοριών
- Κανόνες καθορισμού πότε και πως μια διεργασία στέλνει μηνύματα και ανταποκρίνεται

Πρωτόκολλα προσπέλασης ταχυδρομείου-πλευρά πράκτορα χρήστη
POP3 (Post Office Protocol 3)

- Εξουσιοδότηση (username, password), συναλλαγή (list, retr, dele), έξοδος (quit)
- Έκδοση εντολών, απαντήσεις OK ή ERR
- Τα μηνύματα σημαίνονται για διαγραφή ή όχι και ύστερα από το τέλος της σύνδεσης διαγράφονται όσα είναι μαρκαρισμένα
- Δεν διατηρούνται πληροφορίες κατάστασης - απλοποίηση υλοποίησης εφαρμογής

IMAP (Internet Mail Access Protocol)

- Στο POP3 δεν μπορούν να αποθηκευτούν σε φακέλους όπως στο IMAP και να αρχειοθετηθούν σε πολλούς υπολογιστές το ίδιο. Για αυτό εφεύρεση του IMAP
- Συσχετισμός κάθε μηνύματος με έναν φάκελο, δυνατότητα αναζήτησης, δυνατότητα παραλαβής μόνο τμημάτων μηνυμάτων
- Email μέσω Web

Περιγράψτε εν συντομία το μοντέλο Client - Server και το μοντέλο P2P (ομότιμων)
Client - Server
Στην αρχιτεκτονική αυτή υπάρχει ένας πάντα ενεργός υπολογιστής (εξυπηρετητής) και εξυπηρετεί αιτήσεις από πολλούς άλλους υπολογιστές (πελάτες).

P2P (ομότιμων)
Στην αρχιτεκτονική αυτή υπάρχει μια μικρή ή και καθόλου στήριξη σε αποκλειστικούς εξυπηρετητές σε κέντρα δεδομένων. Αντιθέτως η εφαρμογή εκμεταλλεύεται την απευθείας επικοινωνία ανάμεσα σε ζεύγη συνδεδεμένων υπολογιστών, που καλούνται ομότιμοι.

Είδη συνδέσεων

- Παραμένουσες - Προεπιλεγμένος τρόπος λειτουργίας
- Μη παραμένουσες - Η λήψη κάθε αντικειμένου ξεκινά μια νέα σύνδεση TCP
- Round-trip time (RTT) ενός πακέτου - σύνολο χρόνου του ταξιδιού από τον πελάτη στο δρομολογητή και επιστροφή, τρίδρομη χειραψία

HTTP (θύρα 80) - TCP

Ακαταστατικό (stateless) πρωτόκολλο, δεν κρατάει πληροφορίες για τους πελάτες

Πότε ο πελάτης Web και ο εξυπηρετητής Web χρησιμοποιούν παραμένουσες και πότε μη-παραμένουσες συνδέσεις;

Το HTTP χρησιμοποιεί μια παραμενουσα συνδεση κατά τη διάρκεια ενός αιτήματος μέχρι την ολοκλήρωση του από τον εξυπηρέτη. Κάθε αρχείο που φορτώνεται κατά τη διάρκεια της παραμενουσας σύνδεσης λαμβάνεται με ξεχωριστές μη-παραμένουσες συνδέσεις.

Για ποιους λόγους χρησιμοποιούνται τα cookies; Γιατί αμφισβητείται η χρήση τους;

Είναι συχνά επιθυμητό για τον ιστότοπο να θέλει να αναγνωρίζει χρήστες είτε επειδή θέλει να περιορίσει την προσπέλαση χρηστών είτε επειδή θέλει να παρέχει περιεχόμενο ως μια συνάρτηση της ταυτότητας του χρήστη. Τα cookies επιτρέπουν στους ιστότοπους να παρακολουθούν τους χρήστες. Παραμένουν όμως άκρως αμφισβητήσιμα επειδή μπορούν να θεωρηθούν ως παραβίαση της ιδιωτικότητας του χρήστη.

FTP (θύρα 21) - TCP

- Μεταφορά αρχείων
- Δύο παράλληλες συνδέσεις: ελέγχου/control (παραμένει ανοιχτή) και δεδομένων/data (ανοίγει καινούργια για κάθε αρχείο) (εξωζωνικά - το HTTP είναι ενδοκρινικό)
- Διατηρεί κατάσταση χρήστη- καταστατικό

SMTP (θύρα 25) - TCP

- Μεταφορά μηνυμάτων από τους εξυπηρέτες ταχυδρομείου στους εξυπηρέτες των παραληπτών
- Απαιτεί κωδικοποίηση των μηνυματων σε ASCII 7-bit

DNS (θύρα 53) - UDP

- Αντιστοίχιση ονομάτων υπολογιστή με διευθύνσεις IP
- Κατανεμημένη βάση δεδομένων με ιεραρχία εξυπηρετητών DNS
- Πρωτόκολλο επιπέδου εφαρμογής

Αναφέρατε ένα σημαντικό κοινό χαρακτηριστικό και μια σημαντική διαφορά ανάμεσα στο HTTP και στο FTP
Ομοιότητα
Και τα δύο εκτελούνται πάνω στο TCP

Διαφορά
Το HTTP στέλνει γραμμές κεφαλίδας αιτήσεων μέσα στην ίδια σύνδεση ενώ το FTP χρησιμοποιεί δύο παράλληλες συνδέσεις (σύνδεση ελέγχου και σύνδεση δεδομένων)

Αναφέρατε ένα σημαντικό κοινό χαρακτηριστικό και μια σημαντική διαφορά ανάμεσα στο HTTP και στο SMTP
Ομοιότητα
Και τα δύο πρωτόκολλα χρησιμοποιούνται για μεταφορά αρχείων από έναν υπολογιστή σε έναν άλλον χρησιμοποιώντας μάλιστα και τα δύο παραμένουσες συνδέσεις.

Διαφορά
Το HTTP είναι κυρίως πρωτόκολλο προσέλκυσης (pull protocol) ενώ το SMTP είναι κυρίως πρωτόκολλο προώθησης (push protocol).

Το πρωτόκολλο HTTP είναι ακαταστατικό πρωτόκολλο (stateless protocol) ή διατηρεί την κατάσταση state των χρηστών-συνδέσεων;
Επειδή ένας εξυπηρέτης HTTP δεν κρατά πληροφορίες για τους πελάτες, λέγεται ότι είναι ένα ακαταστατικό πρωτόκολλο (stateless protocol).

Το πρωτόκολλο FTP είναι ακαταστατικό πρωτόκολλο (stateless protocol) ή διατηρεί την κατάσταση state των χρηστών - συνδέσεων;
Το FTP είναι καταστατικό πρωτόκολλο, δηλαδή διατηρεί την κατάσταση state των χρηστών συνδέσεων

Πώς επηρεάζει την απόδοση μεταφοράς αρχείων το αν διατηρεί κατάσταση χρηστών-συνδέσεων (state) ή όχι το πρωτόκολλο;
Όταν ένα πρωτόκολλο είναι ακαταστατικό (stateless) όπως το HTTP, πρέπει να δώσουμε το πλήρες path (τα πλήρη στοιχεία ενός αρχείου), ενώ όταν διατηρεί την κατάσταση state όπως το FTP του βάζουμε μόνο το όνομα του αρχείου.

Πιο αναλυτικά:
Το FTP χρησιμοποιεί δύο παράλληλες συνδέσεις TCP για μεταφορά ενός αρχείου, μία σύνδεση ελέγχου (control connection) και μία σύνδεση δεδομένων (data connection). Η σύνδεση ελέγχου χρησιμοποιείται για αποστολή πληροφοριών ελέγχου ανάμεσα σε δύο υπολογιστές - πληροφοριών όπως όνομα χρήστη, συνθηματικό, εντολές για αλλαγή ενός απομακρυσμένου καταλόγου και εντολές για "τοποθέτηση" και "λήψη" ενός αρχείου. Επειδή το FTP χρησιμοποιεί μία ξεχωριστή σύνδεση ελέγχου, το FTP λέγεται ότι στέλνει τις πληροφορίες ελέγχου εξωζωνικά (out-of-bound).

Το HTTP στέλνει γραμμές κεφαλίδας αιτήσεων και αποκρίσεων μέσω της ίδιας σύνδεσης TCP, που μεταφέρει το ίδιο το μεταφερόμενο αρχείο. Γι αυτό το λόγο, το HTTP λέγεται ότι στέλνει τις πληροφορίες ελέγχου του ενδοζωνικά (in-bound).

Επίπεδο Μεταφοράς

Τί ονομάζεται συνδεσμική υπηρεσία στο επίπεδο μεταφοράς;
Το TCP θεωρειται συνδεσμικο, καθώς δυο διεργασιες πρέπει να κάνουμε μια "χειραψία" μεταξύ τους πριν αρχίσουν να στελνουν δεδομενα η μια στην άλλη, η οποία περιέχει πληροφορίες ελέγχου/μεταβλητές κατάστασης TCP.

Τί ονομάζεται αμφίδρομη υπηρεσία στο επίπεδο μεταφοράς;
Αν σε μια σύνδεση TCP υπάρχει μια διεργασία στον υπολογιστή Α που επικοινωνεί με μια διεργασία στον υπολογιστή Β, τότε η Α μπορεί να στέλνει δεδομένα εφαρμογής στη Β ταυτόχρονα όσο η Β μπορεί να στέλνει δεδομένα εφαρμογής στην Α.

Τί, πότε και γιατί καλεί την διαδικασία ταχείας αναμετάδοσης το πρωτόκολλο TCP;
Όταν συμβεί απώλεια πακέτων ο αποστολέας το καταλαβαίνει απο τα διπλότυπα ACK. Όταν ληφθούν 3 διπλότυπα ACK ο αποστολέας εκτελεί την λειτουργία ταχείας αναμετάδοσης ώστε να σταλούν τα πακέτα σωστά στον προορισμό.

Τί προσπαθεί να πετύχει ο έλεγχος συμφόρησης στο επίπεδο μεταφοράς;
Ο μηχανισμός ελέγχου συμφόρησης του TCP ρυθμίζει μία διεργασία αποστολής (πελάτη ή εξυπηρέτη) όταν το δίκτυο έχει συμφόρηση ανάμεσα στον πομπό και στον δέκτη.

Αναφέρετε αν τα πιο γνωστά πρωτόκολλα επιπέδου μεταφοράς TCP και UDP περιλαμβάνουν συνδεσμική υπηρεσία και έλεγχο συμφόρησης.
TCP: ΝΑΙ, περιλαμβάνει μία συνδεσμική υπηρεσία (connection-oriented service) και έναν μηχανισμό ελέγχου συμφόρησης.

UDP ΟΧΙ: είναι ασυνδεσμικό (connectionless) και δεν περιλαμβάνει έναν μηχανισμό ελέγχου συμφόρησης.

Τί δηλώνει ο αριθμός ακολουθίας σε ένα TCP τμήμα;
Ο αριθμός ακολουθίας για ένα τμήμα είναι ο αύξων αριθμός του πρώτου byte μέσα στο τμήμα απ' το συνολικό ρεύμα από byte.

Τί δηλώνει ο αριθμός επιβεβαίωσης σε ένα TCP τμήμα;
Ο αριθμός επιβεβαίωσης που θέτει ο υπολογιστής Α στο τμήμα του είναι ο αριθμός ακολουθίας του επόμενου byte που περιμένει ο υπολογιστής Α από τον υπολογιστή Β.

Το TCP παρέχει συσσωρευτικές επιβεβαιώσεις ή ανεξάρτητες;
Το TCP λέγεται ότι παρέχει συσσωρευτικές επιβεβαιώσεις.

Ποιός είναι ο χρόνος διαδρομής στο TCP πρωτόκολλο και ποιός ο χρόνος αναμετάδοσης;
Χρόνος διαδρομής: Ο χρόνος που κάνει ένα TCP τμήμα (segment) που στέλνω από τη στιγμή που το στέλνω μέχρι να φτάσει και να πάρει την επιβεβαίωση (το RTT που λέει στο βιβλίο).

Χρόνος αναμετάδοσης είναι ο χρόνος που περιμένω από τη στιγμή που το στέλνω μέχρι το χρόνο που αν δεν πάρω επιβεβαίωση θα πρέπει να το ξαναστείλω (να κάνω αναμετάδοση δηλαδή).

Σύγκριση TCP με UDP
Το μοντέλο υπηρεσίας TCP περιλαμβάνει μία συνδεσμική υπηρεσία (connection-oriented service) και μία υπηρεσία αξιόπιστης μεταφοράς δεδομένων. Όταν μία εφαρμογή χρησιμοποιεί το TCP ως πρωτόκολλο μεταφοράς εφαρμογή δέχεται και τις δύο αυτές υπηρεσίες από το TCP. Το TCP περιλαμβάνει επίσης έναν μηχανισμό ελέγχου συμφόρησης, μία υπηρεσία για την συνολική ευεξία του Διαδικτύου αντί του άμεσου οφέλους των επικοινωνουσών διεργασιών. Ο μηχανισμός ελέγχου συμφόρησης του TCP ρυθμίζει μία διεργασία αποστολής (πελάτη ή εξυπηρέτη) όταν το δίκτυο έχει συμφόρηση ανάμεσα στον πομπό και στον δέκτη.

Το UDP είναι ένα απλό, ελαφρύ πρωτόκολλο μεταφοράς, παρέχοντας ελάχιστες υπηρεσίες. Το UDP είναι ασυνδεσμικό (connectionless), οπότε δεν υπάρχει διαδικασία χειραψίας πριν οι δύο διεργασίες αρχίσουν να επικοινωνούν. Το UDP παρέχει μία αναξιόπιστη υπηρεσία μεταφοράς δεδομένων - δηλαδή, όταν μία διεργασία στέλνει ένα μήνυμα σε μία UDP socket, το UDP δεν παρέχει καμία εγγύηση ότι το μήνυμα θα φτάσει ποτέ στη διεργασία λήψης. Επιπλέον, τα μηνύματα που φτάνουν στη διεργασία λήψης μπορούν να φθάσουν με εκτός σειράς. Το UDP δεν περιλαμβάνει έναν μηχανισμό ελέγχου συμφόρησης, οπότε η διεργασία αποστολής του UDP μπορεί να τροφοδοτεί με δεδομένα το υποκείμενο του επίπεδο (το επίπεδο δικτύου) με όποιον ρυθμό θέλει (η πραγματική διεκπεραιωτική ικανότητα από-άκρο-σε-άκρο μπορεί να είναι μικρότερη απ' αυτόν το ρυθμό, λόγω του περιορισμένου εύρους ζώνης των ενδιάμεσων ζεύξεων ή λόγω συμφόρησης).

Για ποιους λόγους μία εφαρμογή θα προτιμούσε το UDP απο το TCP;
Ένας λόγος θα ήταν ότι το UDP είναι πολύ πιο ελαφρύ από το TCP, ένας ακόμα λόγος θα ήταν η εξοικονόμηση πόρων καθώς στο UDP δεν χρειάζεται η διατήρηση της κατάστασης της σύνδεσης και τέλος το UDP έχει πολύ μικρή καθυστέρηση μετάδοσης του μηνύματος εξαιτίας της πολύ μικρής κεφαλίδας και της μη συνδεσμικής υπηρεσίας του.

Το TCP παρέχει αξιόπιστη μεταφορά δεδομένων. Τι εξασφαλίζει η αξιόπιστη μεταφορά δεδομένων και τι χρησιμοποιεί;
Με την αξιόπιστη μεταφορά δεδομένων το TCP εξασφαλίζει ότι τα δεδομένα αποστέλλονται από την διεργασία αποστολής στη διεργασία λήψης σωστά και με ορθή σειρά χρησιμοποιώντας έλεγχο ροής, αριθμούς ακολουθίας, επιβεβαιώσεις και χρονομετρητές.

Αναφέρετε τη χρήση του πεδίου "ΑΘΡΟΙΣΜΑ ΕΛΕΓΧΟΥ" στην κεφαλίδα του IP πακέτου σε σχέση με τη χρήση του πεδίου "ΑΘΡΟΙΣΜΑ ΕΛΕΓΧΟΥ" στην κεφαλίδα του TCP πακέτου. Γιατί χρησιμοποιούνται δύο "αθροίσματα ελέγχου";
Το άθροισμα ελέγχου κεφαλίδας IP βοηθά έναν δρομολογητή να ανιχνεύει σφάλματα bit σ' ένα λαμβανόμενο δεδομενόγραμμα(datagram) IP.

Το άθροισμα ελέγχου TCP παρέχει ανίχνευση σφαλμάτων. Αυτό σημαίνει ότι το άθροισμα ελέγχου χρησιμοποιείται για να καθορίσει εάν κάποια bit μέσα στο τμήμα TCP έχουν αλλαχτεί κατά τη μεταφορά τους από την προέλευση στον προορισμό.

Χρησιμοποιούνται δύο αθροίσματα ελέγχου γιατί : Πρώτον, στο επίπεδο IP γίνεται έλεγχος αθροίσματος ελέγχου μόνον της κεφαλίδας IP, ενώ το άθροισμα ελέγχου TCP/UDP υπολογίζεται σε όλο το τμήμα TCP ή UDP. Δεύτερον, το TCP/UDP και το IP δε χρειάζεται να ανήκουν και τα δύο στην ίδια στοίβα πρωτοκόλλων. Το TCP μπορεί, κατ' αρχήν, να εκτελείται πάνω από ένα διαφορετικό πρωτόκολλο (π.χ. το ATM) και το IP μπορεί να μεταφέρει δεδομένα που δε θα περνούν στο TCP/UDP.

Περιγράψτε τις λειτουργίες έλεγχο ροής (flow control) και έλεγχο συμφόρησης (congestion control). Ποιες μεταβλητές συμμετέχουν, πως λειτουργούν, σε τι εξυπηρετούν κτλ.
Το TCP παρέχει μία υπηρεσία ελέγχου ροής (flow-control service) στις εφαρμογές του για να εξαλείψει την πιθανότητα να υπερχειλίσει ο αποστολέας του ενταμιευτή του παραλήπτη. Ο έλεγχος ροής είναι λοιπόν μία υπηρεσία (ταιριάσματος ταχυτήτων) που ταιριάζει το ρυθμό με τον οποίο ο αποστολέας στέλνει, με το ρυθμό με τον οποίο διαβάζει η εφαρμογή λήψης.

Έλεγχος συμφόρησης (congestion control)

Απαγορεύει σε οποιαδήποτε TCP σύνδεση να πλημμυρίσει τις ζεύξεις και τους μεταγωγείς ανάμεσα σε επικοινωνούντες υπολογιστές με υπερβολική ποσότητα κίνησης. Το TCP προσπαθεί να δώσει σε κάθε σύνδεση που διασχίζει ζεύξη δικτύου με συμφόρηση, ίσο εύρος ζώνης αυτό της ζεύξης.

Πώς λειτουργεί η αργή εκκίνηση (slow start) στο TCP πρωτόκολλο και πώς η αποφυγή συμφόρησης (congestion avoidance);

Αφού το διαθέσιμο εύρος ζώνης της σύνδεσης στον αποστολέα TCP μπορεί να είναι πολύ μεγαλύτερο από το MSS/RTT, ο αποστολέας TCP θα θέλει να βρει την ποσότητα του διαθέσιμου εύρους ζώνης γρήγορα. Έτσι, κατά την κατάσταση αργή κίνηση (slow start), η τιμή της cwnd αρχίζει στο 1 MSS και αυξάνεται κατά 1 MSS κάθε φορά που ένα μεταδοθέν τμήμα επιβεβαιώνεται.

Όταν γίνεται είσοδος στην κατάσταση αποφυγής συμφόρησης, η τιμή της cwnd είναι περίπου το μισό της τιμής που είχε όταν παρατηρήθηκε συμφόρηση για πρώτη φορά - η συμφόρηση θα μπορούσε να ήταν έτοιμη να συμβεί! Έτσι, αντί να διπλασιάσει την τιμή της cwnd σε κάθε RTT, το TCP υιοθετεί μία πιο συντηρητική προσέγγιση και αυξάνει την τιμή της cwnd κατά ένα μόνο MSS ανά RTT.

Επίπεδο Δικτύου

Πως παραμετροποιείται (γεμίζει) ένας πίνακας προώθησης σε έναν δρομολογητή. Μια περιεκτική περιγραφή.
Κάθε δρομολογητής έχει έναν πίνακα προώθησης (forwarding table). Ένας δρομολογητής προωθεί ένα πακέτο εξετάζοντας την τιμή ενός πεδίου στην κεφαλίδα του αφικνούμενου πακέτου και μετά χρησιμοποιεί αυτή την τιμή ως δείκτη για να ψάξει στον πίνακα προώθησης του δρομολογητή. Η αποθηκευμένη τιμή στον πίνακα προώθησης υποδεικνύει σε ποια απ τις εξερχόμενες ζεύξης διεπαφής του δρομολογητή θα προωθηθεί το πακέτο. Ανάλογα με το πρωτόκολλο επιπέδου δικτύου, αυτή η τιμή στην κεφαλίδα του πακέτου μπορεί να είναι η διεύθυνση προορισμού του πακέτου ή μία ένδειξη της σύνδεσης στην οποία ανήκει το πακέτο.

Το μοντέλο υπηρεσίας IP είναι μια προσπάθεια βέλτιστης απόδοσης, τι σημαίνει αυτό;
Σημαίνει ότι το IP καταβάλει κάθε δυνατή προσπάθεια ώστε το πακέτο να φτάσει στον προορισμό χωρίς όμως να το εγγυάται.

Διάρκεια/χρόνος ζωής (time-to-live, TTL).
Το πεδίο διάρκειας ζωής (time-to-live, TTL) περιλαμβάνεται για να διασφαλίσει ότι τα δεδομενογράμματα δεν κυκλοφορούν για πάντα (π.χ. λόγω ενός μακροχρόνιου βρόγχου δρομολόγησης) μέσα στο δίκτυο. Αυτό το πεδίο μειώνεται κατά ένα κάθε φορά που περνάει από έναν δρομολογητή. Εάν το πεδίο TTL φτάσει στο 0, το δεδομενόγραμμα πρέπει να απορριφθεί.

Ποιά είναι η λειτουργία του πεδίου "Πρωτόκολλο" στα πεδία της κεφαλίδας του IP πακέτου/δεδομενογράμματος;
Η τιμή αυτού του πεδίου δηλώνει το σε ποιό πρωτόκολλο επιπέδου μεταφοράς πρέπει να παραδοθεί το δεδομενόγραμμα IP. πχ (TCP ή UDP)

Ποιά είναι η λειτουργία της μετατόπισης κατάτμησης (Fragment offset);
Η λειτουργία του είναι να προσδιορίζει τη θέση του κάθε τμήματος στο IP πακέτο ώστε ο τελικός αποδέκτης να διευκολυνθεί στην επανασυγκόλληση.

Ποιά πεδία του IP δεδομενογράμματος/πακέτου εξετάζει ο υπολογιστής προορισμού για να καθορίσει ότι δύο από τα δεδομενογράμματα που λαμβάνει είναι ή όχι συνεχόμενα τεμάχια του μεγαλύτερου δεδομενογράμματος; Πώς είναι απολύτως σίγουρος ότι έχει λάβει και το τελευταίο τεμάχιο του αρχικού δεδομενογράμματος;
Τα πεδία είναι ο αριθμός ταυτότητας (Identification number), ένδειξης (Flags) και μετατόπισης κατάτμησης (Fragment offset) στο δεδομενόγραμμα IP.

