

ΠΕΡΙΕΧΟΜΕΝΑ

SOS ΕΡΩΤΗΣΕΙΣ ΕΞΕΤΑΣΤΙΚΗΣ 2023 , ΟΠΩΣ ΑΝΑΦΕΡΘΗΚΑΝ ΣΤΟ ΤΕΛΕΥΤΑΙΟ
ΕΠΑΝΑΛΗΠΤΙΚΟ ΜΑΘΗΜΑ

ΓΕΝΙΚΕΣ ΕΡΩΤΗΣΕΙΣ

Σ/Λ

ΑΠΑΝΤΗΣΕΙΣ ΣΤΙΣ ΕΡΩΤΗΣΕΙΣ ΤΟΥ ΒΙΒΛΙΟΥ :

Κεφ 1 απαντήσεις στις επαναληπτικές ερωτήσεις βιβλίου
Κεφ 2 απαντήσεις στις επαναληπτικές ερωτήσεις βιβλίου
Κεφ 3 απαντήσεις στις επαναληπτικές ερωτήσεις βιβλίου
Κεφ 4 απαντήσεις στις επαναληπτικές ερωτήσεις βιβλίου
Κεφ 5 απαντήσεις στις επαναληπτικές ερωτήσεις βιβλίου
Κεφ 6 απαντήσεις στις επαναληπτικές ερωτήσεις βιβλίου

Πυρήνας του Δικτύου
Μεταγωγή κυκλώματος
Μεταγωγή Κυκλώματος vs Μεταγωγή Πακέτου
Επίπεδο Εφαρμογής
Επίπεδο Μεταφοράς
Επίπεδο Δικτύου
Επίπεδο Ζεύξης

Chapter 1 : Introduction
Chapter 2 : Application Layer
Chapter 3 : Transport Layer
Chapter 4: The Network Layer: Data Plane
Chapter 5: The Network Layer: Control Pane

Quiz

πολλαπλης :

https://media.pearsoncmg.com/ph/esm/ecs_kurose_compnetwork_8/cw/content/self-assessment-mc/self-assessment-mc.php

True/False :

https://media.pearsoncmg.com/ph/esm/ecs_kurose_compnetwork_8/cw/content/self-assessment-tf/self-assessment-tf.php

λυσεις σε ολες τις επαναληπτικες ασκησεις του βιβλιου :
Solutions Manual for Computer Networking A Top Down Approach - COMP 4123 - PVAMU -
Studocu

**SOS ΕΡΩΤΗΣΕΙΣ ΕΞΕΤΑΣΤΙΚΗΣ 2023 , ΟΠΩΣ ΑΝΑΦΕΡΘΗΚΑΝ ΣΤΟ
ΤΕΛΕΥΤΑΙΟ ΕΠΑΝΑΛΗΠΤΙΚΟ ΜΑΘΗΜΑ**

Παραμενουσες / μη παραμενουσες Πότε ο πελάτης Web και ο εξυπηρετητής Web χρησιμοποιούν παραμένουσες και πότε μη-παραμένουσες συνδέσεις;	σελίδα 98	ενοτητα 2.2.2 Πρωτη παραγραφος
Κυρια Συστατικά Ηλεκτρονικου Ταχυδρομειου	σελιδα 116	ενοτητα 2.3
Τι ειναι: Παραθυρο ληψης, παράθυρο συμφόρησης (ποιο χρησιμοποιεί ο αποστολεας TCP)	σελίδα 247 264	(247)Το TCP παρεχει...ξεχωριστο παραθυρο ληψης (264)Ο μηχανισμος ελεγχου...τελος τυπου
Χρονος διαδρομης στο TCP(Round Trip Time-RTT)	σελίδα 235	Το δείγμα RTT...μία επιβεβαίωση για το τμήμα.
Τι ειναι το διπλοτυπο ACK στο TCP πρωτοκολλο	σελίδα 243	Ο αποστολεας μπορει συχνά..μια προηγουμενη επιβεβαιωση
Ποια ειναι η ενεργεια παραληπτη TCP: Αφιξη τμηματος εκτος σειρας με μεγαλυτερο απο τον αναμενομενο αριθμο ακολουθιας	σελίδα 244	**ΠΙΝΑΚΑΚΙ** ΣΥΣΤΑΣΗ ΠΑΡΑΓΩΓΗΣ TCP ACK:
Slow start, αποφυγη συμφορησης	σελίδα 266-267	(266)Ετσι στην κατασταση ...φασης αργης εκκινησης (267) Κατα την εισοδο...μια νεα επιβεβαιωση
[SOS] Ποια πεδια του πακετου IP εξεταζει ο προορισμος και πως καθοριζει αν ειναι συνεχομενα πακετα του ιδιου μεγαλυτερου πακετου	σελίδα 332	<i>Ταυτοτητα,σημαιες, μετατοπιση κατατμησης</i> ΕΙΚΟΝΑ ΒΙΒΛΙΟΥ 7ης ΈΚΔΟΣΗΣ με περιγραφη : Ποια πεδία του IP δεδομενογράμματος/πακέτου εξετάζει ο υπολογιστής προορισμού και πως καθορίζει ότι δύο δεδομενογράμματα που