Για να είναι ο υπολογιστής προορισμού απολύτως σίγουρος ότι έχει λάβει το τελευταίο τεμάχιο του αρχικού δεδομενογράμματος , το τελευταίο τεμάχιο έχει ένα bit-σημαία με τιμή 0, ενώ όλα τα άλλα τεμάχια έχουν σ' αυτό το bit-σημαία την τιμή 1.

Επίσης, για να μπορεί να καθορίσει ο υπολογιστής προορισμού εάν λείπει ένα τεμάχιο (κι επίσης να μπορέσει να ανασυνθέσει τα τεμάχια με τη σωστή τους σειρά), το πεδίο μετατόπισης κατάτμησης χρησιμοποιείται για να καθορίσει πού μπαίνει το τεμάχιο μέσα στο αρχικό δεδομενόγραμμα IP.

Πως λειτουργει το ping;
Το γνωστό πρόγραμμα ping στέλνει ένα μήνυμα ICMP με τύπο 8, κωδικό 0 στον καθορισμένο υπολογιστή. Ο υπολογιστής προορισμού, βλέποντας την αίτηση ηχούς, στέλνει πίσω μία απόκριση ICMP με τύπο 0, κωδικό 0. Οι περισσότερες υλοποιήσεις TCP/IP υποστηρίζουν τον εξυπηρέτη ping απ' ευθείας απ' το λειτουργικό τους σύστημα. Δηλαδή ο εξυπηρέτης δεν είναι μία διεργασία. Το πρόγραμμα πελάτη πρέπει να είναι σε θέση να υποχρεώσει το λειτουργικό σύστημα να παράγει ένα μήνυμα ICMP τύπου 8 κωδικού 0.

Πως λειτουργει το traceroute;
Το πρόγραμμα Traceroute επιτρέπει σε κάποιον να ιχνηλατεί μία διαδρομή από έναν υπολογιστή προς έναν οποιονδήποτε άλλο υπολογιστή στον κόσμο. Είναι ενδιαφέρον ότι το Traceroute υλοποιείται με μηνύματα ICMP. Για να καθορίσει τα ονόματα και τις διευθύνσεις των δρομολογητών ανάμεσα στην προέλευση και στον προορισμό, το Traceroute στην προέλευση στέλνει μία σειρά συνηθισμένων δενδρογραμμάτων IP προς τον προορισμό.

Ποιές είναι οι βασικές παράμετροι δικτύου, για να μπορέσει κάποιος σταθμός να συνδεθεί στο Internet;
Χρειαζόμαστε :

- Μία IP address υπολογιστή (τη δική μας)
- Το default gateway (πρέπει να ξέρω ποιά είναι η IP του υπολογιστή που με εξυπηρετεί, δηλ. του router του). Αν δεν μπορώ να στείλω απευθείας, το στέλνω εκεί
- Τη subnet mask (δείχνει ποιά bit της IP είναι του δικτύου). Πρέπει να έχουμε τον ίδιο αριθμό bits στο network id

Είναι υποχρεωτικό να έχουμε και DNS server;

Αν θέλουμε να κάνουμε χρήση ονομάτων αντιστοιχισμένων με διευθύνσεις IP, τότε πρέπει να έχουμε και DNS server, του οποίου η λειτουργία είναι να μεταφράζει ονόματα σε διευθύνσεις IP.

Επίπεδο Ζεύξης

Μεταγωγείς vs Δρομολογητές:
Μεταγωγείς χρησιμοποιούνται σε μικρά δίκτυα, αυξάνουν την συνολική διεκπεραιωτική ικανότητα και απλοποιούν την σύνδεση.

Δρομολογητές χρησιμοποιούνται σε μεγάλα δίκτυα, παρέχουν πιο στιβαρή απομόνωση κίνησης, ελέγχουν τον καταιγισμό εκπομπής και χρησιμοποιούν πιο έξυπνες διαδρομές μέσα στο δίκτυο.

Ποια είναι τα 4 βήματα του DHCP;
- Ανακάλυψη εξυπηρέτη DHCP.
- Προσφορά(ές) εξυπηρέτη DHCP.
- Αίτηση DHCP.
- DHCP ACK.

Βήματα εύρεσης διεύθυνσης ARP:
- Δημιουργία πακέτου ARP με πεδία διεύθυνσης αποστολής και λήψης IP και MAC, ίδια μορφή σε μηνύματα απόκρισης και ερώτησης. Ενθυλάκωση με διεύθυνση MAC broadcast και προώθηση στο δίκτυο
- Το πλαίσιο λαμβάνεται από όλους τους προσαρμογείς στο υποδίκτυο και περνά σε μια μονάδα ARP εφόσον προορίζεται για όλους. Κάθε προσαρμογέας ελέγχει αν η διεύθυνση IP στο πακέτο ARP αντιστοιχεί στην δική της
- Αυτή που ταιριάζει δημιουργεί ένα πακέτο ARP και το προωθεί σε αυτόν που έκανε το ερώτημα
- Αυτός που έκανε το ερώτημα λαμβάνει την απάντηση και ενημερώνει τον πίνακα ARP του. Τώρα έχει την απάντηση
- Το ARP είναι ένα πρωτόκολλο ανάμεσα στο επίπεδο ζεύξης και δικτύου
- Για να σταλεί ένα πακέτο έξω από το τοπικό δίκτυο πρέπει να γνωρίζει ο υπολογιστής την διεύθυνση MAC του default router. Αυτό γίνεται με το ARP. Όταν μάθει την διεύθυνση MAC, το δεδομενόγραμμα ενθυλακώνει σε ένα frame με διεύθυνση αποστολής την διεύθυνση MAC του default router.

-- Ping- λειτουργία.

Το γνωστό πρόγραμμα ping στέλνει ένα μήνυμα ICMP με τύπο 8, κωδικό 0 στον καθορισμένο υπολογιστή. Ο υπολογιστής προορισμού, βλέποντας την αίτηση ηχούς, στέλνει πίσω μία απόκριση ICMP με τύπο 0, κωδικό 0. Οι περισσότερες υλοποιήσεις

TCP/IP υποστηρίζουν τον εξυπηρετητή ping απ' ευθείας απ' το λειτουργικό τους σύστημα. Δηλαδή ο εξυπηρετητής δεν είναι μία διεργασία. Το πρόγραμμα πελάτη πρέπει να είναι σε θέση να υποχρεώσει το λειτουργικό σύστημα να παράγει ένα μήνυμα ICMP τύπου 8 κωδικού 0.

-- Πώς λειτουργεί το traceroute;

Το πρόγραμμα Traceroute επιτρέπει σε κάποιον να ιχνηλατεί μία διαδρομή από έναν υπολογιστή προς έναν οποιονδήποτε άλλο υπολογιστή στον κόσμο. Είναι ενδιαφέρον ότι το Traceroute υλοποιείται με μηνύματα ICMP. Για να καθορίσει τα ονόματα και τις διευθύνσεις των δρομολογητών ανάμεσα στην προέλευση και στον προορισμό, το Traceroute στην προέλευση στέλνει μία σειρά συνηθισμένων δενδρογραμματων IP προς τον προορισμό.

-- Ποιες είναι οι βασικές παράμετροι δικτύου, για να μπορέσει κάποιος σταθμός να συνδεθεί στο Internet;

Χρειαζόμαστε :

- μία IP address υπολογιστή (τη δική μας)
- το default gateway (πρέπει να ξέρω ποια είναι η IP του υπολογιστή που με εξυπηρετεί, δηλ. του router του). Αν δεν μπορώ να στείλω απευθείας, το στέλνω εκεί
- τη subnet mask (δείχνει ποια bit της IP είναι του δικτύου). Πρέπει να έχουμε τον ίδιο αριθμό bits στο network id

-- Είναι υποχρεωτικό να έχουμε και DNS server;

Αν θέλουμε να κάνουμε χρήση ονομάτων αντιστοιχισμένων με διευθύνσεις IP, τότε πρέπει να έχουμε και DNS server, του οποίου η λειτουργία είναι να μεταφράζει ονόματα σε διευθύνσεις IP.

-- Μια εγγραφή πόρου στο DNS περιλαμβάνει ποια πεδία ;

- όνομα (name),
- Τιμή (value),
- Τύπος (type),
- Χρονικό διάστημα παραμονής της εγγραφής (TTL).

-- Για ποιους λόγους χρειαζόμαστε το DNS caching;

Το DNS caching γίνεται στους εξυπηρετητές του DNS. Οι εξυπηρετητές αποθηκεύουν τις πρόσφατες αναζητήσεις DNS έτσι ώστε να μη χρειαστεί να στέλνουν αιτήματα σε κάθε επίσκεψη, για την αντιστοίχιση της IP με ένα domain.

Chapter 1 : Introduction

1. Τι είναι πρωτόκολλο;
    - Σελ. 9.
2. Μεταγωγή πακέτου έναντι Μεταγωγής Κυκλώματος
    - Σελ 30-31. Πως δουλεύει.

Chapter 2 : Application Layer

1. Application Architectures – Client-Server Architecture – P2P Architecture **
    - Ποια είναι η διαφορά τους, Ποιες είναι οι δύο αρχιτεκτονικές.
    - Αν το Client-server το γράψουμε Master-slave είναι το ίδιο;
        i. Σαν αρχιτεκτονική ναι είναι το ίδιο όμως δεν έχουν την ίδια επικοινωνία. Master είναι κάποιος που έχει μεγαλύτερη γνώση και είναι πάνω από τον client.
    - Στο Peer-to-peer έχουμε Master-slave;
        i. Όχι επειδή έχουμε ισότητα. Επικοινωνούν δύο hosts μεταξύ τους απευθείας.
2. Processes Communicating
    - Ποιος ξεκινάει την επικοινωνία; Ο εξυπηρετητής; Σ/Λ Γιατί;
        i. Διεργασία πελάτη – Εκκίνηση
        ii. Διεργασία εξυπηρετητής – Αναμονή
3. Sockets **
    - Είναι μία software διεπαφή. Κλπ.
4. Addressing Processes
    - Identifier = Συνδυασμός IP:Port.
5. What Transport Service does an app need? ** Πολλαπλής επιλογής, Σ/Λ ή πχ ερώτηση ➔ Στα διαδικτιακά παιχνίδια η απαίτηση μας είναι να έχουμε ασφάλεια ή χρονισμό; Κλπ.
    - Τα 4 requirements + τι είναι το κάθε ένα και παραδήγματα που χρησιμοποιούνται.
6. Transport Service Requirements: Common Apps **

Εφαρμογή	Απώλεια δεδομένων	Ρυθμαπόδοση	Ευαισθησία ως προς το χρόνο
Μεταφορά αρχείου	όχι απώλειες	ελαστική	όχι
e-mail	όχι απώλειες	ελαστική	όχι
Έγγραφα Web	όχι απώλειες	ελαστική	όχι
Ήχος/ βίντεο πραγματικού χρόνου	ανοχή στις απώλειες	ήχος: 5kbps-1Mbps, βίντεο:10kbps-5Mbps	ναι, 100δες msec
Αποθηκευμένος ήχος/βίντεο	ανοχή στην απώλειες	ίδια με παραπάνω	ναι, λίγα secs
Διαδραστικά παιχνίδια	ανοχή στην απώλειες	ως λίγα kbps	ναι, 100δες msec
Μηνύματα κειμένου	όχι απώλειες	ελαστική	ναι και όχι

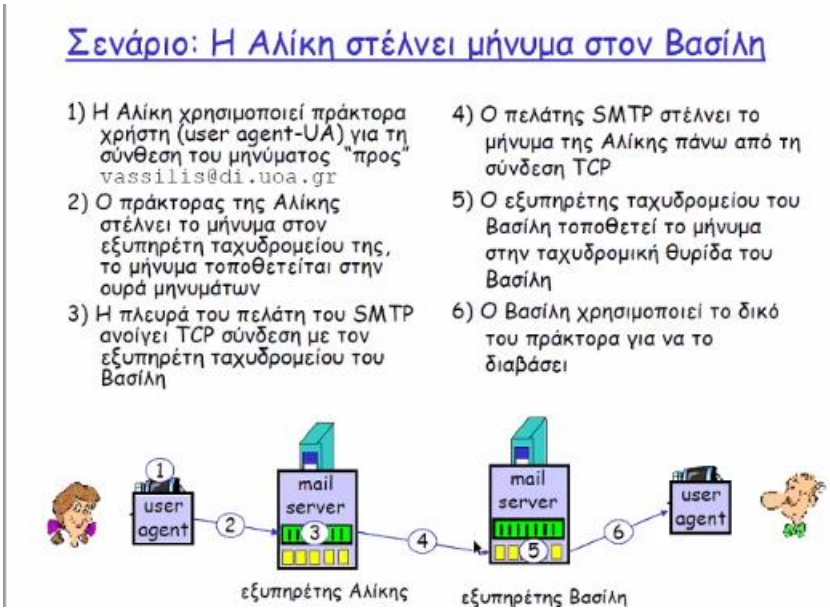
7. Internet Transport Protocols Services
    - Σύγκριση TCP – UDP.
    - Το TCP έχει κρυπτογράφηση;
        i. Έχει έμμεσα κρυπτογράφηση μέσω του SSL στο 5ο επίπεδο. Δεν έχει αυτόματα μέσα του το TCP κρυπτογράφηση. Το καθορίζει ο προγραμματιστής.
    - Γιατί υπάρχει το UDP; (Πλεονεκτήματα)
        i. Ταχύτητα (λόγω μικρής κεφαλίδας)
    - Τι δεν παρέχει από κοινού το TCP και το UDP;
        i. Ρυθμαπόδοση. Γιατί δεν παρέχει ρυθμαπόδοση;
8. Internet Apps: Application, Transport Protocols ** Αντιστοίχηση. Σελ 96.

Εφαρμογή	Πρωτόκολλο εφαρμογής	Υποκείμενο Πρωτόκολλο μεταφοράς
Ηλεκτρονικό ταχυδρομείο e-mail	SMTP [RFC 2821]	TCP
Απομακρυσμένη προσπέλαση τερματικού	Telnet [RFC 854]	TCP
Web	HTTP [RFC 2616]	TCP
Μεταφορά αρχείων	FTP [RFC 959]	TCP
Πολυμέσα συνεχούς ροής	HTTP (π.χ. YouTube), RTP[RFC 1889]	TCP ή UDP
Τηλεφωνία Διαδικτύου	SIP, RTP, ιδιοταγές (π.χ. Skype)	TCP ή UDP

    - Πχ στο Youtube την ώρα που θα βάζω τα στοιχεία μου για log-in σε SSL, χρησιμοποιείται TCP και για την ροή του βίντεο χρησιμοποιείται το UDP.
    - Τηλεφωνία Διαδικτύου ➔ Δεν είμαστε σίγουροι επειδή είναι ιδιοταγές. Όταν είναι ιδιοτικό δεν ξέρουμε τι χρησιμοποιεί.
9. HTTP Overview *
    - Τα πάντα.
    - Δεν χρησιμοποιείται το UDP
    - Τι είναι καταστατικό και τι ακαταστατικό. Ποια πρωτόκολλα είναι ακαταστατικά και ποια ακαταστατικά. ** Σελ. 101-102 (4ου επιπέδου είναι η σύνδεση παραμένουσα – μη παραμενουσα)
10. HTTP Connections **

- Τι είναι παραμένουσα και τι μη παραμενουσα. Σελ. 101-102 (4ου επιπέδου είναι η σύνδεση παραμένουσα – μη παραμενουσα)

11. Persistent HTTP **** Θα ζητηθεί. Πόσα RTT χρειάζεται για το κάθε αντικείμενο για να μεταφερθεί στις μη-παραμένουσες; Ή Πόσα RTT χρειάζεται για παραμένουσες συνδέσεις για κάθε αντικείμενο; (1 RTT)
    - Σύγκριση non-persistent με persistent.
12. Cookies
    - Τι εξυπηρετούν και τι υπάρχει σαν αντίλογος (γιατί δεν θέλουν να χρησιμοποιούνται;)
        i. Επίσης πρέπει να σε ρωτάνε αν θες να τα κάνεις accept
13. Web Caches (Proxy Server)
    - Τι είναι και γιατί χρησιμοποιούνται;
    - Θετικά
14. Conditional Get
    - Τι είναι και πως λειτουργεί με τον proxy server;
15. Electronic mail
    - SMTP τα πάντα.
    - Τρία κύρια συστατικά μέρη και η ανάλυση τους.
    - Σύγκριση SMTP με HTTP τι κοινό έχουν; (7-bit ASCII ➔ Διαβάζονται από τον άνθρωπο). ***** σελ. 121 Είναι και τα δύο ακαταστατικά, pull ή push; Κοινά – Διαφορά.
        i. Στο SMTP στέλνουμε στον server και δεν παίρνουμε απόκριση από τον server. Ο παραλήπτης θα διαβάζει από τον δικό του mail server, εκτός και αν μοιραζόμαστε τον ίδιο mail server. Το HTTP είναι pull γιατί παω στον server και ζητάω να κατεβάσω, ενώ στο SMTP στέλνουμε στον server.
    -



- Ερώτηση ➔ Στα 2,4,6 χρησιμοποιούμαι το ίδιο πρωτόκολλο; *** Πολλαπλής. Με ποια πρωτόκολλα επικοινωνούν οι Servers; (SMTP) ή πως στέλνει ο πελάτης στον mail server του; (SMTP – Όταν στέλνουμε ένα mail, στέλνουμε με SMTP).
    i. 2,4 ➔ SMTP (Πάντα τα mails στέλνονται με SMTP)
    ii. 6 ➔ POP, IMAP ή HTTP. (Μόνο στο κατέβασμα-download έχουμε αυτά τα τρία πρωτόκολλα)
    iii. Με ένα πρωτόκολλο στέλνουμε και με πολλά διαβάζουμε τα Mails μας.
- Σύγκριση POP – IMAP. ***

16. DNS – Services, Structure **
    - Μηνύματα, πως λειτουργεί. Σελ. 127
        i. Εμείς ως χρήστες δεν κάνουμε DNS Query.
    - Σελ. 128 Ψευδώνυμα (Υπηρεσίες)
    - Γιατί δεν είναι κεντρικοποιημένο;
    - Κατανεμημένη, Ιεραρχική Βάση Δεδομένων (DNS, TLD, AUTHENTIC DNS)
    - Άλλο πράγμα είναι το domain και άλλο η συγκεκριμένη υπηρεσία σε αυτό το domain.
    - Local DNS Name Server (ISP)
    - Σύγκριση αναδρομικού ερωτήματος με επαναληπτικό ερώτημα + σχήματα. Π.Χ Δίνεται σχήμα και πρέπει να πούμε τι είδους ερώτημα είναι και εξηγήστε γιατί.
    - DNS caching. (Σε ποιο πρωτόκολλο δεν υπάρχει caching; Στο SMTP)
        i. Έχουμε push – pull. Που έχουμε caching;
            a. Πάντα στο Pull έχουμε cache server. Στο SMTP φεύγει από εμένα, άρα δεν υπάρχει λόγος να κρατήσω κάτι. Ενώ στο pull τραβάω δεδομένα για να μην χρειάζεται να τραβάω κάθε λίγο.
    - DNS Records ****
        i. Ανάλογα με το TYPE, τι τιμές θα πάρει το name και το value.** (πχ με ποιο τύπο μπορώ να πάρω ip διεύθυνση στο value;) Πολλαπλής επιλογής. Ή δίδεται εγγραφή με πραγματικές τιμές και ζητείται ποιος τύπος χρησιμοποιείται.
    - P2P απλά την ύπαρξη του.

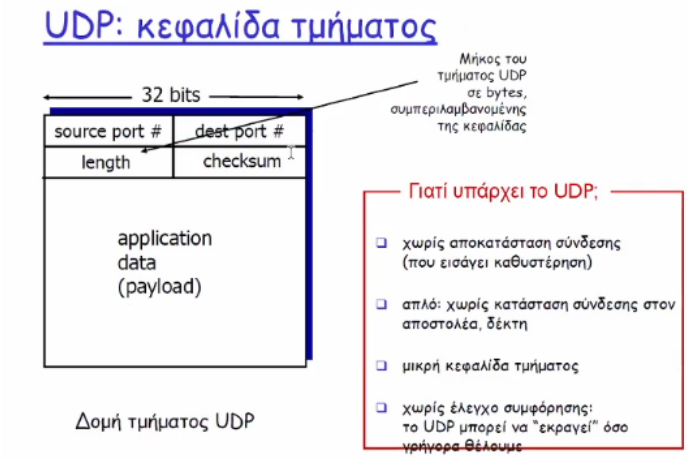
Chapter 3 : Transport Layer

1. Transport Services and Protocols
    - Λογική σύνδεση.
    - Σελ 191
2. Internet Transport-Layer Protocols

- Σύγκριση TCP – UDP (Τι έχει και θεωρείται αξιόπιστο, τι έχει και θεωρείται αναξιόπιστο) σελ 191.

3. Multiplexing/Demultiplexing
    - Τι είναι και που συμβαίνει και πως λειτουργεί το κάθε ένα.
4. UDP **
    - Στο 4ο επίπεδο έχουμε δύο πρωτόκολλα. Γιατί είναι απαραίτητο να έχουμε το UDP αφού δεν είναι αξιόπιστο κλπ; Γιατί κάποιος θα πρότεινε να κάνει εφαρμογή με UDP; Θα μπορούσε να παρέχει αξιοπιστία; Μπορεί μία εφαρμογή που τρέχει πάνω σε UDP να παρέχει αξιόπιστη μεταφορά δεδομένων; ***
        i. Ναι μπορεί να παρέχει αξιόπιστη μεταφορά αλλά αυτό είναι στο χέρι του προγραμματιστή στο 5ο επίπεδο. Το UDP θα κάνει απλά την μεταφορά αλλά δεν θα είναι αξιόπιστη. Ο προγραμματιστής θα πρέπει να προγραμματίσει το πρόγραμμα για την αξιοπιστία και για την επαναμετάδοση.
    - Στο UDP υπάρχει επαναμετάδοση; **
        i. Όχι. Αν χαθεί, χάθηκε.
    - Πως μπορούμε σε ένα streaming να έχουμε ανοχή στις απώλειες;
    - Best effort

5. UDP: κεφαλίδα τμήματος



    -
    - Σε bytes, όχι σε bits.
6. Principles of Reliable Data Transfer σελ 206
    - Τι ειναι αξιοπιστία, τι προυποθέσεις έχει (όλα τα πακέτα παραλαμβάνονται με την σειρά που στέλνονται).
    - Σε ποιο άλλο επίπεδο έχουμε έλεγχο για σφάλματα; Checksum. Γιατί να υπάρχουν και στα δύο επίπεδα έλεγχοι και τα δύο υλοποιούνται με τον ίδιο τρόπο; ***
        i. Έχουμε στο δεύτερο επίπεδο. (CRC)
        ii. Στο δεύτερο επίπεδο πως κάνει τον έλεγχο;

a) Με hardware. Πήλη XOR

- Στο checksum πέρασε τον έλεγχο του 2ου επιπέδου και είδε ότι δεν έχει λάθη. Αφού δεν έχει λάθη στο 2ο επίπεδο, μπορεί να έχει λάθη στο 4ο επίπεδο; ****

7. Rdt2.0: Channel with bit errors
    - ACKs – NAKs
8. Rdt2.0 has a fatal flaw! Σελ 210. **
    - Τι συμβαίνει αν καταστραφεί το ACK/NAK;
9. Rdt2.1: Discussion σελ. 214
10. Rdt2.2: A NAK-free Protocol
    - Τι είναι διπλότυπο ACK;
    - Αν πάρω ένα διπλότυπο ACK είναι σαν να πήρα NAK από τον παραλήπτη με αποτέλεσμα ο αποστολέας να πρέπει να το ξανά στείλει.
11. Rdt3.0: channels with errors and loss. (Πραγματικότητα)
    - Πως δουλεύει από την πλευρά και των δύο; Σελ 216-218
    - Πότε γίνεται η αίσθηση ότι χάσαμε ένα πακέτο;
12. Pipelined Protocols **
    - Τι σημαίνει διοχέτευση;
    - Δύο μορφές διοχέτευσης, εκτενής ανάλυση τους και σύγκριση. ** σελ. 221-225
    - Πόσους χρονομετρητές έχει το go-back-n και πόσους η επιλεκτική επανάληψη;
    - Γιατί να υπάρχουν και τα δύο;
    - Go-back-n τα πάντα. (window size Κλπ) όχι fsm
    - Selective Repeat πως λειτουργεί, τα πάντα. Όχι fsm
13. TCP: Overview
    - Γιατί υπάρχουν πολλά RFCs;
        i. Επειδή σε κάθε RFC βελτιώνω την έκδοση του προηγούμενου.
    - Πλήρες αμφίδρομα.
    - Mss σελ 235
14. TCP Segment Structure σελ. 236-239
    - Ποια είναι τα κοινά με το UDP;
    - Τι είναι το sequence number και τι το acknowledgement number; (Και τα δύο μετριούνται σε bytes) ***
        i. Το sequence number δεν είναι ο αύξον αριθμός του τμήματος αλλά ποιο byte είναι η αρχή αυτού του τμήματος που ξεκινάει.
15. TCP Sequence Numbers, ACKs
    - Σελ 240-241 παράδειγμα
16. TCP Round Trip Time, Timeout
    - Τι θα γίνει αν βάλουμε μικρό RTT και μεγάλο timeout; Τι θα γίνει αν βάλουμε μεγάλο RTT και μικρό timeout;
    - Τι ειναι το RTT;
    - Σελ 242.
17. TCP Reliable data transfer

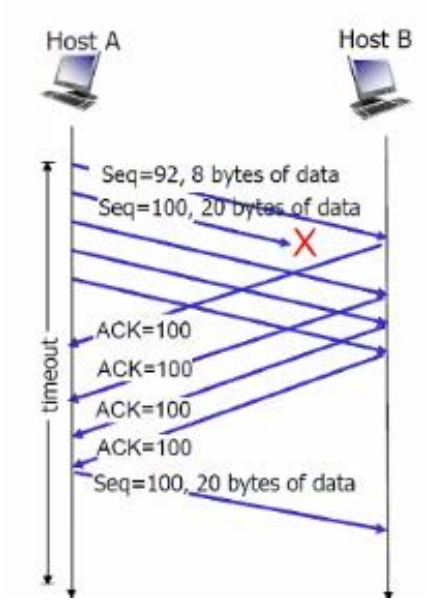
- Τα πάντα
- Πότε γίνεται η αναμετάδοση;

18. TCP Sender Events
    - Τα πάντα.
    - Τι θεωρεί αξιόπιστο το TCP;
        i. Σελ 244
        ii. Αναλίοτο = χωρίς χαμένα bits
        iii. Χωρίς κενά = τα στέλνει ταξινομημένα
        iv. Χωρίς διπλότυπα ACK = Όχι αναμετάδοση
        v. Χρησιμοποιεί ένα χρονομετρητή
19. Σενάρια αναμεταδόσεων TCP ****
    - Σενάριο συσσωρευτικού ACK
        i. Αφού δεν πήρα το ACK 100 και πήρα το ACK 120, θα κάνω αναμετάδοση;
        ii. Έστω ότι στέλνει με seq num = X και έχει X bytes. Ποιο θα είναι το ACK που θα πάρει; Ή ποιο θα είναι το επόμενο seq num.
            a) Συνδυασμός seq num + data bytes.

Παραγωγή TCP ACK [RFC 1122, RFC 2581]

Συμβάν στο δέκτη	Ενέργεια δέκτη TCP
Άφιξη τμήματος σε σειρά με αναμενόμενο # ακολουθίας. Όλα τα δεδομένα μέχρι τον αναμενόμενο # ακολουθίας έχουν επιβεβαιωθεί	Καθυστερημένο ACK. Αναμονή 500ms για το επόμενο τμήμα. Αν όχι επόμενο τμήμα στείλε ACK
Άφιξη τμήματος σε σειρά με αναμενόμενο # ακολουθίας. Ένα άλλο τμήμα περιμένει για μετάδοση ACK	Άμεση αποστολή ενός συσσωρευτικού ACK που κάνει επιβεβαίωση και για τα δύο τμήματα που έφτασαν σε σειρά
Άφιξη τμήματος εκτός σειράς με μεγαλύτερο του αναμενόμενου # ακολουθίας. Ανίχνευση κενού	Άμεση αποστολή *duplicate ACK* που δηλώνει # ακολουθίας επόμενου αναμενόμενου byte
Άφιξη τμήματος που μερικώς ή πλήρως συμπληρώνει κενό στα ληφθέντα δεδομένα	Άμεση αποστολή ACK, αρκεί το τμήμα αυτό να αρχίζει στο κάτω άκρο του κενού

20.
    - Σελ 250 ***
        i. Τι συμβαίνει στον δέκτη, τι συμβαίνει στο TCP. Όταν συμβαίνει το X ποια είναι η ενέργεια του δέκτη;
21. TCP Fast Retransmit ***** σελ. 249
    - Αν ο αποστολέας λάβει 3 διπλότυπα ACKs για τα ίδια δεδομένα, ξανά στέλνει το μη επιβεβαιωμένο τμήμα με το μικρότερο sequence num.

- 

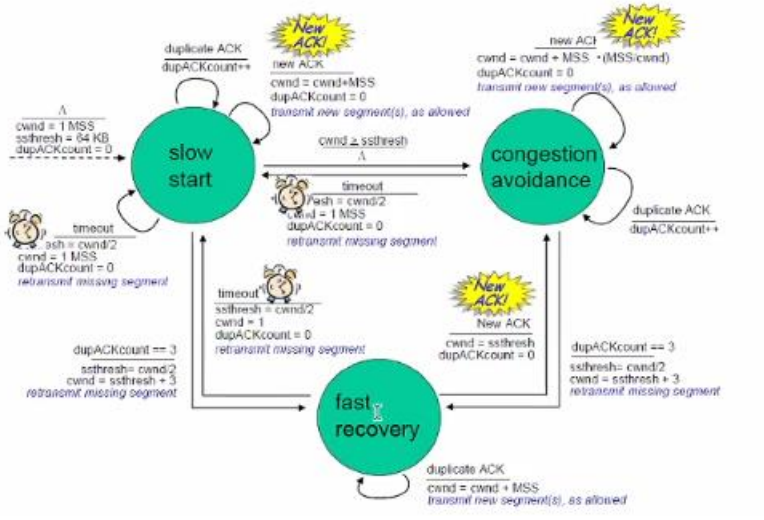
    i. Τι δουλεύει; Go-Back-N ή Selective Repeat;
        a) Δουλευει Selective Repeat γιατί ξέρει ακριβώς ποιο θέλει να ξανά στείλει. Σελ 252.

22. TCP Flow Control σελ 252-254 **
    - Υπηρεσία ταιριάσματος ταχύτητας ➔ ταίριασμα.... στην πλευρά του παραλήπτη. Αφού έχουμε receive buffer
    - Στο free buffer space μπαίνουν αυτά που έρχονται από τον αποστολέα και τα buffered data είναι αυτά που είναι ταξινομημένα και έτοιμα να τα πάρει το 5^{ο} επίπεδο. Ο αποστολέας δεν μπορεί να στείλει περισσότερο από ότι χωράει ο Buffer.
23. Connection Management σελ 255***
    - Ποια ειναι τα βήματα για την τριμερή χειραψία; **
    - Το rcvBuffer size είναι μέρος της δομής TCP;
        i. Το TCP έχει το rcvWindow. Το rcvBuffer είναι μεταβλητή και δεν έχει κάποια σχέση με τον rcvWindow.
24. TCP: Closing a Connection***
    - Ποια είναι τα βήματα για το κλείσιμο;
    - Σελ 258-259. Αν είναι παραμένουσα η σύνδεση μπορεί να κάνει close wait ο σέρβερ και να περιμένει. Ενώ αν είναι μη, κατευθείαν από το established, με το που θα ζητήσει ο άλλος να κλείσει δεν θα πάει σε close wait, θα παει απευθείας σε close.
25. Principles of congestion control
    - Διαφορά ελέγχου ροής με ελέγχου συμφώρησης.
26. TCP Congestion Control ****** PERMA SOS
    - Additive increase, multiplicative decrease.
    - Σελ 269 3 ερωτήσεις.
    - Τι είναι το cwnd; Πως καθορίζεται; ****

i. Είναι μεταβλητή. Δεν υπάρχει στην δομή του TCP.

- Μαθηματικός τύπους σελ 270.

27. Slow Start **** Θέματα ανάπτυξης.
    - 3 καταστάσεις (Πως λειτουργούν) *** σελ 272-274
        i. Αργή εκκίνηση
        ii. Αποφυγή συμφόρησης
        iii. Ταχεία ανάκαμψη
    - Όσο παίρνω απαντήσεις, ανεβαίνει ο ρυθμός.
    - Όταν ξεκινά η σύνδεση, CongWin = 1MSS
        i. ΠΧ MSS = 500Bytes & RTT = 200msec
        Αρχικός ρυθμός = 20kbps
        (500bytes*8bits/byte*1/0/2sec) ****** Για να βρούμε τον ρυθμό.
        MSS/RTT
    - TCP: Detecting, Reacting to Loss
        i. TCP Tahoe, TCP Reno (τι είναι, πως χρησιμοποιούνται, rules, threshold ½, Κλπ). Σελ 276-277
        ii. Πότε πρέπει να γίνει η αλλαγή από εκθετική σε γραμμική αύξηση;
    - Summary: TCP Congestion Control **** Σ/Λ
        i. Είμαστε σε κατάσταση fast recovery και γίνεται timeout. Σε ποια κατάσταση θα παω;
            a) Στο slow start.
        ii. Είμαστε σε κατάσταση fast recovery και παίρνω ACK. Σε ποια κατάσταση θα παω;
            a) Στο congestion avoidance.
        iii.



- Ποια είναι η σύγκριση ανάμεσα στην ταχεία ανάκαμψη και στην ταχεία αναμετάδοση; Ομοιότητες και διαφορές. (το ταχεία δεν παροτρίνει ότι είναι ομοιότητα). Σελ 249-251, 274-276. ****

28. Σύνοψη: Έλεγχος συμφόρησης του TCP σελ 278

- Είναι διαφορετικό το Window receiver από το Congestion Window. Το window receiver είναι πεδίο μέσα στην κεφαλίδα του TCP που λέει πόσα είναι τα ελεύθερα byte στον buffer. Το congestion window είναι μεταβλητή.

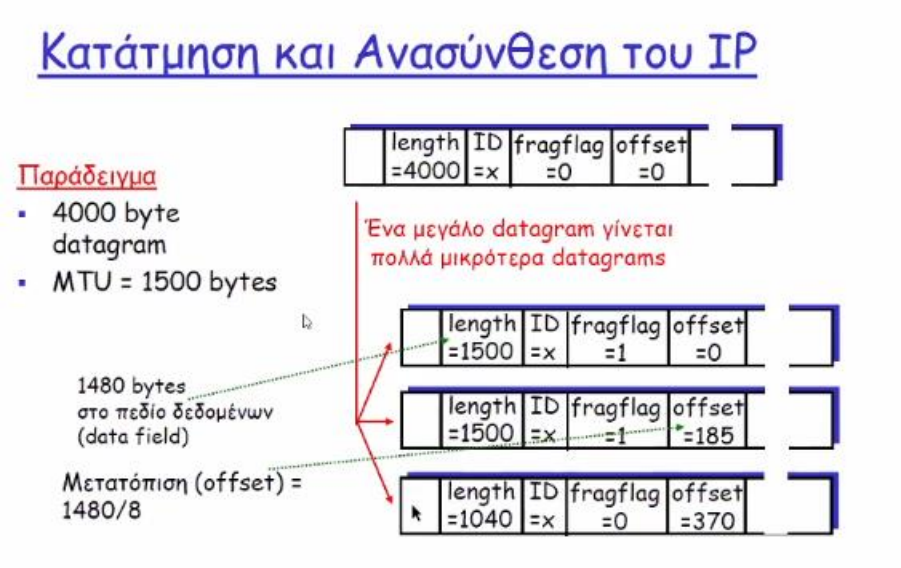
29.

Κατάσταση	Συμβάν	Ενέργεια αποστολέα TCP	Σχόλια
Αργή Εκκίνηση Slow Start (SS)	Λήψη ACK για δεδομένα που δεν έχουν επιβεβαιωθεί προηγουμένως	CongWin = CongWin + MSS, If (CongWin > Threshold) θέσε κατάσταση σε «Αποφυγή Συμφόρησης»	Έχει ως αποτέλεσμα διπλασιασμό του CongWin σε κάθε RTT
Αποφυγή Συμφόρησης Congestion Avoidance (CA)	Λήψη ACK για δεδομένα που δεν έχουν επιβεβαιωθεί προηγουμένως	CongWin = CongWin+MSS * (MSS/CongWin)	Προσθετική αύξηση που έχει ως αποτέλεσμα αύξηση του CongWin κατά 1 MSS σε κάθε RTT
SS ή CA	Ανίχνευση συμβάντος απώλειας από τρία διπλότυπα ACK	Threshold = CongWin/2, CongWin = Threshold, θέσε κατάσταση σε «Αποφυγή Συμφόρησης»	Ταχεία επαναφορά, υλοποιώντας πολλαπλασιαστική μείωση. Το CongWin δεν θα πέσει κάτω από1 MSS.
SS ή CA	Λήξη χρόνου (Timeout)	Threshold = CongWin/2, CongWin = 1 MSS, Θέσε κατάσταση σε «Αργή Εκκίνηση»	Είσοδος σε «Αργή Εκκίνηση»
SS ή CA	Διπλότυπο ACK	Αύξηση του μετρητή διπλότυπων ACK για το τμήμα η λήψη του οποίου επιβεβαιώθηκε	Τα CongWin και Threshold δεν αλλάζουν

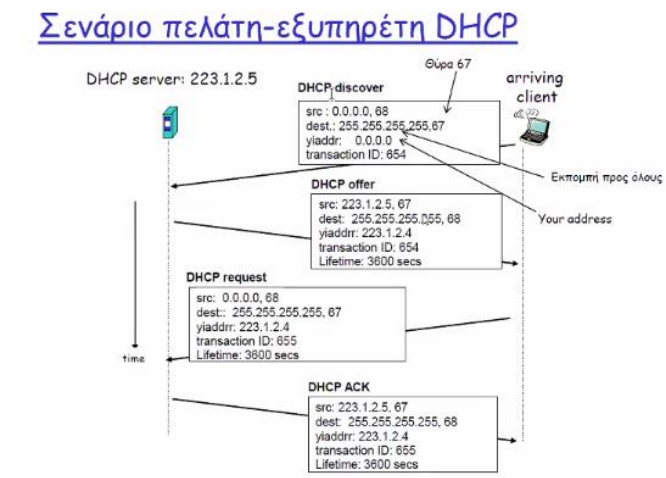
*****

Chapter 4 : The Network Layer: Data Plane

1. Two Key Network-Layer Functions
    - Τι είναι προώθηση, τι είναι δρομολόγηση;
    - Ο κάθε ένας δρομολογητής πρέπει να έχει ένα πίνακα προώθησης.
2. Μοντέλο υπηρεσιών δικτύου
    - Τι συμβαίνει στα ξεχωριστά datagrams και τι στη ροή datagrams
3. IP datagram format
4. Κατάτμηση σελ 333-334 ****
    - Γιατί συμβαίνει η κατάτμηση;
    - Η ανασύνθεση γίνεται στον τελευταίο δρομολογητή.



-
    i. Το 1040 από που βγήκε και γιατί 1500;
        a. Τα καθαρά data είναι length value - 40 bytes(20IP+20TCP/αλλιώς +8UDP)
    ii. Τι είναι τα fragflag, offset
5. DHCP **** σελ 342
    - Πως λειτουργεί; Πως είναι η διαδικασία για να πάρω IP Address;
    - Επισκόπηση DHCP



-
    i. Από το 5ο επίπεδο έρχεται το DHCP Discover
6. NAT σελ 345-347
    - Τι είναι και πως λειτουργεί;

Chapter 5: The Network Layer: Control Pane

1. ICMP σελ 419

- Τι είναι, πως λειτουργεί το traceroute.
- Κριτήριο λήξης

Chapter 6: The Link Layer and LANs

1. Διευθυνσιοδότηση
    - Διευθυνσιοδότηση έχουμε μόνο στο $3^{ο}$ και $2^{ο}$ επίπεδο. Στο $4^{ο}$ δεν έχουμε διευθυνσιοδότηση αλλά έχουμε τον αριθμό θύρας όπου με τον συνδυασμό των IPs βγάζουν το socket.
2. Link Layer: Introduction
    - Το επίπεδο ζεύξης δεδομένων έχει την ευθύνη μεταφοράς των datagrams από ένα κόμβο σε φυσικά γειτονικό κόμβο πάνω από μία ζεύξη. (η λειτουργία του)
3. Link Layer: Context
4. Link Layer Services σελ 442-443
    - Όλα
5. Where is the Link Layer Implemented
    - Συνδυασμός hardware, software, firmware.
    - Που υλοποιείται το επίπεδο ζεύξης; Σε ένα Η/Υ που συμβαίνει αυτό; Σελ 443-444 ****
    - Τι είναι το firmware;
        i. Είναι ο driver της κάρτας δικτύου.
6. Error Detection
    - Όλα
7. Πως λειτουργεί ο CRC και τι μπορεί να βρει;
    - Όχι μαθηματικά.
8. Multiple Access Links, Protocols
    - Δύο είδη ζεύξεων
    - Σύγκρουση σελ. 453
    - Broadcast
9. An ideal multiple access protocol
    - Γιατί θέλουμε να είναι απλό το πρωτόκολλο;
        i. Γιατι το έχουμε να υλοποιείται κυκλωματικά. Με hardware. Αν ήταν περίπλοκο θα έπρεπε να χρησιμοποιήσουμε software με αποτέλεσμα να είναι αργό.
10. MAC Protocols: Taxonomy
    - Τρεις κατηγορίες.
    - TDMA, FDMA ανάλυση τους. Σελ 454-455

11. Random Access Protocols σελ 455-456
    - Απλή γνώση
12. CSMA σελ. 459

- Τι είναι το CSMA, πως λειτουργεί;
- Συγκρούσεις CSMA

13. CSMA/CD σελ. 461
    - Ανίχνευση σύγκρουσης (γίνεται κυκλωματικά)
14. Ethernet CSMA/CD Algorithm σελ 464
    - Τα βήματα αλλά mostly βήμα 5.
15. Taking Turns MAC Protocols
    - Token passing, polling
16. MAC Addresses and ARP Σελ 468-469
    - Τι είναι τα MAC Addresses;
    - Γιατί υπάρχουν δύο είδη διευθυνσιοδότησης;
17. ARP: Address Resolution Protocol σελ 470-471 ***
    - Είναι αυτό που ζευγαρώνει τις διευθυνσιοδοτήσεις 3ου επιπέδου με τις διευθυνσιοδοτήσεις 2ου επιπέδου.
    - Τι μαθαίνουμε μέσω του ARP;
    - Σύγκριση ARP – DNS ****
        i. Όπως και το dns ψάχνουμε μία ip ενός συγκεκριμένου server, έτσι αντίστοιχα ψάχνουμε μία συγκεκριμένη διεύθυνση που αντιστοιχεί σε μία συγκεκριμένη MAC. ΚΑΙ ΑΛΛΕΣ ΟΜΟΙΟΤΗΤΕΣ ΔΙΑΦΟΡΕΣ ΣΤΟ ΤΕΤΡΑΔΙΟ.
    - Πατάει και σε 3ο και σε 2ο επίπεδο. Δεν είναι ξεκάθαρα του 2ου επειδή παίρνει πληροφορίες και από τα δύο επίπεδα.
    - Πως μαθαίνουμε την MAC διεύθυνση του άλλου;
        i. Εξήγηση στο τετράδιο. Broadcast – Unicast.
18. Routing to another LAN όλες οι υποθέσεις
    - Routing to Another LAN σελ. 473 ***
        i. Πως θα παει στο επόμενο subnet;
    - Αν ο Β είναι ένας server, με ποιο πρωτόκολλο θα μάθουμε την IP του;
        i. Με DNS θα μάθω την IP του και μετά μέσω του ARP θα μάθουμε την MAC του και να μεταφερθεί το πακέτο.
    - 3η υπόθεση. (πως;) Με ποιο πρωτόκολλο μαθαίνει το gateway; ΔΕΝ χρησιμοποιείται static routing.
        i. Με το DHCP θα μάθουμε ποιος είναι ο router πρώτου hop.
    - 4η υπόθεση. (πως;)
        i. Με ARP θα μάθουμε την MAC.
19. Ethernet σελ 475
    - Είναι ελεύθερο συγκρούσεων. Πως;
20. Δομή πλαισίου
    - Σύγκριση 3ου επιπέδου με 2ου επιπέδου στα source – destination. Γιατί στο Ethernet είναι πρώτα το dest και μετά source ενώ στο IP είναι πρώτα το source και μετά το dest;

i. Επειδή η MAC Address βλέπει πρώτα το destination για να δει αν το πλαίσιο προωρίζεται για αυτήν. Αν δεν είναι για αυτήν τότε δεν προχωράει στα παραπάνω επίπεδα και συνεχίζεται το ψάξιμο για να βρει το πλαίσιο που ανήκει.

- Το CRC μας δίχνει από το destination και όλα τα data. Άρα όταν θα φτάσουμε στον παραλήπτη και εφόσον δει ότι το dest add είναι για αυτόν, παίρνει τα data και το CRC και κάνει compare το δικό του CRC με τις NIC. Αν είναι ίδια τότε οκευ, αλλιώς απορρίπτεται το πλαίσιο. Σελ 477.
- Ερώτηση τετραδίου για σύγκριση πρωτοκόλλων.
- Παραμένουσα – μη παραμένουσα. Σε ποια άλλα πρωτόκολλα έχουμε παραμένουσα – μη παραμένουσα; ****
    i. HTTP
    ii. Η σύνδεση που έχει ο Η/Υ μου με το default gateway είναι παραμένουσα ή μη παραμένουσα;
        1. ARP Table. Για όσο υπάρχει το TTL και βρίσκεται μέσα στον πίνακα μου, για όλο αυτό το χρονικό διάστημα είναι παραμένουσα. Γιατί ξέρω ότι μέσα στον πίνακα του ARP ποια είναι η φυσική σύνδεση η MAC Address που είναι το default gateway για εμένα. Έχω αντίστοιχα και την IP του, αν δεν την έχω την βρίσκω μέσω DNS (αν προσφέρει κάποιο service) αλλιώς δεν μπορώ να μάθω την IP οποιουδήποτε Η/Υ μέσω του DNS.
- Τι είναι η δυαδική οπισθοχώρηση;
- Τι είναι ο μεταγωγέας;

21. Switches
    - Όλα
    - Ιδιότητες μεταγωγέων σελ 484.
    - Σελ 486-487 σύγκριση μεταγωγών – δρομολογητών. Τι έχει ο δρομολογητής και τι ο μεταγωγέας. Υπερ – Κατά. Και οι δύο έχουν πίνακες δρομολόγησης***
22. A day in the life of a web request. ******
    - Το παράδειγμα. Τετράδιο.
    - Συγκρίσεις ARP – DNS
    - Που χρησιμοποιούμε TCP, UDP, IP, Ethernet.

Chapter 1: Introduction

1. Τι είναι πρωτόκολλο;
    - Ένα πρωτόκολλο ορίζει την μορφή και την σειρά των μηνυμάτων που ανταλλάσσονται ανάμεσα σε δύο ή περισσότερες επικοινωνούσες οντότητες, όπως και τις ενέργειες που λαμβάνουν χώρα κατά την διάρκεια της μετάδοσης και/ή της λήψης ενός μηνύματος ή άλλου συμβάντος.

2. Μεταγωγή πακέτου έναντι Μεταγωγής Κυκλώματος
    - Η μεταγωγή πακέτου επιτρέπει σε περισσότερους χρήστες να χρησιμοποιούν το δίκτυο ενώ στην μεταγωγή κυκλώματος από την μία άκρη στην άλλη άκρη, δεσμεύονται όλες οι συνδέσεις έτσι ώστε να είναι σαν reserved μεταξύ του αποστολέα και του παραλήπτη.
    - Η μεταγωγή πακέτου προσφέρει καλύτερο διαμοιρασμό της χωρητικότητας μετάδοσης από την μεταγωγή του κυκλώματος
    - Η μεταγωγή πακέτου είναι απλούστερη, πιο αποδοτική και λιγότερο ακριβή να υλοποιηθεί από την μεταγωγή κυκλώματος.
        i. Η μεταγωγή κυκλώματος είναι πιο αποδοτική γιατί δεσμεύει εκ των προτέρων την χρήση της ζεύξης μετάδοσης, ανεξάρτητα από την ζήτηση, οπότε ο δεσμευμένος, αλλά μη χρησιμοποιούμενος χρόνος ζύξης παραμένει αχρησιμοποίητος. Η μεταγωγή πακέτου από την άλλη, δεσμεύει την χρήση της ζεύξης κατα απαίτηση. Η δυνατότητα μετάδοσης της ζεύξης μοιράζεται κατά πακέτο, μόνον ανάμεσα σε εκείνους τους χρήστες που έχουν πακέτα, τα οποία πρέπει να μεταδοθούν μέσω της ζεύξης.

Chapter 2: Application Layer

1. Ποιες είναι οι δύο αρχιτεκτονικές; Εξηγήστε τι κάνει η κάθε μία.
    a. Client – Server
        i. Στην αρχιτεκτονική Client – Server υπάρχει ένας διαθέσιμος εξυπηρέτης (server) ο οποίος δέχεται αιτήσεις για υπηρεσίες από άλλους υπολογιστές (clients).
        ii. Ο server έχει static IP και όχι dynamic IP. Δηλαδή η IP του είναι σταθερή και δεν αλλάζει ποτέ. Ξέρουμε ότι σε αυτή την IP θα απαντάει πάντα ο συγκεκριμένος Server.
        iii. Οι clients επικοινωνούν με τον server για να εξυπηρετηθούν. Έχουν dynamic IP την οποία την παίρνουν από τον ISP και συνδέονται ανά διαστήματα στους servers.
    b. P2P
        i. Είναι μία αρχιτεκτονική στην οποία μιλάνε δύο End-devices μεταξύ τους απευθείας χωρίς την ύπαρξη κάποιου server. Ανάλογα με το ποιος ζητάει

και ποιος δίνει, χαρακτηρίζεται και ο client-server. Άρα είναι και clients και servers.

ii. Ένα χαρακτηριστικό είναι η αυτοκλιμάκωση τους (self-scalability). Αυτό σημαίνει ότι μπορεί και να δίνει αρχεία και να παίρνει αρχεία ταυτόχρονα.

2. Σύγκριση Client-Server – P2P
    a. Διαφορές
        i. Στο Client-Server υπάρχει επικοινωνία μεταξύ end-device και server, ενώ στο P2P η επικοινωνία είναι μεταξύ των end-devices.
        ii. Στο Client-Server ο client είναι μόνο πελάτης, ενώ στο P2P είναι και πελάτης και server ταυτόχρονα.
        iii. Στο Client-Server υπάρχουν οι servers, ενώ στο P2P δεν υπάρχουν.

3. Αν το Client-Server το γράψουμε Master-Slave είναι το ίδιο;
    a. Σαν αρχιτεκτονική ναι είναι το ίδιο, όμως δεν έχουν την ίδια επικοινωνία. Master είναι κάποιος που έχει μεγαλύτερη γνώση και είναι πάνω από τον Client.

4. Στο P2P έχουμε Master-Slave;
    a. Όχι επειδή έχουμε ισότητα. Επικοινωνούν δύο hosts-end-devices μεταξύ τους απευθείας.

5. Ποιος ξεκινάει την επικοινωνία; Ο εξυπηρετητής;
    a. Ο πελάτης πάντα εκκινεί την επικοινωνία. Η διεργασία του πελάτη εκκινεί την επικοινωνία και η διεργασία του εξυπηρετητή περιμένει για να εξυπηρετήσει το αίτημα.

6. Τι είναι τα sockets;
    a. Τα sockets είναι μία software διεπαφή (API) η οποία βοηθάει στο να στείλουμε και να παραλάβουμε μηνύματα από το δίκτυο. Όταν μία διεργασία (αποστολέα) θέλει να στείλει ένα μήνυμα σε μία άλλη διεργασία, που βρίσκεται σε έναν άλλον υπολογιστή, σπρώχνει το μήνυμα έξω από την πόρτα της (socket). Όταν το μήνυμα φτάσει στον υπολογιστή προορισμού, περνά μέσα από την πόρτα (socket) της διεργασίας λήψης και η διεργασία λήψης ενεργεί επί του μηνύματος.

7. Διευθυνσιοδότηση διεργασιών
    a. Για να προσδιορίσει κάποιος την ταυτότητα της διεργασίας λήψης, πρέπει να καθοριστούν οι πληροφορίες για την IP Address του υπολογιστή και τον αριθμό θύρας που σχετίζεται με την διεργασία στον υπολογιστή. IP Address : Port Number = Socket.

8. Τι πρέπει να ορίζει ένα πρωτόκολλο επιπέδου εφαρμογής;

a. Πρέπει να ορίζει:
    i. Τι είδους μηνύματα ανταλλάσσονται ➔ Αίτηση, απόκριση
    ii. Την σύνταξη του μηνύματος ➔ Τα πεδία που υπάρχουν (θέση, αριθμός)
    iii. Την σημασιολογία του μηνύματος ➔ Με βάση τις πληροφορίες των πεδίων.
    iv. Τους κανόνες ➔ Πότε και πως οι διεργασίες στέλνουν και απαντούν στα μηνύματα. Υπάρχουν διαφορετικοί κανόνες στις δύο αρχιτεκτονικές μεταξύ τους.

9. Τι υπηρεσίες μεταφοράς απαιτούν οι εφαρμογές; Που χρησιμοποιούνται;
    a. Αξιόπιστη μεταφορά
        i. Τα πακέτα πρέπει να πάνε με αξιοπιστία
        ii. Είναι αναγκαία στις εφαρμογές για ηλεκτρονικό ταχυδρομείο, μεταφοράς αρχείων, χρηματοοικονομικές εφαρμογές κλπ.
    b. Ρυθμαπόδοση (Throughput)
        i. Είναι ο χρονικός ρυθμός με τον οποίον ένας υπολογιστής αποστέλλει ή λαμβάνει δεδομένα. Πόσα μπιτ μεταδίδονται μέσω αυτών των συνδέσεων.
    c. Χρονισμός
        i. Η απαίτηση χαμηλής καθυστέρησης για να είναι αποτελεσματικές
        ii. Είναι αναγκαία στα παιχνίδια, στα βίντεο με ήχο
    d. Ασφάλεια
        i. Η ανάγκη κρυπτογράφησης και η ακεραιότητα των δεδομένων
        ii. Είναι αναγκαία σχεδόν παντού.

10.

Εφαρμογή	Απώλεια δεδομένων	Ρυθμαπόδοση	Ευαισθησία ως προς το χρόνο
Μεταφορά αρχείου	όχι απώλειες	ελαστική	όχι
e-mail	όχι απώλειες	ελαστική	όχι
Έγγραφα Web	όχι απώλειες	ελαστική	όχι
Ήχος/ βίντεο πραγματικού χρόνου	ανοχή στις απώλειες	ήχος: 5kbps-1Mbps, βίντεο:10kbps-5Mbps	ναι, 100δες msec
Αποθηκευμένος ήχος/βίντεο	ανοχή στην απώλειες	ίδια με παραπάνω	ναι, λίγα secs
Διαδραστικά παιχνίδια	ανοχή στην απώλειες	ως λίγα kbps	ναι, 100δες msec
Μηνύματα κειμένου	όχι απώλειες	ελαστική	ναι και όχι

11. TCP – UDP

a. TCP
    i. Η σύνδεση μεταξύ των διεργασιών είναι αμφίδρομη. Δηλαδή οι δύο διεργασίες μπορούν να στέλνουν μηνύματα μεταξύ τους μέσω της σύνδεσης ταυτόχρονα.
    ii. Έχει αξιόπιστη μεταφορά μεταξύ των διεργασιών
    iii. Έχει έλεγχο ροής. Δηλαδή δεν θα υπερφορτώσει τον παραλήπτη.
    iv. Έχει έλεγχο συμφόρησης. Ενημερώνει τον χρήστη αν το πακέτο που θα αργήσει λόγω υπερφόρτωσης του δικτύου.
    v. Δεν προσφέρει χρονισμό, minimum throughput και security.
    vi. Πρέπει να γίνει η τριμερής χειραψία πριν ξεκινήσει η μεταφορά.
b. UDP
    i. Δεν είναι αξιόπιστη η μεταφορά. Δηλαδή το μήνυμα μπορεί να μην φτάσει ποτέ στον παραλήπτη. Αν φτάσουν τα μηνύματα, μπορούν να φτάσουν εκτός σειράς.
    ii. Είναι ασυνδεσμικό οπότε δεν χρειάζεται η χειραψία.
    iii. Δεν έχει έλεγχο συμφόρησης οπότε μπορεί να τροφοδοτεί με δεδομένα το επίπεδο δικτύου με όποιο ρυθμό θέλει.
    iv. Δεν προσφέρει αξιοπιστία, έλεγχο ροής, έλεγχο συμφόρησης, χρονισμό, throughput, security και connection oriented.
c. Σύγκριση TCP – UDP
    i. Διαφορές
        1. Στο TCP υπάρχει η τριμερής χειραψία για να ξεκινήσει η μεταφορά των δεδομένων, ενώ στο UDP όχι.
        2. Στο TCP υπάρχει αξιόπιστη μεταφορά δεδομένων μεταξύ των διεργασιών, ενώ στο UDP δεν υπάρχει αξιοπιστία.
        3. Στο TCP υπάρχει ο έλεγχος ροής αλλά στο UDP όχι.
        4. Στο TCP υπάρχει ο έλεγχος συμφόρησης ενώ στο UDP όχι.
    ii. Κοινά
        1. Και στα δύο μπορούν οι διεργασίες να στέλνουν και να λαμβάνουν δεδομένα ταυτόχρονα.
        2. Και στα δύο δεν υπάρχει η ρυθμαπόδοση.
        3. Δεν παρέχουν ασφάλεια.
        4. Δεν παρέχουν χρονισμό.
d. Το TCP έχει κρυπτογράφηση;
        1. Έχει έμμεσα κρυπτογράφηση μέσω του SSL στο 5^{ο} επίπεδο. Δεν έχει αυτόματα μέσα του το TCP κρυπτογράφηση. Το καθορίζει ο προγραμματιστής στο 5^{ο} επίπεδο.
e. Γιατί υπάρχει το UDP;
    i. Επειδή είναι γρήγορο λόγω της μικρής κεφαλίδας και το ότι δεν χρειάζεται η τριμερής χειραψία.

12.

Εφαρμογή	Πρωτόκολλο εφαρμογής	Υποκείμενο Πρωτόκολλο μεταφοράς
Ηλεκτρονικό ταχυδρομείο e-mail	SMTP [RFC 2821]	TCP
Απομακρυσμένη προσπέλαση τερματικού	Telnet [RFC 854]	TCP
Web	HTTP [RFC 2616]	TCP
Μεταφορά αρχείων	FTP [RFC 959]	TCP
Πολυμέσα συνεχούς ροής	HTTP (π.χ. YouTube), RTP[RFC 1889]	TCP ή UDP
Τηλεφωνία Διαδικτύου	SIP, RTP, ιδιοταγές (π.χ. Skype)	TCP ή UDP

   a. Τηλεφωνία διαδικτύου ➔ Δεν είμαστε σίγουροι επειδή είναι ιδιωταγές. Όταν είναι ιδιωτικό δεν ξέρουμε τι χρησιμοποιεί πιο κάτω.

13. HTTP
   a. Το HTTP είναι πρωτόκολλο 5ου επιπέδου και είναι ορίζει πως οι πελάτες ζητούν ιστοσελίδες από το Web και πως οι servers μεταφέρουν ιστοσελίδες σε πελάτες. Ο browser στέλνει μηνύματα αίτησης HTTP για τα αντικείμενα της σελίδας στον server. Ο Server λαμβάνει τις αιτήσεις και αποκρίνεται με μηνύματα απόκρισης HTTP τα οποία περιέχουν τα αντικείμενα.
   b. Το HTTP χρησιμοποιεί TCP ως πρωτόκολλο μεταφοράς. Ο πελάτης εκκινεί πρώτα μία σύνδεση TCP με τον σερβερ και ανταλλάσσουν τα δεδομένα μέσω των sockets.
   c. Το HTTP είναι ακαταστατικό(stateless). Δηλαδή δεν κρατά πληροφορίες για τους πελάτες. Ο σερβερ στέλνει τα αιτούμενα αρχεία σε πελάτες, χωρίς να αποθηκεύει πληροφορίες κατάστασης για τον πελάτη. Αν ένας συγκεκριμένος πελάτης ζητήσει το ίδιο αντικείμενο δύο φορές μέσα σε μία περίοδο χρόνου, ο σερβερ δεν αποκρίνεται λέγοντας ότι μόλις έδωσε το αντικείμενο στον πελάτη. Αντί αυτού ο σερβερ θα απαντήσει στην αίτηση του πελάτη επειδή έχει ξεχάσει τελείως τι έκανε προηγουμένως.
   d. Το HTTP χρησιμοποιεί την αρχιτεκτονική εφαρμογής Client-Server.
   e. Το HTTP δεν ασχολείται με τα χαμένα δεδομένα. Είναι ευθύνη του TCP.
   f. Τι είναι καταστατικό και τι ακαταστατικό. Ποια πρωτόκολλα είναι ακαταστατικά και ποια ακαταστατικά.

14. Τι είναι παραμένουσα και τι μη-παραμένουσα;
   a. Μη παραμένον HTTP είναι όταν κάθε σύνδεση TCP κλείνει αφού ο σέρβερ στείλει το αντικείμενο στον πελάτη. Άρα αν ζητήσω πολλά πράγματα, θα πρέπει να ανοιγοκλείνω συνέχεια την σύνδεση.
   b. Παραμένον HTTP είναι όταν έχουμε ένα ανοιχτό κανάλι TCP μεταξύ του πελάτη και του σέρβερ και μπορούμε να ανταλλάσσουμε συνέχεια τα αντικείμενα που θέλουμε από την ίδια σύνδεση η οποία δεν κλείνει.

15. Παραμένον HTTP – Μη-Παραμένον HTTP – RTT

a. Το RTT είναι ο χρόνος που χρειάζεται το οποιοδήποτε πακέτο για να ταξιδέψει από τον πελάτη προς τον σέρβερ και μετά πάλι πίσω στον πελάτη.
b. Πόσα RTT χρειάζεται για το κάθε αντικείμενο για να μεταφερθεί στις μη-παραμένουσες και πόσες στις παραμένουσες;
    i. Στις μη-παραμένουσες για κάθε αντικείμενο απαιτούνται 2 RTT. Ένα για το TCP και ένα για την αποστολή.
    ii. Στις παραμένουσες απαιτούνται 2 RTT και στην συνέχεια 1 RTT. Αρχικά τα 2 RTT για να γίνει η εγκαθίδρηση της σύνδεσης και για το αντικείμενο και μετά αφού θα παραμείνει η σύνδεση ανοιχτή θα απαιτείται 1 RTT μόνο για το αντικείμενο.

16. Cookies
    a. Τι είναι τα cookies, σε τι εξυπηρετούν και γιατί δεν θέλουμε να χρησιμοποιούνται;
        i. Τα cookies είναι ένας τρόπος έτσι ώστε να βοηθήσουν στο να κρατούν μία κατάσταση. Μπορούν να βοηθήσουν στο να γίνεται η πιστοποίηση, να αποθηκεύονται τα shopping carts, να σου εμφανίζονται recommendations και για να κρατάει τα δεδομένα.
        ii. Δεν θέλουμε να χρησιμοποιούνται επειδή μπορούν να θεωρηθούν ως παραβίαση της ιδιοτικότητας μας.

17. Web Caches (Proxy Server)
    a. Τι είναι και πως χρησιμοποιούνται;
        i. Οι Proxy Servers είναι κάποιοι ενδιάμεσοι σέρβερς οι οποίοι έχουν τον δικό τους χώρο αποθήκευσης και κρατάνε αντίγραφα από ιστοσελίδες που ζητήθηκαν πρόσφατα. Ο χρήστης πρέπει να ορίσει τον browser ότι θέλει να έχει access μέσο του web cache για να μην χρειάζεται να πηγαίνει στον origin και να υπάρχει καθυστέρηση.
        ii. Βήματα ζήτησης αντικειμένου
            1. Ο browser καθορίζει μία σύνδεση TCP προς τον Proxy Server και στέλνει μία αίτηση HTTP για το αντικείμενο στον Proxy Server.
            2. Ο Proxy Server ελέγχει για να δει αν έχει αποθηκευμένο τοπικά ένα αντίγραφο του αντικειμένου. Αν το έχει τότε επιστρέφει το αντικείμενο στον πελάτη.
            3. Αν ο Proxy Server δεν έχει το αντκείμενο, τότεο ο Proxy Server ανοίγει μία σύνδεση TCP με τον Origin Server. Ο Proxy Server στέλνει μία αίτηση HTTP για το αντικείμενο. Αφού λάβει αυτήν την αίτηση, ο Origin στέλνει το αντικείμενο μέσα σε ένα HTTP Response στον Proxy Server.
            4. Όταν ο Proxy Server λάβει το αντικείμενο, αποθηκεύει ένα αντίγραφο του στον τοπικό χώρο αποθήκευσης και στέλνει ένα άλλο αντίγραφο στον πελάτη.

b. Ο Proxy Server είναι ταυτόχρονα και σερβερ και πελάτης. Όταν δέχεται αιτήσεις είναι σέρβερ και όταν στέλνει αιτήσεις στον Origin είναι πελάτης.
c. Ποιά είναι τα θετικά του Proxy Server;
    i. Μειώνει τον χρόνο αναμονής του πελάτη γιατί δεν χρειάζεται να επικοινωνήσει με τον origin.
    ii. Μειώνει την κίνηση με την ζεύξη που έχει το ίδρυμα-εταιρία προς τα έξω.
    iii. Σε κάποιους ISP που έχουν φτωχό περιεχόμενο μοιράζει πιο έξυπνα το περιεχόμενο.

18. Τι είναι το Get υπο συνθήκη και πως λειτουργεί με τον Proxy Server;
    a. Το GET υπο συνθήκη είναι ένας μηχανισμός του HTTP ο οποίος επιτρέπει στην cache να επιβεβαιώνει ότι όλα τα αντικείμενα της είναι ενημερωμένα. Όποτε ζητάει ο Proxy Server ένα request, γίνεται το request If-modified-since:<date> στον origin. Αν είναι outdated τότε πρέπει να κατεβάσει το καινούργιο. Αν είναι dated τότε του απαντάει με 304 Not Modified.

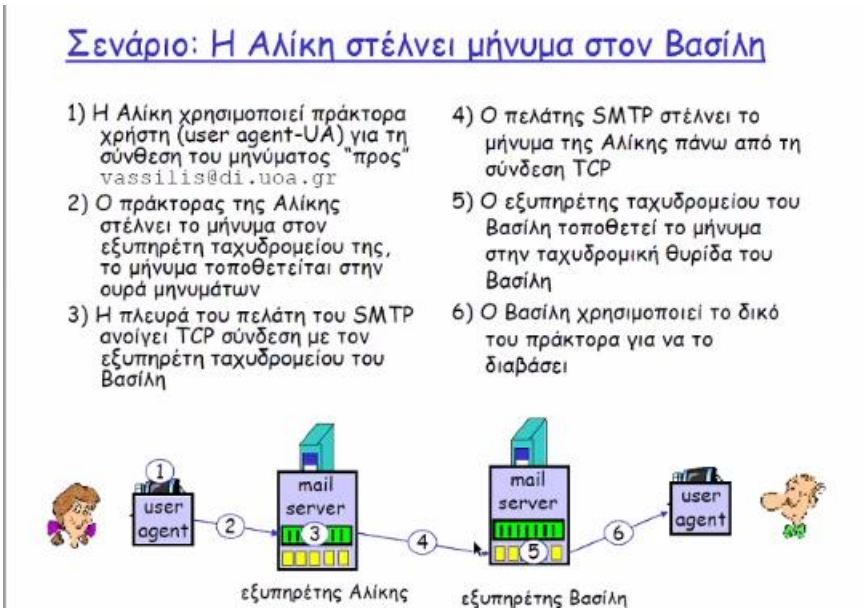
19. Ηλεκτρονικό ταχυδρομείο
    a. Ποια είναι τα τρία κύρια συστατικά μέρη και τι είναι το κάθε ένα;
        i. Πράκτορες χρήστη (user agents)
            1. Οι πράκτορες χρήστη είναι οι εφαρμογές που χρησιμοποιούμε για να διαβάζουμε τα emails.
        ii. Εξυπηρέτες ταχυδρομείου (mail servers)
            1. Οι mail servers έχουν γραμματοθυρίδες για τον κάθε εγγεγραμμένο χρήστη.
            2. Όταν στείλουμε ένα mail, το παίρνει ο mail server, το βάζει σε μία ουρά και έχει status to-be-send. Σε αυτή την ουρά αρχίζει και στέλνει τα mails στους άλλους mail servers.
            3. Ο κάθε mail server όταν στέλνει είναι πελάτης και όταν δέχεται είναι σέρβερ.
        iii. Πρωτόκολλο SMTP
    b. SMTP
        i. Το SMTP χρησιμοποιεί TCP για την αξιόπιστη μεταφορά των mails μέσω της πόρτας 25.
        ii. Στο SMTP μιλάνε μόνο σέρβερ μεταξύ τους και δεν εμπλέκονται end-devices.
        iii. Υπάρχει η τριμερής χειραψία.
        iv. Είναι παραμένον επειδή εαν ο πελάτης έχει και άλλα μηνύματα να στείλει στον σέρβερ θα τα στείλει μέσω της ίδιας TCP σύνδεσης και αφού τελειώσει θα δώσει εντολέι στο TCP να κλείσει την σύνδεση.

20. Σύγκριση SMTP – HTTP
    a. Κοινά

i. Και τα δύο πρωτόκολλα χρησιμοποιούνται για μεταφορά αρχείων από έναν υπολογιστή σε έναν άλλον.
ii. Και τα δύο πρωτόκολλα για την μεταφορά των αρχείων χρησιμοποιούν παραμένουσες συνδέσεις.
iii. Είναι και τα δύο ακαταστατικά
iv. Και τα δύο πρωτόκολλα απαντάνε με status code και φράσεις
v. Και τα δύο πρωτόκολλα έχουν ASCII text commands.

b. Διαφορές
i. Το HTTP είναι ένα πρωτόκολλο pull. Δηλαδή οι χρήστες χρησιμοποιούν το HTTP για να τραβήξουν τις πληροφορίες από τον σέρβερ. Ενώ το SMTP είναι ένα πρωτόκολλο push. Δηλαδή ο σέρβερ προωθεί το αρχείο στον σέρβερ του παραλήπτη.
ii. Το HTTP ενθυλακώνει κάθε αντικείμενο μέσα στο δικό του μήνυμα απόκρισης HTTP. Ενώ το SMTP τοποθετεί όλα τα αντικείμενα του μηνύματος μέσα σε ένα μήνυμα.

c.



i. Στα 2,4,6 χρησιμοποιούμαι το ίδιο πρωτόκολλο;
1. 2,4 ➔ SMTP (Πάντα τα mails στέλνονται με SMTP)
2. 6 ➔ POP, IMAP ή HTTP. (Μόνο στο κατέβασμα-download έχουμε αυτά τα τρία πρωτόκολλα)
3. Με ένα πρωτόκολλο στέλνουμε και με πολλά διαβάζουμε τα Mails μας.

21. Σύγκριση POP3 – IMAP
a. Στο POP3 γίνεται αποθήκευση των μηνυμάτων σε υπολογιστές ή σε σκληρούς δίσκους. Δηλαδή δεν μπορούμε να διαβάσουμε τα mails μας σε άλλο υπολογιστή διαφορετικού εκείνου που το κατεβάσαμε. Ενώ στο IMAP είναι όλα επάνω στον

mail server και μπορούμε να βλέπουμε τα mails μας σε οποιοδήποτε υπολογιστή.

b. Το POP3 είναι ακαταστατικό ενώ το IMAP καταστατικό
c. Στο POP3 για να κάνεις “download and keep”, αντιγράφει τα μηνύματα σε διαφορετικούς clients.

22. DNS
    a. Τι είναι το DNS και πως λειτουργεί;
        i. Το DNS είναι μία κατανεμημένη βάση δεδομένων η οποία υλοποιείται σε μία ιεραρχία από πολλούς name servers όπου κρατούν την IP και το αντίστοιχο name. Το DNS κάνει μία αντιστοίχηση ανάμεσα στην IP και στο name. Είτε θα δώσεις την IP και θα σου επιστρέψει το name, είτε θα δώσεις το name και θα σου επιστρέψει την IP. Για να μιλήσεις στην βάση και να πάρεις την πληροφορία από τους name servers, απαιτείται ένα πρωτόκολλο. Άρα το DNS αποτελείται από μία κατανεμημένη βάση και ένα πρωτόκολλο 5^{ου} επιπέδου το οποίο επικοινωνούν τα end-devices με τους name servers. Επίσης είναι κατανεμημένη επειδή αν ήταν κεντρικοποιημένη θα ήταν μοναδική με αποτέλεσμα να ήταν δύσκολο να ενημερώνεται και θα δεχόταν περισσότερες επιθέσεις.

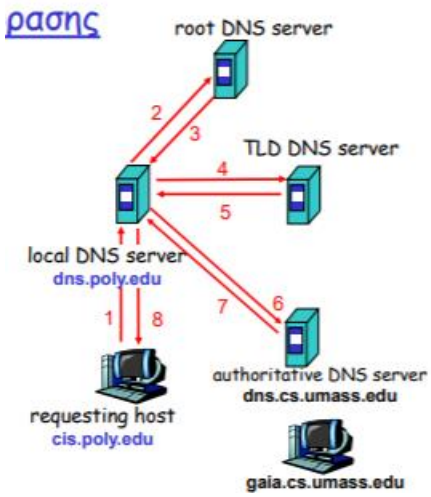
    b. Τι υπηρεσίες προσφέρει εκτός από την μετάφραση IP-NAME, NAME-IP;
        i. Ψευδώνυμα υπολογιστών
            1. Τα ψευδώνυμα υπολογιστών υπάρχουν για να είναι πιο ευκολομνημόνευτα από ένα κανονικό όνομα υπολογιστή.
        ii. Ψευδώνυμα εξυπηρέτη ταχυδρομείου
            1. Τα ψευδώνυμα εξυπηρέτη ταχυδρομείου υπάρχουν για να είναι πιο ευκολομνημόνευτα και για να μπορούν να έχουν πανομοιότυπα ονόματα υπολογιστών.
        iii. Κατανομή φορτίου
            1. Η κατανομή φορτίου ορίζει εξυπηρέτες-αντίγραφα έτσι ώστε οι πελάτες να επικοινωνούν και με τους εξυπηρέτες-αντίγραφα για εξυπηρέτηση. Με αυτό τον τρόπο αποφεύγουν τον φόρτο πάνω στον κεντρικό σέρβερ.

    c. Τι προβλήματα έχει η κεντρικοποιημένη βάση;
        i. Υπάρχει το ρίσκο αν καταρρεύσει ο σερβερ DNS, θα καταρρεύσει και το διαδίκτυο.
        ii. Υπάρχει ο όγκος κίνησης. Ένας μοναδικός εξυπηρέτης DNS δεν θα μπορεί να διαχειριστεί όλα τα ερωτήματα DNS.

iii. Υπάρχει το πρόβλημα της συντήρησης.

d. Ποιες είναι οι κλάσεις των DNS σερβερ;
    i. Εξυπηρέτες Root DNS
        1. Οι εξυπηρέτες Root παρέχουν τις διευθύνσεις IP των εξυπηρετών TLD.
    ii. Εξυπηρέτες τομέα ανωτάτου επιπέδου (TLD)
        1. Οι TLD είναι υπεύθυνοι για τομείς ανωτάτου επιπέδου (com, org, gov, edu) και για όλους τους τομείς ανωτάτου επιπέδου χωρών (gr, du, uk). Οι TLD παρέχουν τις διευθύνσεις IP για αυθεντικούς ξυπηρέτες DNS.
    iii. Αυθεντικοί εξυπηρέτες DNS (Authoritative DNS servers)
        1. Οι εξυπηρέτες DNS του οργανισμού που παρέχουν αυθεντικές αντιστοιχίσεις ονομάτων υπολογιστών σε διευθύνσεις IP για τους εξυπηρέτες του οργανισμού.
e. Πως γίνεται η αίτηση ανάμεσα στις κλάσεις των DNS server;
    i. Ο πελάτης έρχεται αρχικά σε επαφή με έναν root server, ο οποίος επιστρέφει διευθύνσεις για εξυπηρέτη TLD για τον τομέα ανωτάτου επιπέδου com. Ο πελάτης έρχεται κατόποιν σε επαφή με έναν από τους TLD ο οποίος επιστρέφει την IP ενός αυθεντικού εξυπηρέτη για την amazon.com. τέλος ο πελάτης έρχεται σε επαφή με έναν από τους αυθεντικούς εξυπηρέτες για την amazon.com, ο οποίος επιστρέφει την διεύθυνση IP για το όνομα υπολογιστή www.amazon.com.
f. Τι είναι ο local DNS server και γιατί υπάρχει;
    i. Ο local DNS server είναι αυτός που μας δίνεται από τον ISP και δεν είναι μέρος της ιεραρχίας. Όταν κάποιο end-device κάνει ένα DNS Query, το query γίνεται στον local DNS server. Ο local έχει μία cache μνήμη με τις πιο συχνές ερωτοαπαντήσεις σε σχέση name-IP αλλά μπορεί να είναι Out of date γιατί δεν έχει ενημερωθεί.

g.

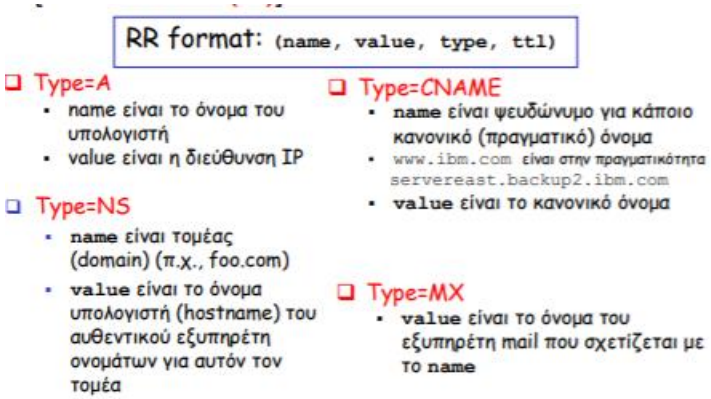


   i. Όλα τα ερωτήματα μπορούν να είναι και επαναληπτικό ή αναδρομικό.
   ii. Αναδρομικό είναι όταν ζητάς από κάποιον να βρει την αντιστοίχιση εκ μέρους του.
   iii. Επαναληπτικό είναι όταν όλες οι αποκρίσεις επιστρέφονται απευθείας σε αυτόν που κάνει την δουλειά της αναδρομής.

h. Τι είναι το DNS caching;
   i. Οποιοσδήποτε name Server μαθαίνει την αντιστοίχιση IP-name, το κάνει caching. Το βάζει στην δικιά του μνήμη για ένα χρονικό διάστημα TTL και όταν περάσει αυτός ο χρόνος η πληροφορία θα διαγραφεί.

i. Σε ποιο πρωτόκολλο δεν υπάρχει caching; Όταν έχουμε push – pull, που έχει caching;
   i. Στο SMTP δεν υπάρχει caching. Στο SMTP φεύγει από εμένα, άρα δεν υπάρχει λόγος να κρατήσω κάτι. Άρα στο PULL πάντα έχουμε cache server, ενώ στο PULL τραβάω δεδομένα για να μην χρειάζεται να τραβάω κάθε λίγο.

j. DNS Records



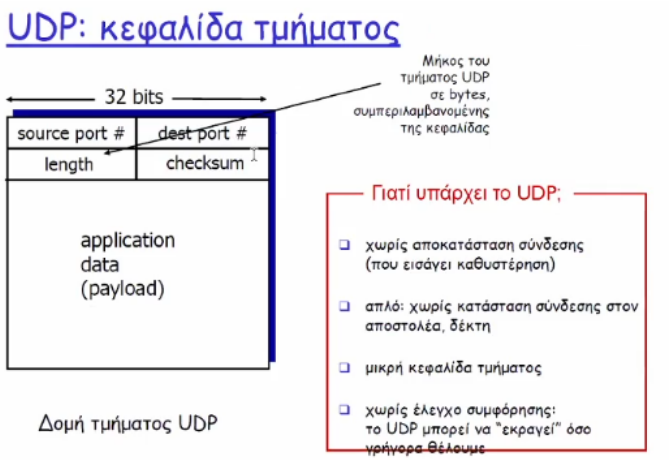
   i.

Chapter 3: Transport Layer

1. Τι παρέχει ένα πρωτόκολλο μεταφοράς;
    a. Υπάρχει μία λογική σύνδεση ανάμεσα στις διεργασίες του 5ου επιπέδου. Ένα πρωτόκολλο μεταφοράς μπορεί να προσφέρει υπηρεσία αξιόπιστης μεταφοράς δεδομένων σε μία εφαρμογή, ακόμη και όταν το υποκείμενο πρωτόκολλο δικτύου είναι αναξιόπιστο, δηλαδή ακόμη και όταν το πρωτόκολλο δικτύου χάνει, μπερδεύει ή δημιουργεί πολλαπλά διπλότυπα πακέτων.
2. Γιατί το TCP θεωρείται αξιόπιστο και το UDP όχι;
    a. Το TCP θεωρείται αξιόπιστο επειδή έχει αξιόπιστη μεταφορά δεδομένων, άρα τα δεδομένα μας δεν πρόκειται να χαθούν στην πορεία. Επίσης παρέχει έλεγχο συμφόρησης ο οποίος είναι πολύ σημαντικός γιατί απαγορεύει να πλημμυρίζει τις ζεύξεις και τους μεταγωγείς ανάμεσα στις επικοινωνούσες οντότητες με υπερβολική ποσότητα κίνησης. Επίσης παρέχει έλεγχο ροής ο οποίος είναι υπεύθυνος στο να μην υπερφορτώνεται ο παραλήπτης με δεδομένα.
3. Τι είναι η πολύπλεξη(multiplexing) και τι η αποπολύπλεξη(demultiplexing); Πως δουλεύουν;
    a. Η εργασία συλογής ομάδων δεδομένων στον υπολογιστή προέλευσης από διαφορετικές sockets, η ενθυλάκωση κάθε ομάδας δεδομένων με πληροφορίες κεφαλίδας για δημιουργία τμημάτων και το πέρασμα των τμημάτων στο επίπεδο δικτύου καλείται πολύπλεξη. Άρα είναι η διαδικασία που βάζεις το σωστό socket από ποια διεργασία ξεκινάς για να στείλεις.
    b. Η εργασία παράδοσης των δεδομένων σε ένα τμήμα επιπέδου μεταφοράς στην σωστή socket καλείται αποπολύπλεξη. Άρα είναι η διαδικασία που πρέπει να δεις ποιο είναι το socket που έχει το πακέτο που έρχεται και να το διανέμεις στο σωστό socket.
    c. Στην αποπολύπλεξη το end-device αφού έχει όλα τα επίπεδα, συνδυάζει την IP-Port number και διανέμει αυτό το τμήμα στο σωστό socket. Άρα παίρνει με βάση το 3ο επίπεδο ποια είναι η IP, ανεβαίνει στο 4ο επίπεδο και βλέπει τον συνδυασμό του IP-Port number όπου έχει ως αποτέλεσμα το socket και ξέρει σε ποιον απευθύνεται.
4. Στο 4ο επίπεδο έχουμε δύο πρωτόκολλα. Γιατί είναι απαραίτητο να έχουμε το UDP αφού δεν είναι αξιόπιστο; Γιατί κάποιος θα πρότεινε να κάνει εφαρμογή με UDP; Θα μπορούσε να παρέχει αξιοπιστία; Πως;
    a. Είναι απαραίτητο να έχουμε UDP γιατί χρησιμοποιείται σε εφαρμογές streaming όπου εκεί μας ενδιαφέρει η συνεχές ροή και όχι τόσο η ασφάλεια, δεν μας ενδιαφέρει και τόσο αν χάσουμε κάποια πακέτα ή αν παραδοθούν εκτός σειράς στις εφαρμογές.
    b. Το UDP μπορεί να προταθεί επειδή είναι πιο γρήγορο λόγο του ότι δεν χρειάζεται χειραψία, επίσης έχει μικρή κεφαλίδα (4bytes) αλλά ολόκληρο είναι 8bytes. Επίσης δεν υπάρχει έλεγχος συμφόρησης άρα παίρνει όλο το bandwidth.

c. Μπορεί να παρέχει αξιόπιστη μεταφορά αλλά αυτό είναι στο χέρι του προγραμματιστή στο 5ο επίπεδο. Το UDP θα κάνει απλά την μεταφορά αλλά δεν θα είναι αξιόπιστη. Ο προγραμματιστής θα πρέπει να προγραμματίσει το πρόγραμμα για την αξιοπιστία και για την επαναμετάδοση.

5. Στο UDP υπάρχει επαναμετάδοση;
   a. Όχι. Αν χαθεί, χάθηκε.

6. 

7. Τι είναι αξιοπιστία και τι προυποθέσεις έχει;
   a. Το 4ο επίπεδο δημιουργεί ένα αξιόπιστο κανάλι έτσι ώστε η διεργασία όπου στέλνει τα δεδομένα προς μία άλλη διεργασία να είναι σίγουρη ότι θα φτάσουν σωστά. Στο αξιόπιστο κανάλι του 4ου επιπέδου δεν αλλοιώνονται τα bytes, δεν καταστρέφονται ή χάνονται και τα πακέτα όταν θα παραδοθούν στην διεργασία του παραλήπτη, παραδίδονται με την σειρά που έχουν σταλεί. Το TCP όμως υλοποιείται επάνω σε ένα αναξιόπιστο επίπεδο δικτύου. Άρα στο αναξιόπιστο μπορούν να αλλοιωθούν, χαθούν και να μην παραδοθούν στην σωστή σειρά τα πακέτα.

8. Σε ποιο άλλο επίπεδο έχουμε έλεγχο για σφάλματα Checksum; Γιατί υπάρχουν και στα δύο επίπεδα έλεγχοι; Υλοποιούνται με τον ίδιο τρόπο και τα δύο;
   a. Έχουμε στο δεύτερο επίπεδο (CRC) το οποίο υλοποιείται με hardware XOR.
9. Στο checksum πέρασε τον έλεγχο του 2ου επιπέδου και είδε ότι δεν έχει λάθη. Αφού δεν έχει λάθη στο 2ο επίπεδο, μπορεί να έχει λάθη στο 4ο επίπεδο;

10. Rdt2.0 ACKs – NAKs
    a. Το υποκείμενο κανάλι δεν χάνει ποτέ δεδομένα ή ACKs αλλά ενδέχεται να αναστρέψει bits τα οποία θα ανιχνευθούν από το checksum.
    b. Ο τρόπος για να διορθώσουμε τα λάθη είναι μέσω των ACKs και NAKs.
       i. Τα ACKs είναι μία απάντηση από τον παραλήπτη προς τον αποστολέα ότι ο παραλήπτης παρέλαβε σωστά το πακέτο και να συνεχίσει για τα επόμενα.

Τα NAKs είναι μία απάντηση από τον παραλήπτη προς τον αποστολέα ότι ο παραλήπτης δεν παρέλαβε ή υπάρχει καποιο σφάλμα με το πακέτο. *Το rdt2.0 παρέχει ανίχνευση λαθών και feedback του παραλήπτη μέσω ACK – NAK.

11. Rdt2.0 Τι συμβαίνει αν καταστραφεί το ACK/NAK;
    a. Αρχικά ο αποστολέας δεν γνωρίζει τι συνέβει στον παραλήπτη. Οι προσεγγίσεις για το τι θα πρέπει να γίνει είναι είτε να προσθέσει αρκετά bit αθροίσματος ελέγχου έτσι ώστε να επιτρέπεται στον αποστολέα όχι μόνο να ανιχνεύει αλλά και να ανακάμπτει από σφάλματα bit, είτε ο αποστολέας να ξανά στείλει το τρέχον πακέτο δεδομένων. Η επαναμετάδοση του πακέτου θα δημιουργήσει το πρόβλημα των διπλότυπων πακέτων. Αυτό λύνεται με την πρόσθεση του πεδίου sequence number το οποίο αριθμεί τα πακέτα που στέλνει ο αποστολέας. Με το sequence number θα μπορεί ο παραλήπτης να ελέγχει αν πρόκειται για επαναμετάδοση ή όχι. Εφόσον υπάρχει το sequence number, ο παραλήπτης σε περίπτωση που του έρθει το ίδιο sequence number θα το κάνει decline.

12. Rdt2.1
    a. Στο rdt2.1 προστέθηκε το sequence number, άρα ξέρουμε τον αριθμό του και το πακέτο. Ο αποστολέας πρέπει να ελέγξει αν το ACK/NAK όπου παρέλαβε είναι κατεστραμένο, άρα πρέπει να υπάρχει checksum για τα data και checksum για τα ACK/NAK. Τέλος η κατάσταση πρέπει να θυμάται αν το αναμενόμενο πακέτο έχει sequence number 0 ή 1.
    b. Ο παραλήπτης πρέπει να ελέγξει αν το λαμβανόμενο πακέτο είναι διπλό μέσω του sequence number. Επίσης δεν μπορεί να γνωρίζει αν το τελευταίο του ACK/NAK έχει ληφθεί σωστά από τον αποστολέα.

13. Rdt2.2
    a. Ένας αποστολέας που δέχεται δύο ACK για το ίδιο πακέτο ξέρει ότι ο παραλήπτης δεν έλαβε σωστά το πακέτο, που ακολουθεί το πακέτο για το οποίο είχε διπλό ACK. Αν ο αποστολέας πάρει ένα διπλότυπο ACK είναι σαν να πήρε NAK από τον παραλήπτη με αποτέλεσμα ο αποστολέας να πρέπει να το ξανά στείλει.
    b. Στο rdt2.2 δεν έχουμε NAK. Ο παραλήπτης στέλνει ACK για το τελευταίο πακέτο που έλαβε σωστά. Ο δέκτης πρέπει να καταλάβει από το sequence number του ACK που θα του έρθει για το ποιο ACK πήρε ο παραλήπτης. Άρα έχοντας ACK για τον αριθμό 0, καταλαβαίνει ότι το 1 δεν παραλήφθηκε σωστά και το ξανά στέλνει.
    c. Διπλότυπα ACKs μπορούν να σταλθούν από τον αποστολέα. Δηλαδή έστειλε το ACK για το 0 και μετά έρχεται ξανά το ACK πάλι για το 0. Αποτέλεσμα της ίδιας ενέργειας όπως ήταν το NAK. Δηλαδή ο αποστολέας ενημερώνει τον παραλήπτη στέλνοντας δεύτερη φορά ACK για το σωστό. Όταν στέλνω δύο φορές ACK για το ίδιο είναι σαν να σου έλεγα ότι δεν πήρα το NAK. Αυτό που θα μου έστελνε ο

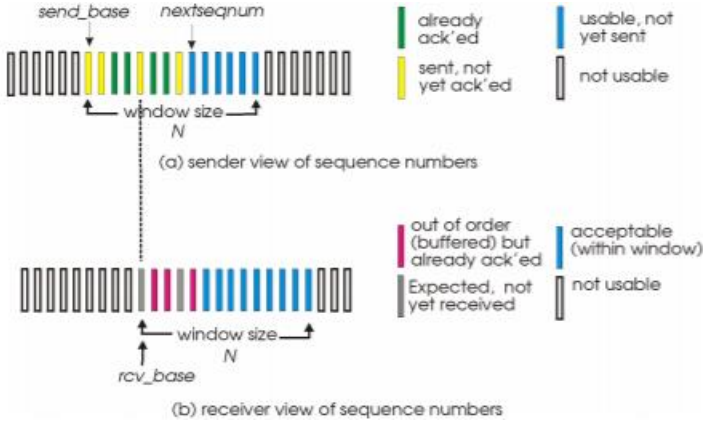
παραλήπτης δεν χρειάζεται γιατί τον ενημερώνω ότι σωστό έχω πάρει μόνο αυτό το 0.

14. Rdt3.0
    a. Ο αποστολέας περιμένει για ένα χρονικό διάστημα για το ACK. Αν δεν ληφθεί ACK σε αυτό το διάστημα τότε αναμεταδίδει. Αν απλά καθυστέρησε τότε οι αναμεταδόσεις θα είναι διπλές (duplicate) αλλά θα αντιμετωπιστεί από το sequence number. Αφού θα χρειαστεί χρονομετρητής για την επαναμετάδοση τότε ο αποστολέας θα πρέπει να εκκινεί τον χρονομετρητή κάθε φορά που στέλνεται ένα πακέτο, να αποκρίνεται σε μία διακοπή χρονομετρητή και να σταματά τον χρονομετρητή.
    b. Πότε γίνεται η αίσθηση ότι χάσαμε ένα πακέτο;
        i. Όταν λάβουμε διπλότυπο ACK ή όταν περάσει ο χρόνος του χρονομετρητή.
    c. Είναι πρωτόκολλο stop-and-wait.
15. Pipelined Protocols
    a. Στα Pipelined Protocols βάζω πολλά πακέτα σε μία διοχέτευση προς επιβεβαίωση. Το εύρος του sequence number πρέπει να αυξηθεί και υπάρχουν buffers στον αποστολέα και στον παραλήπτη.
16. Ποιες είναι οι μορφές πρωτοκόλλων διοχέτευσης;
    a. Go-Back-N
        i. Ο αποστολέας επιτρέπεται να μεταδίδει πολλαπλά πακέτα χωρίς να περιμένει για μία επιβεβαίωση, αλλά περιορίζεται στο να μην έχει περισσότερα από έναν μέγιστο επιτρεπόμενο αριθμό μη επιβεβαιωμένων πακέτων μέσα στην διοχέτευση.
        ii. Ο αποστολέας έχει ένα χρονόμετρο που κρατάει το παλαιότερο πακέτο που δεν έχει επιβεβαιωθεί και αν αργήσει να πάρει ACK τότε είναι υποχρεωμένος να ξανά μεταδώσει όλα τα πακέτα τα οποία δεν έχουν ACK.
        iii. 

        iv. Κάθε φορά που παίρνω τα ACKs για το base και για τα επόμενα, το window προχωράει προς τα δεξιά. Μέσα στο window υπάρχουν και τα πακέτα τα οποία είναι έτοιμα προς αποστολή αλλά δεν τα έχω στείλει. Μετά από το παράθυρο είναι τα πακέτα που δεν είναι έτοιμα προς αποστολή.
        v. Όταν παίρνω ένα ACK για sequence number N, επιβεβαιώνει και όλα τα προηγούμενα ότι είναι ACK. Ενδέχεται ο παραλήπτης να πάρει διπλά ACK.

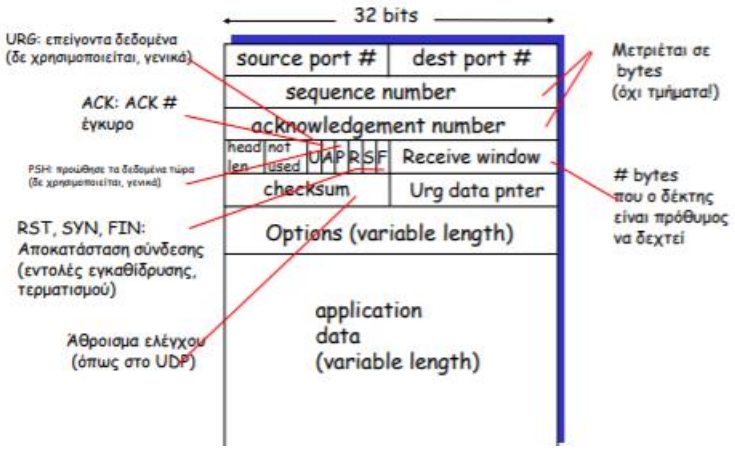
vi. Όταν τελειώσει ο χρονομετρητής, ειδοποιεί την διεργασία και λέει ότι τελείωσε ο χρόνος για το συγκεκριμένο πακέτο N. Άρα με την λήξη του χρόνου αναμεταδίδει το πακέτο N και όλα τα πακέτα με τον υψηλότερο sequence number που υπάρχουν μέσα στο window επειδή δεν τα πήρε.

b. Selective Repeat
   i. Ο παραλήπτης δεν θα κάνει το τελευταίο sequence number ACK αλλά θα επιβεβαιώνει το κάθε ένα ξεχωριστό πακέτο.
   ii. Έχει buffers για να αποθηκεύει τα πακέτα που ήρθαν είτε με την σωστή σειρά, είτε όχι.
   iii. Ο αποστολέας επαναλαμβάνει και στέλνει μόνο τα πακέτα που δεν έγιναν ACK. Άρα δεν έχουμε άσκοπες αναμεταδώσεις.
   iv. Στο παράθυρο του αποστολέα μπορώ να έχω N συνεχόμενα sequence numbers.

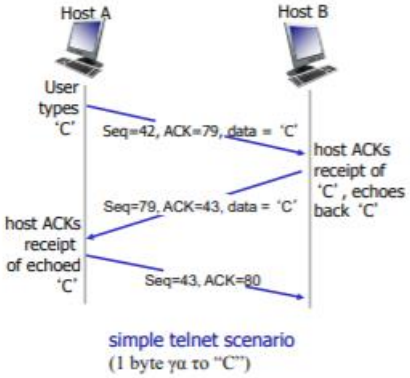


c. Πόσους χρονομετρητές έχει το Go-back-N και πόσους το Selective Repeat;
   i. Το Go-back-N έχει ένα χρονομετρητή ενώ το Selective Repeat έχει ένα χρονομετρητή για το κάθε πακέτο, αφού μόνο ένα πακέτο θα μεταδοθεί κατά την λήξη του χρόνου.

17. TCP
   a. Είναι συνδεσμικό επειδή πρέπει να γίνει πρώτα η τριμερής χειραψία
   b. Η σύνδεση είναι αμφίδρομη. Δηλαδή ο Α και ο Β μπορούν να στέλνουν και να παραλαμβάνουν ταυτόχρονα δεδομένα.
   c. Έχουμε σύνδεση Point-to-Point ανάμεσα σε ένα μόνο αποστολέα και ένα μόνο παραλήπτη.
   d. Τα δεδομένα πάνε με διοχέτευση.
   e. Καθορίζεται ποιο είναι το μέγεθος που μπορώ να στείλω σε κάθε τμήμα μέσω του MSS.
   f. Έχουμε buffers για αποστολή και λήψη.

18. 

    a. Ποια είναι τα κοινά με το UDP;
        i. Source port – Dest port
        ii. Checksum
        iii. Data
    b. Τι είναι το sequence number και τι το acknowledgement number;
        i. Αρχικά και τα δύο μετριούνται σε bytes. Το sequence number δεν είναι ο αύξον αριθμός του τμήματος αλλά είναι ποιο byte είναι η αρχή αυτού του τμήματος που ξεκινάει. Το acknowledgement number είναι ο αριθμός του sequence number για το επόμενο byte που περιμένει από την άλλη πλευρά.



19. Τι είναι το Round Trip Time και το Timeout;
    a. Το RTT είναι ο χρόνος που χρειάζεται το οποιοδήποτε πακέτο για να ταξιδέψει από τον πελάτη προς τον σέρβερ και μετά πάλι πίσω στον πελάτη. Δηλαδή είναι ο χρόνος που μετριέται από την μετάδοση ενός segment, εως την παραλαβή του ACK για το συγκεκριμένο segment. Το timeout είναι ο χρόνος λήξης που σου δίνει ο χρονομετρητής μέχρι να χτυπήσει.
20. Τι θα γίνει αν βάλουμε μικρό RTT και μεγάλο timeout; Τι θα γίνει αν βάλουμε μεγάλο RTT και μικρό timeout;
    a. Αν βάλουμε μικρό RTT και μεγάλο timeout, τότε θα υπάρξουν άσκοπες αναμεταδόσεις.

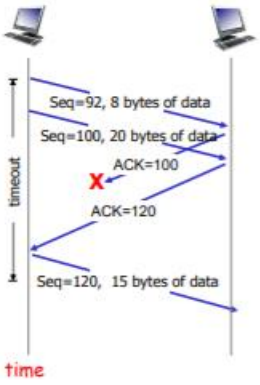
b. Αν βάλουμε μεγάλο RTT και μικρό timeout, τότε θα υπάρχει επίπτωση στην αντίδραση του συστήματος σε περίπτωση που χαθεί κάποιο segment και δεν θα το αναμεταδώσει έγκερα.

21. Αξιόπιστη μεταφορά δεδομένων του TCP
    a. Το TCP δημιουργεί μία υπηρεσία αξιόπιστης μεταφοράς δεδομένων πάνω από την αναξιόπιστη υπηρεσία βέλτιστης πρσπάθειας του IP. Χρησιμοποιεί τμήματα σε διωχέτευση για να τα έχει μαζί και να τα στείλει. Επίσης χρησιμοποιεί σωρευτικά ACKs για να δείχνει για πόσα μαζεμένα δίνει ACKs. Τέλος υπάρχει μόνο ένας χρονομετρητής αναμεταδόσεων για να μην έχει για κάθε τμήμα.
    b. Αρχικά θεωρούμε απλοποιημένο τον αποστολέα του TCP. Δηλαδή αγνοούνται τα διπλότυπα ACKs, αγνοείται ο έλεγχος ροής και ο έλεγχος συμφόρησης.
    c. Πότε γίνεται η αναμετάδοση;
        i. Η αναμετάδοση γίνεται είτε όταν θα έχει λήξει ο χρόνος RTT, είτε υπάρχουν διπλότυπα ACKs.

22. Γεγονότα του αποστολέα TCP
    a. Ο αποστολέας αφού παραλάβει τα δεδομένα από το 5^{ο} επίπεδο, δημιουργεί ένα τμήμα και βάζει και το sequence number. Το sequence number θα είναι ο αριθμός του πρώτου byte των δεδομένων στο τμήμα. Θα εκκινήσει ένα χρονομετρητή και ο χρονομετρητής είναι σαν τον χρονομετρητή του πιο παλιού UNACKed τμήματος.
    b. Στην λήξη του χρόνου θα γίνει αναμετάδοση του τμήματος που προκάλεσαι το timeout και κάνει restart τον timer.
    c. Αν επιβεβαιώνει τμήματα που δεν έχουν ήδη επιβεβαιωθεί τότε ενημερώνει τι είναι ACKed και τι UNACKed.

23. Τι θεωρεί αξιόπιστο το TCP;
    a. Αναλλοίωτο = χωρίς χαμένα bits
    b. Χωρίς κενά = τα στέλνει ταξινομημένα
    c. Χωρίς διπλότυπα ACK = όχι αναμετάδοση
    d. Να χρησιμοποιεί ένα χρονομετρητή

24. Αφού δεν πήρα το ACK 100 και πηρα το ACK 120, θα κάνω αναμετάδοση;



Σενάριο συσσωρευτικού *ACK*

a. Όχι επειδή πήρα ACK για το επόμενο, άρα πάει να πει ότι καλύπτει και όλα τα προηγούμενα.
b. Έστω ότι στέλνει με seq num = X και έχει X bytes. Ποιο θα είναι το ACK που θα πάρει; Ή ποιο θα είναι το επόμενο seq num.
    i. Συνδυασμός seq num + data bytes.

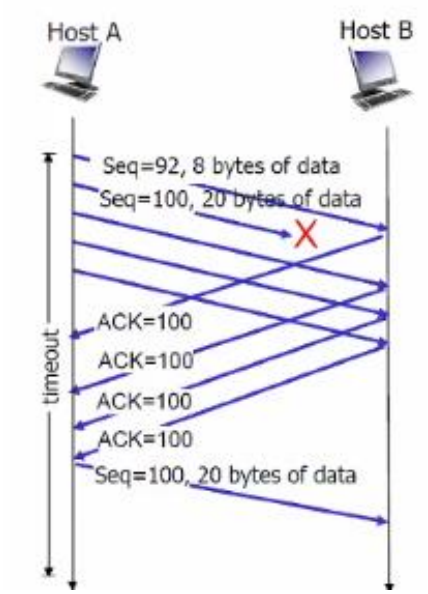
Παραγωγή TCP ACK [RFC 1122, RFC 2581]

Συμβάν στο δέκτη	Ενέργεια δέκτη TCP
Άφιξη τμήματος σε σειρά με αναμενόμενο # ακολουθίας. Όλα τα δεδομένα μέχρι τον αναμενόμενο # ακολουθίας έχουν επιβεβαιωθεί	Καθυστερημένο ACK. Αναμονή 500ms για το επόμενο τμήμα. Αν όχι επόμενο τμήμα στείλε ACK
Άφιξη τμήματος σε σειρά με αναμενόμενο # ακολουθίας. Ένα άλλο τμήμα περιμένει για μετάδοση ACK	Άμεση αποστολή ενός συσσωρευτικού ACK που κάνει επιβεβαίωση και για τα δύο τμήματα που έφτασαν σε σειρά
Άφιξη τμήματος εκτός σειράς με μεγαλύτερο του αναμενόμενου # ακολουθίας. Ανίχνευση κενού	Άμεση αποστολή *duplicate ACK* που δηλώνει # ακολουθίας επόμενου αναμενόμενου byte
Άφιξη τμήματος που μερικώς ή πλήρως συμπληρώνει κενό στα ληφθέντα δεδομένα	Άμεση αποστολή ACK, αρκεί το τμήμα αυτό να αρχίζει στο κάτω άκρο του κενού

25.
    a. Τι συμβαίνει στον δέκτη, τι συμβαίνει στο TCP. Όταν συμβαίνει το X ποια είναι η ενέργεια του δέκτη;

26. Ταχεία αναμετάδοση
    a. Εαν ο αποστολέας TCP δεχθεί τρία διπλότυπα ACK για τα ίδια δεδομένα, εκλαμβάνει αυτή την λήψη ως μία ένδειξη ότι το τμήμα που ακολουθεί εκείνο το τμήμα για το οποίο έχει γίνει επιβεβαίωση τρεις φορές, έχει χαθεί. Άρα στην περίπτωση που ληφθούν τρία διπλότυπα ACK, το TCP κάνει μία ταχεία

επαναμετάδοση, επαναμεταδίδοντας το ελλείπον τμήμα πριν λήξει ο χρονομετρητής αυτού του τμήματος.

b. 

   i. Τι δουλεύει; Go-back-N ή Selective Repeat;
      1. Δουλεύει Selective Repeat επειδή ξέρει ακριβώς ποιο τμήμα θέλει να ξανά στείλει.

27. Έλεγχος ροής του TCP
    a. Το TCP παρέχει μία υπηρεσία ελέγχου ροής στις εφαρμογές του για να εξαλείψει την πιθανότητα να υπερχειλίσει ο αποστολέας τον ενταμιευτή του παραλήπτη. Ο έλεγχος ροής είναι λοιπόν μία υπηρεσία ταιριάσματος ταχυτήτων που ταιριάζει τον ρυθμό αποστολής με τον ρυθμό που η εφαρμογή αντλεί τα δεδομένα.
    b. Ο παραλήπτης κοινοποιεί τον ελεύθερο χώρο του buffer, περιλαμβάνοντας την τιμή του rwnd στην TCP κεφαλίδα.
    c. Ο αποστολέας περιορίζει τα μη επιβεβαιωμένα δεδομένα στην τιμή rwnd του παραλήπτη. Άρα το window που στέλνει ο αποστολέας δεν μπορεί να είναι το δικό του window πιο μεγάλο από το receive window του παραλήπτη.
    d. Στο free buffer space μπαίνουν αυτά που έρχονται από τον αποστολέα και τα buffered data είναι αυτά που είναι ταξινομημένα και έτοιμα να τα πάρει το 5ο επίπεδο. Ο αποστολέας δεν μπορεί να στείλει περισσότερο από ότι χωράει ο buffer.
    e. Το TCP παρέχει έλεγχο ροής κάνοντας τον αποστολέα να διατηρεί μία μεταβλητή που καλείται receive window. Το receive window χρησιμοποιείται για να δίνει στον αποστολέα μία ιδέα για το πόσος ελεύθερος χώρος buffer είναι διαθέσιμος στον παραλήπτη. Επειδή το TCP είναι αμφίδρομο, ο αποστολέας σε κάθε πλευρά της σύνδεσης διατηρεί ένα διακριτό παράθυρο λήψης.

28. Διαχείριση σύνδεσης TCP
    a. Τριμερής χειραψία – Έναρξη σύνδεσης
        i. Βήμα 1
            1. Το TCP στην πλευρά του πελάτη στέλνει πρώτα ένα ειδικό τμήμα TCP στο TCP της πλευράς του εξυπηρέτη. Το ειδικό τμήμα δεν περιέχει δεδομένα 5ου επιπέδου. Ένα από τα bit σημαίας στην κεφαλίδα του τμήματος το SYN BIT τίθεται 1. Αυτό το τμήμα ενθυλακώνεται μέσα σε ένα δεδομενόγραμμα IP και στέλνεται στον εξυπηρέτη.
        ii. Βήμα 2
            1. Μόλις το δεδεμενόγραμμα IP που περιέχει το τμήμα TCP SYN φτάσει στον υπολογηστή εξυπηρέτη, ο εξυπηρέτης εξάγει το τμήμα TCP SYN από το δεδεμενόγραμμα, δεσμεύει τους buffers και τις μεταβλητές TCP στην σύνδεση και στέλνει ένα τμήμα αποδοχής σύνδεσης στον πελάτη TCP. Το τμήμα αποδοχής σύνδεσης ονομάζεται τμήμα SYNACK.
        iii. Βήμα 3
            1. Μετά την λήψη του τμήματος αποδοχής σένδεσης SYNACK, ο πελάτης δεσμεύει επίσης buffers και μεταβλητές στην σύνδεση. Ο υπολογιστής πελάτης κατόπιν στέλνει στον εξυπηρέτη ένα ακόμη τμήμα αυτό το τελευταίο τμήμα επιβεβαιώνει την λήψη του τμήματος αποδοχής σύνδεσης του εξυπηρέτη. Το SYN bit τίθεται σε 0, αφού εγκαθιδρύθηκε η σύνδεση.
    b. Κλείσιμο σύνδεσης
        i. Βήμα 1
            1. Ο πελάτης στέλνει τμήμα ελέγχου του TCP FIN στον εξυπηρέτη.
        ii. Βήμα 2
            1. Ο εξυπηρέτης λαμβάνει FIN, απαντά με ACK, κλείνει την σύνδεση και στέλνει FIN.
        iii. Βήμα 3
            1. Ο πελάτης λαμβάνει FIN, απαντά με ACK.
        iv. Αν είναι παραμένουσα η σύνδεση μπορεί να κάνει close wait ο εξυπηρέτης και να περιμένει. Ενώ αν είναι μη παραμένουσα, κατευθείαν από established, με το που θα ζητήσει ο άλλος να κλέισει δεν θα παει σε close wait αλλά θα πάει απευθείας σε close.
    c. Το rcvBuffer size είναι μέρος της δομής TCP;
        i. Το TCP έχει το rcvWindow. Το rcvBuffer είναι μεταβλητή και δεν έχει κάποια σχέση με τον rcvWindow.

29. Έλεγχος συμφόρησης
    a. Η συμφόρηση δημιουργείται όταν πολλές πηγές στέλνουν πολλά δεδομένα πολύ γρήγορα για να τα χειριστεί το δίκτυο.
    b. Συπτώματα συμφόρησης
        i. Να χαθούν πακέτα επειδή έχω overflow στους buffers των routers.
        ii. Μεγάλες καθυστερήσεις επειδή περιμένουν αρκετή ώρα τα πακέτα στους routers.
30. Ποια είναι η διαφορά ελέγχου ροής με ελέγχου συμφώρησης;
    a. Ο έλεγχος ροής είναι ανάμεσα στην διεργασία πελάτη και στην διεργασία εξυπηρετή που λέει με ποιο ρυθμό μπορώ να διαβάζω από τον receive buffer και πόσο χώρο έχω διαθέσιμο για να ξέρω αν θα σου ζητήσω να στείλεις και άλλα ή όχι. Ο έλεγχος συμφώρησης είναι όταν έχει να κάνει με το πόσο φορτώνουμε το δίκτυο.

31. Έλεγχος συμφόρησης
    a. Στον μηχανισμό συμφόρησης προσθέτουμε ακόμη μία νέα μεταβλητή, το παράθυρο συμφόρησης (cwnd) το οποίο λέει μέχρι πόσα bytes μπορείς να στείλεις μέσα στο δίκτυο.
        i. Ποια είναι η διαφορά του cwnd με το receive window;
            1. Το cwnd είναι μεταβλητή ενώ το receive window είναι ένα πεδίο στην κεφαλίδα του TCP.
    b. Το cwnd θέτει έναν περιορισμό στον ρυθμό με τον οποίο ο αποστολέας TCP μπορεί να στείλει κίνηση μέσα στο δίκτυο. Ο ρυθμός αποστολής του αποστολέα είναι περίπου cwnd/RTT Bytes/sec. Προσαρμόζοντας την τιμή της cwnd, ο αποστολέας μπορεί να ρυθμίσει τον ρυθμό με τον οποίο στέλνει δεδομένα μέσα στην σύνδεση του.
    c. Ανάμεσα στα δύο παράθυρα, ποιο θα χρησιμοποιηθεί;
        i. Θα χρησιμοποιηθεί το μικρότερο από τα δύο. Γιατί μπορούμε να έχουμε ένα cwnd πιο μεγάλο αλλά ο παραλήπτης δεν έχει άλλο χώρο στον δικό του buffer. Αν ο παραλήπτης έχει μεγάλο χώρο, τότεο το cwnd είναι μικρότερο.
    d. Πως αντιλαμβάνεται ο αποστολέας ότι υπάρχει συμφόρηση;
        i. Είτε με την λήξη χρόνου, είτε με τα 3 duplicate ACKs
    e. Πως περιορίζει τον ρυθμό που στέλνει ο αποστολέας;
        i. Περιορίζεται μέσο του cwnd το οποίο θέτει έναν περιορισμό στον ρυθμό με τον οποίο ο αποστολέας TCP μπορεί να στείλει κίνηση μέσα στο δίκτυο. Στέλνει cwnd bytes, περιμένει RTT για ACKs, τότε στέλνει περισσότερα bytes.
32. Έλεγχος συμφόρησης TCP

a. Το TCP χρησιμοποιεί τον έλεγχο για την συμφόρηση μέσω της προσθετικής αύξησης (additive increase) και της πολλαπλασιαστικής μείωσης(multiplicative decrease).
b. Υπάρχει η προσέγγιση αύξηση του ρυθμού μετάδοσης αποστολέα (μέγεθος παραθύρου) και ανίχνευση του χρησιμοποιούμενου εύρους ζώνης. Έτσι ελέγχει κάθε φορά μέχρι να γίνει κάποια απώλεια.
c. Άρα όσο δεν υπάρχει απώλεια, έχουμε την προσθετική αύξηση. Δηλαδή αυξάνεται το cwnd κατά 1 MSS κάθε φορά που συμβαίνει ένα RTT μέχρι να εμφανιστεί απώλεια. Μόλις εμφανιστεί απώλεια, κόβεται το cwnd στο μισό για να αντιμετιπιστεί η συμφώρηση. Η μείωση του cwnd ονομάζεται πολλαπλασιαστική μείωση.

33. TCP Slow Start
    a. Υπάρχουν 3 καταστάσεις
        i. Αργή εκκίνηση
        ii. Αποφυγή συμφόρησης
        iii. Ταχεία ανάκαμψη

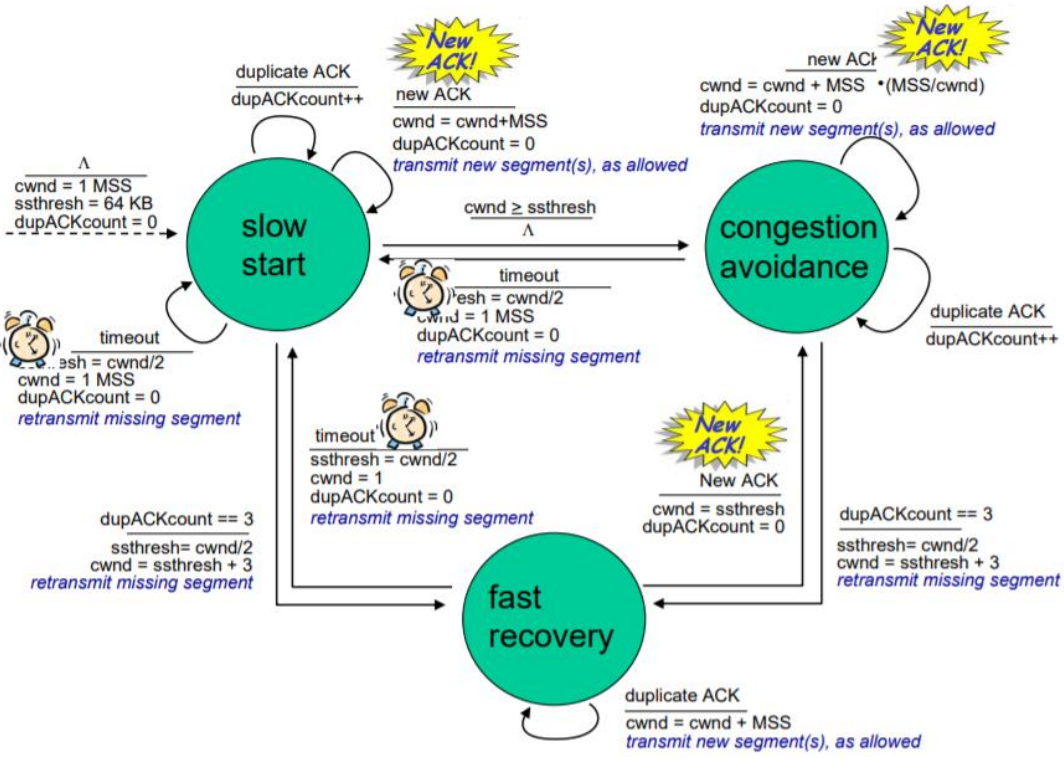
- Όταν ξεκινάει μία σύνδεση TCP, η τιμή της cwnd αρχικοποιείται σε μία μικρή τιμή του 1 MSS. Κατά την κατάσταση αργή εκκίνηση, η τιμή της cwnd αρχίζει στο 1 MSS και αυξάνεται κατά 1 MSS κάθε φορά που ένα μεταδοθέν τμήμα επιβεβαιώνεται.
  Όταν ξεκινά η σύνδεση, CongWin = 1MSS
  ΠΧ MSS = 500Bytes & RTT = 200msec
  Αρχικός ρυθμός = 20kbps
  (500bytes*8bits/byte*1/0/2sec) ****** Για να βρούμε τον ρυθμό. MSS/RTT

    b. Πότε τελειώνει αυτή η εκθετική αύξηση;
        i. Εαν υπάρξει ένα συμβάν απώλειας λόγο του timeout, ο αποστολέας TCP θέτει την τιμή της cwnd σε 1 και αρχίζει την διεργασία αργής εκκίνησης εκ νέου. Επίσης θέτει την τιμή μίας δεύτερης μεταβλητής κατάστασης ssthresh σε cwnd/2 όπου είναι το μισό της τιμής του παραθύρου συμφόρησης. Αφού φτάσει το ssthresh, αυξάνεται γραμμικά και όχι εκθετικά.
        ii. Εαν ανιχνευθούν τρία διπλότυπα ACK, οπότε το TCP εκτελεί μία ταχεία επαναμετάδοση. Αφού ανιχνευθούν τρία διπλότυπα ACK και όχι timeout, πάει να πει ότι το δίκτυο αντέχει. Αφού συμβεί το πρόβλημα, το cwnd μειώνεται στο μισό παράθυρο από ότι ήταν και αυξάνεται γραμμικά στην έκδοση TCP Reno, ενώ στην έκδοση TCP Tahoe κατεβάζει το cwnd στο 1 MSS (είτε συμβαίνει timeout, είτε 3 duplicate ACK).
        iii. Εαν η τιμή της cwnd ισούται με ssthresh, η αργή εκκίνηση τελειώνει και το TCP αλλάζει από αργή εκκίνηση σε αποφυγή συμφόρησης.
        iv. Παράδειγμα
            1. Την χρονική στιγμή 1 ξεκινάμε με 1MSS. Εφόσον παίρνουμε RTT, γίνεται 2, 4, 8 και μετά θα έπρεπε να γίνει 16 αλλά στην χρονική

στιγμή 4, συνέβη κάποιο είδους απώλεια. Αυτό έχει ως αποτέλεσμα να φτάσει στο ssthresh και μετά αρχίζει και αυξάνεται κατά 1 MSS. Από 0-4 έχουμε την κατάσταση αργή εκκίνηση και όταν αρχίσει να ανεβαίνει γραμμικά κατα 1 τότε μπαίνουμε στην επόμενη κατάσταση αποφυγή συμφόρησης.

2. Στην απώλεια με TCP Tahoe, ξανά γυρνάει στο 1MSS και ξεκινάει αργή εκκίνηση.
3. Στην απώλεια με TCP Reno, βλέπει ποιο ήταν το όριο και ξανά γυρνάει στο ½ του ορίου και συνεχίζει γραμμικά. *Στο timeout και οι δύο εκδοχές ξανά γυρνάνε στο 1 MSS. Μόνο στα 3 διπλότυπα ACKs υπάρχει διαφορά.

c. Πότε γίνεται η αλλαγή από εκθετική σε γραμμική αύξηση;
   i. Αφού το παράθυρο συμφώρησης φτάσει το ssthresh, αυξάνεται γραμμικά και όχι εκθετικά.



34.

a. Είμαστε σε κατάσταση fast recovery και γίνεται timeout. Σε ποια κατάσταση θα παω;
   i. Στο slow start
b. Είμαστε σε κατάσταση fast recovery και παίρνω ACK. Σε ποια κατάσταση θα παω;
   i. Στο congestion avoidance

35. Ποια είναι η σύκγριση ανάμεσα στην ταχεία ανάκαμψη και στην ταχεία αναμετάδοση; Ομοιότητες και διαφορές.

a. Είναι δύο εντελώς διαφορετικά πράγματα. Η ταχεία ανάκαμψη έχει να κάνει με το cwnd. Η ταχεία ανάκαμψη για κάθε διπλότυπο ACK που λαμβάνεται για το ελλειπόν τμήμα αυξάνει το cwnd. Η ταχεία αναμετάδοση έχει να κάνει με την επαναμετάδοση των χαμένων πακέτων σε περίπτωση που πάρει 3 διπλότυπα ACKs. Στην περίπτωση των 3 διπλοτύπων ACKs, πρέπει να επαναμεταδόσει το ελλειπόν τμήμα πριν λήξει ο χρονομετρητής του τμήματος.

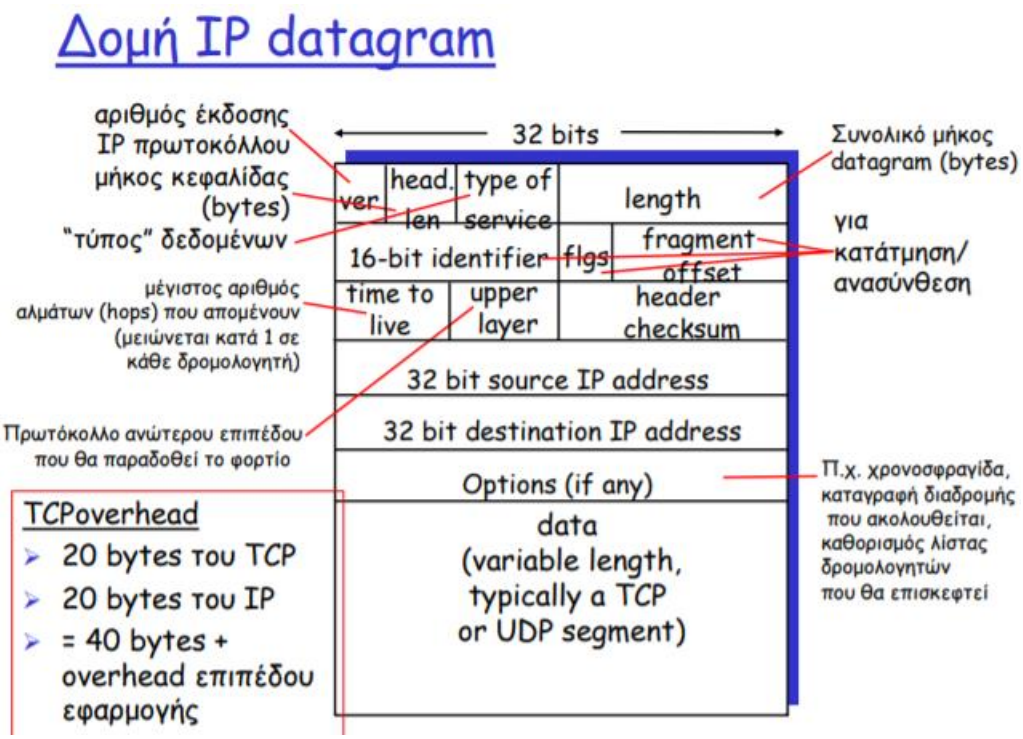
36. Σύνοψη: Έλεγχος συμφόρησης του TCP
    a. Είναι διαφορετικό το Window receiver από το Congestion Window. Το window receiver είναι πεδίο μέσα στην κεφαλίδα του TCP που λέει πόσα είναι τα ελεύθερα byte στον buffer. Το congestion window είναι μεταβλητή.

37.

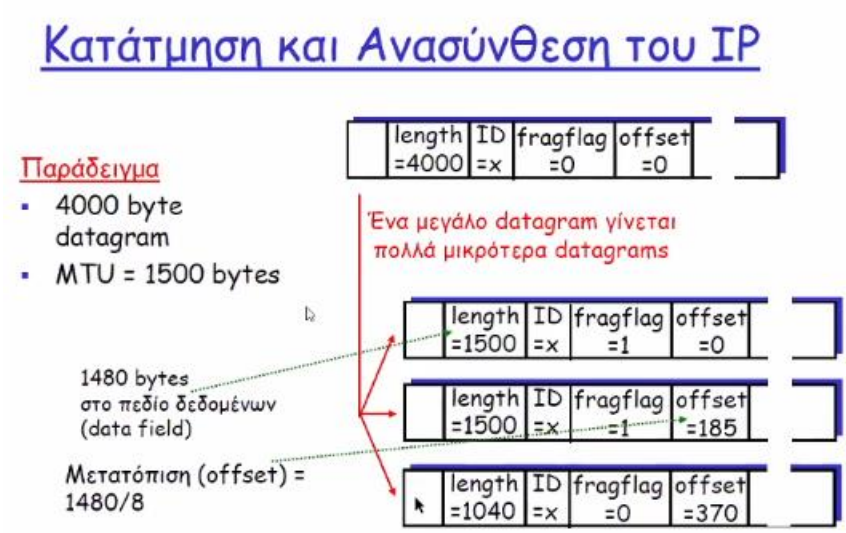
Κατάσταση	Συμβάν	Ενέργεια αποστολέα TCP	Σχόλια
Αργή Εκκίνηση Slow Start (SS)	Λήψη ACK για δεδομένα που δεν έχουν επιβεβαιωθεί προηγουμένως	CongWin = CongWin + MSS, If (CongWin > Threshold) θέσε κατάσταση σε «Αποφυγή Συμφόρησης»	Έχει ως αποτέλεσμα διπλασιασμό του CongWin σε κάθε RTT
Αποφυγή Συμφόρησης Congestion Avoidance (CA)	Λήψη ACK για δεδομένα που δεν έχουν επιβεβαιωθεί προηγουμένως	CongWin = CongWin+MSS * (MSS/CongWin)	Προσθετική αύξηση που έχει ως αποτέλεσμα αύξηση του CongWin κατά 1 MSS σε κάθε RTT
SS ή CA	Ανίχνευση συμβάντος απωλειας από τρία διπλότυπα ACK	Threshold = CongWin/2, CongWin = Threshold, θέσε κατάσταση σε «Αποφυγή Συμφόρησης»	Ταχεία επαναφορά, υλοποιώντας πολλαπλασιαστική μείωση. Το CongWin δεν θα πέσει κάτω από1 MSS.
SS ή CA	Λήξη χρόνου (Timeout)	Threshold = CongWin/2, CongWin = 1 MSS, Θέσε κατάσταση σε «Αργή Εκκίνηση»	Είσοδος σε «Αργή Εκκίνηση»
SS ή CA	Διπλότυπο ACK	Αύξηση του μετρητή διπλότυπων ACK για το τμήμα η λήψη του οποίου επιβεβαιώθηκε	Τα CongWin και Threshold δεν αλλάζουν

Chapter 4: The Network Layer: Data Plane

1. Τι είναι προώθηση και τι είναι δρομολόγηση;
    a. Προώθηση είναι η μετακίνηση των πακέτων από την είσοδο του δρομολογητή στην κατάλληλη έξοδο του δρομολογητή.
    b. Δρομολόγηση είναι ο καθορισμός διαδρομής που ακολουθούν τα πακέτα από την προέλευση στον προορισμό.
2. Τι συμβαίνει στα ξεχωριστά datagrams και τι στην ροή datagrams;
    a. Στα ξεχωριστά datagrams υπάρχει εγγυημένη παράδοση με καθυστέρηση μικρότερη από 40 msec.
    b. Στην ροή datagrams υπάρχει σε σειρά παράδοση των datagrams. Επίσης είναι εγγυημένο το ελάχιστο εύρος ζώνης στην ροή και υπάρχουν περιορισμοί στις αλλαγές των αποστάσεων των πακέτων.

3. 

   a. Ποια πεδία του IP εξετάζονται για να δούμε αν τα πακέτα είναι τμήματα του ίδιου datagram;
      i. Αν έχουν το ίδιο 16-bit identifier, σημαίνει ότι έχουμε τμήματα του ίδιου μεγαλύτερου datagram. Από εκεί και ύστερα κοιτάζει τα flags και το fragment offset.
4. Κατάτμηση



   a.
      i. Το 1040 από που βγήκε και γιατί 1500;
         1. Τα καθαρά data είναι length value – 40 bytes(20IP+20TCP Ή 20IP + 8 UDP)
      ii. Τι είναι το fragflag και τι το offset

1. Το fragflag αποδικνύει αν το δεδεμενόγραμμα είναι μέρος ενός τμήματος ή όχι.
2. Το offset είναι η μετατόπιση.

b. Γιατί συμβαίνει η κατάτμηση;
   i. Ο λόγος που συμβαίνει η κατάτμηση είναι επειδή δεν ξέρουμε με τι σύνδεση συνδέεται ο κάθε router με τον άλλον. Άρα όταν θα φτάσει σε κάποιο router ένα μεγάλο IP datagram το οποίο δεν μπορεί να περάσει από την συγκεκριμένη ζεύξη, ο ίδιος ο router λέει ότι η ζεύξη για να συνδεθώ με τον άλλον είναι πιο μικρή και έχω τον περιορισμό. Αυτό τον αναγκάζει να κόψει το αρχικό μεγάλο datagram που είχε σε μικρότερα πακέτα για να χωρέσει λόγο του περιορισμού που υπάρχει. Η ανασύνθεση των δεδεμενογραμμάτων γίνεται στον τελευταίο δρομολογητή.

5. DHCP
   a. Το πρωτόκολλο DHCP επιτρέπει σε έναν υπολογιστή να αποκ΄τα μία προσωρινή διεύθυνση IP αυτόματα που θα είναι διαφορετική κάθε φορά που ο υπολογιστής συνδέεται στο δίκτυο.
   b. Λόγω της δυνατότητας του DHCP να αυτοματοποιεί τις εργασίες που σχετίζονται με το δίκτυο για σύνδεση ενός υπολογιστή μέσα σε ένα δίκτυο, το πρωτόκολλο αυτό συχνά αναφέρεται ως plug-and-play.
   c. Το DHCP είναι ένα πρωτόκολλο client-server. Ένας πελάτης είναι συνήθως ένας νέος υπολογιστή που θέλει να πάρει πληροφορίες δικτύου. Κάθε υποδίκτυο έχει έναν εξυπηρέτη DHCP. Εαν δεν έχει τότε απαιτείται ένας πράκτορας αναμετάδοσης DHCP (συνήθως ένας δρομολογητής), που να γνωρίζει την διεύθυνση ενός εξυπηρέτη DHCP για το δίκτυο.
   d. Επισκόπηση DHCP
      i. DHCP discover ➔ Ο υπολογιστής εκπέμπει ένα πακέτο UDP το οποίο είναι ενθυλακομένο σε ένα IP δεδεμενόγραμμα και ψάχνει να βρει έναν εξυπηρέτη DHCP. (Έρχεται από το $5^{ο}$ επίπεδο).
      ii. DHCP offer ➔ Ο εξυπηρέτης DHCP αποκρίνεται στον πελάτη.
      iii. DHCP request ➔ Ο υπολογιστής ζητά διεύθυνση IP.
      iv. DHCP ack ➔ Ο εξυπηρέτης DHCP στέλνει την διεύθυνση.

6. NAT
   a. Πως γίνεται η μετάφραση διευθύνσεων δικτύου;
      i. Όλα τα πακέτα που φεύγουν από το τοπικό δίκτυο, θα έχουν την διεύθυνση IP που έχει ο local router προς τον έξω κόσμο. Άρα δεν ξέρουν ποιος υπολογιστής το έστειλε, αλλά ξέρουν από ποιο router. Αυτό που είναι διαφορετικό είναι οι αριθμοί θύρας προέλευσης.
   b. Το τοπικό δίκτυο χρησιμοποιεί μόνο μία IP όσον αφορά τον εξωτερικό κόσμο. Με την χρησιμοποίηση του NAT μπορώ να μην ξοδεύω πολλές πραγματικές IPv4 διευθύνσεις. Άρα
      i. Δεν απαιτείται σύνολο διευθύνσεων από τον ISP, άρα παίρνω λιγότερες.

ii. Μπορούν να ανακτούν οι διευθύνσεις των συσκευών στο τοπικό δίκτυο χωρίς να ειδοποιηθεί ο έξω κόσμος.
iii. Μπορεί να αλλάξει ο ISP χωρίς να αλλάξουν οι IP στο τοπικό δίκτυο.
iv. Μία συσκευή εντός του τοπικού δικτύου δεν είναι ορατή από τον έξω κόσμο ως διευθυνσιοδοτημένη.

c. Πως γίνεται η υλοποίηση μέσω NAT.
i. Στα εξερχόμενα datagrams όταν φεύγουν προς τα έξω και να αλλάζει η source IP σε NAT IP και το port number σε new port number που εμείς θέλουμε. Οι πελάτες θα απαντήσουν μετα καινούργια NAT και Port.

d. Όταν γυρίσει πίσω το θυμάται μέσω του NAT translation table όπου αποθηκεύεται η κάθε IP:PORT του local network με το αντίστοιχο NAT IP:PORT που του δώθηκε.

e. Τα εισερχόμενα datagrams κάνουν αντικατάσταση NAT IP:PORT στα πεδία προωρισμού κάθε εισερχόμενου datagram. Σε αυτή την περίπτωση αλλάζει το destination αφού παραλαμβάνουμε.

7. ICMP
a. Το ICMP είναι 3^{ου} επιπέδου και χρησιμοποιείται από υπολογιστές και δρομολογητές για ανταλλαγή πληροφορίας 3^{ου} επιπέδου. Με αυτό τον τρόπο ελέγχουμε λάθη, σφάλματα και Pings.

b. Τα ICMP messages είναι πάνω από το IP. Δηλαδή τα μηνύματα είναι σαν data που βάζω κεφαλίδα IP. Άρα το ICMP είναι τα data του 3^{ου} επιπέδου και βάζει μπροστά την κεφαλίδα του IP πρωτοκόλλου.

c. Κριτήριο λήξης
i. Το τμήμα UDP τελικά φτάνει στον υπολογιστή προορισμό. Ο προορισμός επιστρέφει πακέτο ICMP και όταν η προέλευση παίρνει αυτό το πακέτο ICMP, σταματά.

Chapter 6: The Link Layer and LANs

1. Διευθυνσιοδότηση
a. Διευθυνσιοδότηση έχουμε μόνο στο 3^{ο} και 2^{ο} επίπεδο. Στο 4^{ο} δεν έχουμε διευθυνσιοδότηση αλλά έχουμε τον αριθμό θύρας όπου με τον συνδυασμό των IP, βγάζουν τα sockets.

2. Που υλοποιείται το επίπεδο ζεύξης;
a. Το επίπεδο ζεύξης υλοποιείται σε κάθε συσκευή με την βοήθεια της κάρτας δικτύου(NIC). Μέσα στο NIC βρίσκεται ο ελεγκτής επιπέδου δικτύου που συνήθως είναι ένα μοναδικό τσιπ πυ υλοποιεί πολλές από τις υπηρεσίες επιπέδου δικτύωσης (πλαισίωση, προσπέλαση ζεύξης, ανίχνευση σφάλματος). Είναι ο συνδυασμός hardware, software και firmware. Το firmware είναι ο driver της NIC.

3. Ποια είναι η λειτουργία του επιπέδου ζεύξης;

a. Το επίπεδο ζεύξης δεδομένων έχει την ευθύνη μεταφοράς των datagrams από ένα κόμβο σε φυσικό γειτονικό κόμβο πάνω από μία ζεύξη.

4. Τι υπηρεσίες παρέχει το επίπεδο ζεύξης;
    a. Πλαισίωση
        i. Τα πρωτόκολλα επιπέδου ζεύξης ενθυλακώνουν κάθε δεδομενόγραμμα επιπέδου δικτύου μέσα σε ένα πλαίσιο επιπέδου ζεύξης πριν το μεταδώσουν μέσω της ζεύξης. Ένα πλαίσιο αποτελείται από ένα πεδίο δεδομένων, μέσα στο οποίο εισάγεται το δεδομενόγραμμα επιπέδου δικτύου, μία κεφαλίδα και μία ουρά. Χρησιμοποιούνται MAC Addresses και μπαίνουν στις κεφαλίδες για να καθορίσουμε ποια είναι η πηγή και ποιος ο προορισμός.
    b. Αξιόπιστη παράδοση
        i. Εγγυάται την μετακίνηση κάθε δεδομενογράμματος επιπέδου δικτύου στην ζεύξη χωρίς σφάλματα.
        ii. Στις ασύρματες ζεύξεις έχουμε υψηλούς ρυθμούς σφαλμάτων.
    c. Ανίχνευση σφαλμάτων
        i. Ο δέκτης ανιχνεύει το σφάλμα και είτε ειδοποιεί τον αποστολλεα για αναμετάδωση, είτε απορρίπτει το πλαίσιο. Η ανίχνευση σφάλματος υλοποιείται σε υλικό.
    d. Διόρθωση σφαλμάτων
        i. Ο δέκτης αναγνωρίζει και διορθώνει σφάλματα bit χωρίς να καταφεύγει στην αναμετάδοση. Αυτό γίνεται με το να κάνουμε τον μεταδίδοντα κόμβο να συμπεριλάβει bits ανίχνευσης στο πλαίσιο και τον παραλαμβάνοντα κόμβο να εκτελεί έλεγχο σφάλματος.
    e. Ημι-αμφίδρομη (Half-duplex) και αμφίδρομη (Full-duplex)
        i. Με half-duplex και οι δύο κόμβοι μπορούν να μεταδόσουν αλλά όχι ταυτόχρονα. (Ασύρματοι).
        ii. Με full-duplex και οι δύο κόμβοι μπορούν να μεταδόσουν ταυτόχρονα.
5. Ανίχνευση σφαλμάτων
    a. Στην ανίχνευση σφαλμάτων βάζουμε περισσότερα bits στο ήδη υπάρχων datagram για να μπορούμε να είμαστε σίγουροι ότι δεν υπάρχουν σφάλματα. Τα δεδομένα που προστατεύονται από τον έλεγχο σφαλμάτων ενδέχεται να περιλαμβάνουν πεδία της κεφαλίδας. Λέγονται D.
    Η ανίχνευση σφαλμάτων δεν είναι 100% αξιόπιστη αλλά όσο μεγαλύτερο είναι το EDC(Error detection and correction bits), τόσο πιο σίγουροι είμαστε ότι τα δεδομένα προστατεύονται. Μεγαλύτερο EDC = Μεγαλύτερη καθυστέρηση.
    b. Στον παραλήπτη ελέγχονται τα D’ και EDC’ με την βοήθεια του controller της NIC και αν είναι όλα εντάξει τότε το ανεβάζει στο 3^{ο} επίπεδο, αλλιώς έχουμε error.
    c. Το checksum του 2^{ου} επιπέδου υλοποιείται μόνο σε software και ελέγχει τα data και την κεφαλίδα που κουβαλάει. Το checksum του 4^{ου} ελέγχει μόνο τα data, του 3^{ου} μόνο την κεφαλίδα και του 2^{ου} και τα δύο.
6. Τι είναι το CRC;

a. Το CRC χρησιμοποιείται στο 2^{ο} επίπεδο, είναι μέθοδος ανίχνευσης σφαλμάτων και υλοποιείται πάντοτε με κύκλωμα (hardware).

7. Πρωτόκολλα και ζεύξεις πολλαπλής πρόσβασης
    a. Point-to-point (Unicast)
    b. Broadcast (καλώδιο ή μέσο κοινής χρήσης όπως ο αέρας)

8. Πρωτόκολλα πολλαπλής πρόσβασης
    a. Αφού οι κόμβοι μεταδίδουν ταυτόχρονα, υπάρχει περίπτωση ο κόμβος να λάβει δύο ή περισσότερα σήματα ταυτόχρονα με αποτέλεσμα να δημιουργηθεί σύγκρουση και τα πλαίσια χάνονται.
    b. Η σύγκρουση αντιμετοπίζεται με το να υπάρχει ένας κατανεμημένος αλγόριθμος που θα καθορίζει πως οι κόμβοι μοιράζονται το κανάλι, άρα καθορίζει πότε ο κόμβος θα μεταδώσει. Επίσης η επικοινωνία για την κοινή χρήση του καναλιού πρέπει να χρησιμοποιήσει το ίδιο κανάλι. Δεν υπάρχει εκτός ζώνης κανάλι για συντονισμό.
9. Γιατί θέλουμε να είναι απλό το πρωτόκολλο;
    a. Γιατί το έχουμε να υλοποιείται κυκλωματικά. Με hardware. Αν ήταν περίπλοκο θα έπρεπε να χρησιμοποιήσουμε software με αποτέλεσμα να είναι αργό.

10. MAC Protocols
    a. Αυτά τα πρωτόκολλα ταξινομούνται σε 3 κλάσεις
        i. Διαμέριση καναλιού
            1. Διαιρούμε το κανάλι σε μικρότερα κομμάτια που λέγονται χρονοθυρίδες ή συχνότητα ή κώδικας. Αυτό το κομμάτι το δίνουμε σε κάθε κόμβο για αποκλειστική χρήση.
        ii. Τυχαία πρόσβαση
            1. Το κανάλι δεν διαιρείται αλλά επιτρέπονται οι συγκρούσεις
        iii. Εκ περιτροπής λειτουργία
            1. Οι κόμβοι να μεταδίδουν με την σειρά αλλά οι μεταδόσεις των κόμβων που έχουν να στείλουν περισσότερα, μπορεί να διαρκέσουν περισσότερο.
    b. Τι είναι το TDMA και τι το FDMA
        i. Το TDMA διαιρεί τον χρόνο σε πλαίσια χρόνου και διαρεί κάθε χρονικό πλαίσιο σε N χρονοθυρίδες. Κάθε χρονοθυρίδα εκχωρείται κατόπιν σε κάθε έναν από τους N κόμβους.
        ii. Το FDMA διαιρεί το κανάλι σε διαφορετικές συχνότητες και εκχωρεί μία συχνότητα σε κάθε ένα από τους N κόμβους.
        iii. Και τα δύο αποφεύγουν τις συγκρούσεις, διαιρούν το εύρος ζώνης δίκαια ανάμεσα στους N κόμβους. Και τα δύο περιορίζονται σε ένα εύρος ζώνης.

11. Τι είναι το CSMA και CSMA/CD και τι κανόνες χρησιμοποιεί;
    a. Το CSMA είναι ένα πρωτόκολλο πολλαπλής προσπέλασης με ανίχνευση φέροντος και το CSMA/CD είναι ένα πρωτόκολλο με ανίχνευση σύγκρουσης. Χρησιμοποιούν τους κανόνες ανίχνευση φέροντος και ανίχνευση σύγκρουσης.
    b. Στο CSMA αν το κανάλι ανιχνευτεί ανενεργό, μεταδίδει ολόκληρο το πλαίσιο αλλά αν ανιχνευτεί απασχολημένο τότε αναβάλει την μετάδοση και περιμένει.
    c. Στο CSMA/CD για να γίνει η αποφυγή της σύγκρουσης, κάνουμε αναβολή μετάδοσης και ανίχνευση σύγκρουσης.
    d. Η ανίχνευση φέροντος είναι περίμενε μέχρι να τελειώσει. Δηλαδή ένας κόμβος κάνει ακρόαση στο κανάλι πριν μεταδώσει. Εάν ένα πλαίσιο από έναν άλλο κόμβο μεταδίδεται αυτήν την στιγμή μέσα στο κανάλι, τότε ο κόμβος περιμένει μέχρι να ανιχνεύσει ότι δεν υπάρχει μετάδοση για ένα μικρό χρονικό διάστημα και μετά αρχίζει την μετάδοση.
    e. Η ανίχνευση σύγκρουσης είναι εάν κάποιος άλλος αρχίσει να μιλά ταυτόχρονα, σταμάτα να μιλάς. Δηλαδή ένας κόμβος που μεταδίδει κάνει ακρόαση στο κανάλι ενώ μεταδίδει. Εάν ανιχνεύσει ότι ένας άλλος κόμβος μεταδίδει ένα πλαίσιο και κάνει παρεμβολές, τότε σταματά να μεταδίδει και περιμένει ένα τυχαίο χρονικό διάστημα πριν να επαναλάβει τον κύκλο ανίχνευσης και μετάδοσης όταν το κανάλι είναι αδρανές.

12. Ethernet CSMA/CD αλγόριθμος
    a. Αφού διακόψει ο controller, μπαίνει σε μία δυαδική εκθετική οπισθοχώρηση. Μετά την m-οστή σύγκρουση, η κάρτα δικτύου (NIC) επιλέγει ένα τυχαίο K στο διάστημα {0,1,2,...2m-1}. Περιμένει για κ*512 bit χρόνους και επιστρέφει στο βήμα 2(ανίχνευση φέροντος). Μεγαλύτερο διάστημα οπισθοχώρησης με περισσότερες συγκρούσεις.
    b. Ο αλγόριθμος υλοποιείται κυκλωματικά.

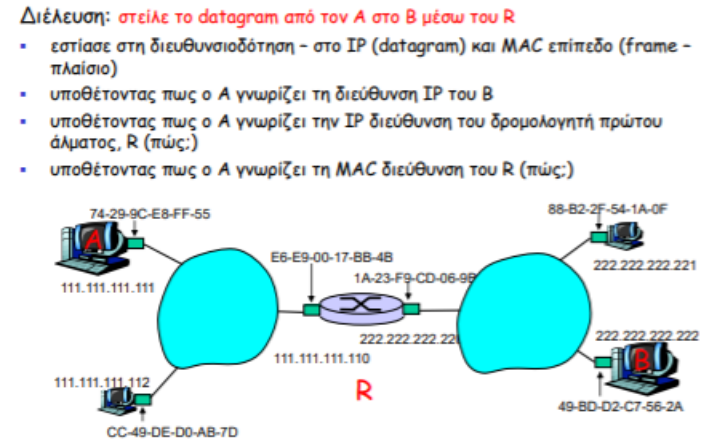
13. MAC Addresses και ARP
    a. Γιατί υπάρχουν δύο είδη διευθυνσιοδότησης;
        i. Χρειαζόμαστε δύο είδη γιατί το ARP είναι σε software ενώ οι MAC σε hardware-NIC.
    b. Διαφορά MAC address – IP address
        i. Οι MAC addresses επειδή είναι στο hardware είναι μεταφέρσιμες. Δηλαδή μπορούμε να συνδεόμαστε σε διαφορετικά δίκτυα, ενώ η IP δεν είναι μεταφέρσιμη. Η IP κρέμμεται από τον ISP και όταν δουλεύουμε με DHCP μας δίνει ο ISP τις διευθύνσεις.
    c. Τι είναι η MAC και τι η ARP;
        i. Η MAC χρησιμοποιείται τοπικά για να πάρει ένα πλαίσιο από την μία διεπαφή μίας NIC για να το πάει σε μία άλλη φυσικά συνδεδεμένη διεπαφή μέσα στο ίδιο δίκτυο.

ii. Η ARP παρέχει ένα μηχανισμό για μετάφραση IP addresses σε MAC addresses.

14. ARP – LAN
    a. Τι μαθαίνουμε μέσω του ARP;
        i. Το ARP πατάει και σε 3ο και σε 2ο επίπεδο. Δεν είναι ξεκάθαρα του 2ου επιπέδου επειδή παίρνει πληροφορίες και από τα δύο επίπεδα για να κάνει την μετάφραση από IP σε MAC. Άρα μέσω του ARP μαθαίνουμε ποια είναι η MAC ποιας IP.
    b. Πως μαθαίνουμε την MAC διεύθυνση του άλλου;
        i. Κάθε υπολογιστής και δρομολογητής έχει ένα πίνακα ARP μέσα στην μνήμη του, που περιέχει αντιστοιχίσεις IP – MAC. Ο πίνακας ARP περιέχει επίσης μία τιμή TTL που υποδηλώνει πότε θα διαγραφεί η κάθε αντιστοίχιση από τον πίνακα.
        ii. Εάν ο πίνακας δεν έχει μία αντιστοίχιση που χρειάζεται τοτε ο αποστολέας χρησιμοποιεί το πρωτόκολλο ARP για να ανάγει την διεύθυνση. Πρώτα ο αποστολέας δημιουργεί ένα ειδικό πακέτο ARP το οποίο έχει τις διευθύνσεις αποστολής και λήψης IP και MAC το οποίο το κάνει broadcast στην MAC FF-FF-FF-FF-FF-FF. Με την MAC FF-FF-FF-FF-FF-FF όλοι οι κόμβοι του LAN θα πάρουν αυτό το ARP ερώτημα.
        iii. Ο Β θα ανοίξει το ARP πακέτο και αφού το ανοίξει θα δει ότι η IP ταιριάζει με την δική του και απαντάει πίσω στον αποστολέα με την δικιά του MAC. Άρα έχουμε unicast.
        iv. Αφού ο αποστολέας πάρει την απάντηση του Β, καταχωρεί το ζεύγος του στον ARP πίνακα.

15. Σύκγριση ARP – DNS
    a. Αντιστοίχηση δεν κάνει το DNS όπως και το ARP;
        i. Όπως και το DNS ψάχνει μία IP ενός συγκεκριμένου server, έτσι αντίστοιχα και το ARP ψάχνει μία συγκεκριμένη IP που αντιστοιχεί σε μία συγκεκριμένη MAC. Η διαφορά ανάμεσα τους είναι ότι το ARP ανάγει διευθύνσεις μόνο για το δικό του υποδίκτυο, ενώ το DNS κάνει τα Queries-Requests στους servers που βρίσκονται σε όλο το δίκτυο και όχι μόνο στο δικό του υποδίκτυο.

16. ARP – Έξω από το υποδίκτυο
    a. Ο Α δημιουργεί datagram(3ου) με τις source-dest IP.
    b. Ο Α εγκυβοτίζει το datagram σε ένα πλαίσιο προστέθοντας την MAC dest αυτή του router και MAC source του Α.
    c. Το πλαίσιο φεύγει και φτάνει στον router. Αφαιρεί το 2ο επίπεδο, κοιτάζει το 2ο επίπεδο για την IP και διαβάζει ποια είναι η dest IP. Άρα παίρνει το πλαίσιο, αφαιρεί τις πληροφορίες του 2ου και μένει μόνο το datagram. Διαβάζει το datagram και συγκρίνει την IP για να κάνει routing.

d. Ο router αλλάζει την MAC source και MAC dest. Για MAC source βάζει του router και για MAC dest του B. Οι IP 3ου μένουν οι ίδιες. Άρα το πλαίσιο περιέχει το datagram και τις καινούργιες MAC και το προοθεί.
e. Όταν φτάσει στο B, ο B θα αφαιρέσει τις πληροφορίες του 2ου, θα δει στο 3ο ότι πρόκειται για την δικιά του IP και ανοίγει το πακέτο.
f. 

    i. Αν ο B είναι ένας server, με ποιο πρωτόκολλο θα μάθουμε την IP του;
        1. Με DNS θα μάθω την IP του και μετά μέσω του ARP θα μάθουμε την MAC του και να μεταφερθεί το πακέτο
    ii. 3η υπόθεση. Με ποιο πρωτόκολλο μαθαίνει το gateway; (Δεν χρησιμοποιείται static routing.
        1. Με το DHCP θα μάθουμε ποιος είναι ο router πρώτου Hop.
    iii. 4η υπόθεση. Πως;
        1. Με ARP θα μάθουμε την MAC.

17. Ethernet
    a. Πως το Ethernet είναι ελεύθερο συγκρούσεων;
        i. Είναι ελεύθερο συγκρούσεων επειδή χρησιμοποιείται τοπολογία αστέρα. Δηλαδή υπάρχει στο κέντρο ένα switch και η κάθε συσκευή συνδέεται στο switch με ξεχωριστό Ethernet. Άρα από την στιγμή που συνδέονται ξεχωριστά, δεν υπάρχουν συγκρούσεις κόμβων.
18. Ethernet δομή
    a. Σύγκριση 3ου επιπέδου με 2ου επιπέδου στα source – destination. Γιατί στο Ethernet είναι πρώτα το dest και μετά source ενώ στο IP είναι πρώτα το source και μετά το dest;
        i. Επειδή η MAC Address βλέπει πρώτα το destination για να δει αν το πλαίσιο προωρίζεται για αυτήν. Αν δεν είναι για αυτήν τότε δεν προχωράει στα παραπάνω επίπεδα και συνεχίζεται το ψάξιμο για να βρει το πλαίσιο που ανήκει.
    b. Το CRC κάνει ένα κυκλικό έλεγχο πλεονασμού στον συγκεκριμένο δέκτη και ανιχνεύει αν υπάρχει λάθος στο πλαίσιο. Αν υπάρχει λάθος γίνεται απόρριψη του πλαισίου

i. Αν γίνει απόρριψη, θα γίνει αναμετάδοση; Αν ναι, ποιος θα ζητήσει αναμετάδοση; Ποιο επίπεδο;
    1. Γίνεται αναμετάδοση και μόνο το επίπεδο μεταφοράς θα το ζητήσει. Θα διαπιστώσει ότι ο παραλήπτης δεν έστειλε ACK για το συγκεκριμένο πακέτο, οπότε θα γίνει αναμετάδοση. Για το Ethernet και για τα τυχαίας προσπέλασης πρωτόκολλα αν δεν συμβεί σύγκρουση, έχει την εγγύηση ο αποστολέας ότι πήγε στον παραλήπτη. Αν έχει λάθη το 2ο επίπεδο θα γίνει απόρριψη και δεν θα ανέβει στα πιο πάνω επίπεδα. Το 3ο επίπεδο θα καταλάβει ότι δεν του έφτασε IP datagram, το 4ο επίπεδο θα πει ότι υπάρχει loss. Άρα το TCP αν δεν πάρει ACK σε ένα συγκεκριμένο timeout ή αν πάρει 3 διπλότυπα ACKs ακόμα και αν δεν τελειώσει το timeout τότε καταλαβαίνει ότι έχει χαθεί κάτι και κάνει αναμετάδοση.

ii. Άρα για το CRC αν δεν έχω σύγκρουση και βρω όμως ότι έχω σφάλμα, θα γίνει drop. Ενώ όταν έχω σύγκρουση γίνεται backoff(CSMA/CD) και ξανά προσπαθώ να μεταδόσω γιατί όταν πήγα να ξεκινήσω υπάρχει σύγκρουση.

c. Το Ethernet είναι αναξιόπιστο σαν υπηρεσία και ασυνδεσμικό σαν υπηρεσία.
    i. Ασυνδεσμικό είναι γιατί δεν χρειάζεται η χειραψία των προσαρμογέων.
    ii. Αναξιόπιστο είναι γιατί ο προσαρμογέας λήψης δεν στέλνει ACK/NAK στον προσαρμογεα αποστολής. Άρα τα δεδομένα που απορρίφθηκαν ανακτόνται μόνο αν ο αρχικός αποστολέας χρησιμοποιήσει αξιόπιστη μεταφορά σε TCP, αλλιώς με UDP θα χαθούν.

d. Σύγκριση Ethernet – UDP
    i. S

e. Με βάση τα πρωτόκολλα διαφορετικών επιπέδων τι είναι στο κομμάτι συνδεσμικότητας, αξιοπιστίας, τι είναι το κάθε ένα; (TCP, UDP, IP, Ethernet).
    i. D

f. Τι είναι παραμένουσα – μη παραμένουσα. Σε ποια άλλα πρωτόκολλα έχουμε;
    i. Μη παραμένον είναι όταν κάθε σύνδεση TCP κλείνει αφού ο σέρβερ στείλει το αντικείμενο στον πελάτη. Άρα αν ζητήσω πολλά πράγματα, θα πρέπει να ανοιγοκλείνω συνέχεια την σύνδεση.
    ii. Παραμένον είναι όταν έχουμε ένα ανοιχτό κανάλι TCP μεταξύ του πελάτη και του σέρβερ και μπορούμε να ανταλλάσσουμε συνέχεια τα αντικείμενα που θέλουμε από την ίδια σύνδεση η οποία δεν κλείνει.
    iii. Στο HTTP έχουμε παραμένουσα – μη παραμένουσα.

g. Η σύνδεση που έχει ο υπολογιστής με το default gateway είναι παραμένουσα ή μη;
    i. Αυτό έχει να κάνει με τον ARP πίνακα. Για όσο υπάρχει το TTL και βρίσκεται μέσα στον πίνακα, για όλο αυτό το χρονικό διάστημα είναι παραμένουσα. Γιατί ξέρω ότι μέσα στον πίνακα ARP ποια είναι η φυσική

σύνδεση MAC, όπου είναι το default gateway. Έχω αντίστοιχα και την IP του (αν δεν την έχω την βρίσκω μέσω DNS αλλιώς δεν μπορώ να μάθω την IP οποιουδήποτε υπολογιστή μέσω του DNS.

19. Τι είναι η δυαδική οπισθοχώρηση;
    a. Η δυαδική οπισθοχώρηση είναι το πως καθορίζεται το τυχαίο διάστημα για να επαναληφθεί η διαδικασία μετάδοσης μετά από σύγκρουση.
20. Τι είναι το εκθετικό back off;
    a. Το εκθετικό back-off είναι ο αλγόριθμος που χρησιμοποιεί η δυαδική οπισθοχώρηση για να ορίσει το διάστημα για την διαδικασία μετάδοσης.

21. Switch vs Router
    a. Και τα δύο αποθηκεύουν και προωθούν.
        i. Τα routers είναι επιπέδου δικτύου και εξετάζουν την κεφαλίδα 3ου επιπέδου.
        ii. Τα switches είναι επιπέδου ζεύξης και εξετάζουν τις κεφαλίδες 2ου επιπέδου.
    b. Και τα δύο έχουν πίνακες προώθησης
        i. Τα routers υπολογίζουν τους πίνακες χρησιμοποιόντας αλγορίθμους routing με βάση τις IP addresses.
        ii. Τα switches μαθαίνουν μόνα τους και γεμίζουν τον πίνακα προώθησης χρησιμοποιόντας το flooding, έχουν την αυτό-εκμάθηση και μαθαίνουν τις MAC.
    c. Επίπεδο ποιο θεωρείται ότι είναι;
        i. Το switch είναι επίπεδο γιατί είναι hardware και μπορώ να το πάρω από το δίκτυο και να το συνδέσω κάπου αλλού και θα κάνει την ίδια δουλειά. (plug and play)
        ii. Ένας router ανοίκει κάτω από το δίκτυο στο οποίο τον έχουμε βάλει, άρα είναι ιεραρχικό. Δεν είναι Plug and play αφού πρέπει να το σετάρω πρώτα.