		καθορίστηκε ότι ανήκουν στο ίδιο μεγαλύτερο δεδομενόγραμμα είναι ή όχι συνεχόμενα τεμάχια του μεγαλύτερου δεδομενογράμματος;
[SOS] Αφου ολα τα πακετα που φτανουν σε εναν δρομολογητη NAT απο το ιντερνετ εχουν την ιδια διευθυνση προορισμου IP, πως ξερει ο δρομολογητης τον εσωτερικο υπολογιστη που πρεπει να προωθησει το πακετο [SOS]	σελίδα 345-346	Ο δρομολογητης με δυνατοτητες NAT...μεσα στο οικιακο δικτυο

ΓΕΝΙΚΕΣ ΕΡΩΤΗΣΕΙΣ

1. Γιατί το TCP λέγεται ότι είναι συνδεσμικό;

(σελιδα 91 8η, σελ 93 7η)

Το TCP περιλαμβάνει μια συνδεσμική υπηρεσία, κάνει τον πελάτη και τον εξυπηρέτη να ανταλλάσσουν πληροφορίες ελέγχου επιπέδου μεταφοράς μεταξύ τους, πριν αρχίσουν να ρέουν τα μηνύματα επιπέδου εφαρμογής.

Αυτή η αποκαλούμενη διαδικασία **χειραψίας** προειδοποιεί τον πελάτη και τον εξυπηρέτη, επιτρέποντάς τους να προετοιμαστούν για ανταλλαγή πακέτων.

Μετά τη φάση χειραψίας, λέγεται ότι υπάρχει μια σύνδεση TCP ανάμεσα στις υποδοχές των δύο διεργασιών. Η σύνδεση είναι μία πλήρως αμφίδρομη σχέση, επειδή οι δύο διεργασίες μπορούν να στέλνουν ταυτόχρονα μηνύματα μεταξύ της διαμέσου σύνδεσης. Όταν η εφαρμογή τελειώσει με την αποστολή μηνυμάτων, διακόπτει τη σύνδεση.

(σελ 227)

Το TCP) λέγεται ότι είναι συνδεσμικό, επειδή προτού ξεκινήσει μια διαδικασία εφαρμογής να στέλνει δεδομένα σε μια άλλη, οι δύο διεργασίες πρέπει πρώτα να «**χαιρετιστούν**» μεταξύ τους—δηλαδή, πρέπει να στείλουν ορισμένα προκαταρκτικά τμήματα το ένα στο άλλο για να καθορίσουν τις παραμέτρους του την επακόλουθη μεταφορά δεδομένων. Ως μέρος της δημιουργίας 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;

(ΣΕΛ 82, ΣΕΛ 244 8η, σελ 249 7η)

Εάν ο αποστολέας TCP λάβει **τρία διπλότυπα ACK** για τα ίδια δεδομένα, το λαμβάνει ως ένδειξη ότι το τμήμα που ακολουθεί το τμήμα που έχει λάβει ACK τρεις φορές έχει χαθεί. Στην περίπτωση που ληφθούν τρία διπλότυπα ACK, ο αποστολέας TCP εκτελεί μια γρήγορη αναμετάδοση, ανα μεταδίδοντας το τμήμα που λείπει πριν λήξει ο χρονοδιακόπτης αυτού του τμήματος. το TCP δεν μπορεί να πει με βεβαιότητα εάν ένα τμήμα ή το ACK του έχει χαθεί, καταστραφεί ή καθυστερήσει υπερβολικά. Στον αποστολέα, η απάντηση του TCP θα είναι η ίδια: επαναμετάδοση του εν λόγω τμήματος.

3. Περιγράψτε εν συντομία την αρχιτεκτονική client-server και την αρχιτεκτονική ομότιμων.

(ΣΕΛ 84, 85)

Σε μία αρχιτεκτονική client-server:

- υπάρχει ένας πάντα ενεργός υπολογιστής, που καλείται εξυπηρετητής, όπου έχει μια σταθερή, γνωστή διεύθυνση, που ονομάζεται διεύθυνση IP. Ρολος του, να εξυπηρετεί αιτήσεις για υπηρεσίες από πολλούς άλλους υπολογιστές, που καλούνται πελάτες
- επειδή ο διακομιστής είναι **πάντα ενεργοποιημένος**, ένας πελάτης μπορεί πάντα να επικοινωνήσει με τον διακομιστή στέλνοντας ένα πακέτο στη διεύθυνση IP του διακομιστή. Για το λόγο αυτό, ένα κέντρο δεδομένων, που στεγάζει μεγάλο αριθμό κεντρικών υπολογιστών, χρησιμοποιείται συχνά για τη δημιουργία ενός ισχυρού εικονικού διακομιστή
- Για κάθε **ζεύγος** διαδικασιών επικοινωνίας, τυπικά χαρακτηρίζουμε τη μία από τις δύο διεργασίες ως πελάτη και την άλλη ως διακομιστή.
- οι πελάτες δεν επικοινωνούν απευθείας μεταξύ τους.

Σε μία αρχιτεκτονική ομοτίμων:(P2P)

- υπάρχει **μικρή ή και καμία εξάρτηση** από αποκλειστικούς εξυπηρετές (servers) σε κέντρα δεδομένων. Αντιθέτως, η εφαρμογή εκμεταλλεύεται την απευθείας επικοινωνία ανάμεσα σε ζεύγη κατά διαστήματα 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 εξυπηρετή, η αρχιτεκτονική καλείται αρχιτεκτονική ομοτίμων.

- σε ορισμένες εφαρμογές, όπως στην κοινή χρήση αρχείων P2P, μια διεργασία μπορεί να είναι και πελάτης και διακομιστής.
- σημαντικό χαρακτηριστικό: η **αυτο-κλιμάκωση** (**scalability** τους. Για παράδειγμα, παρόλο που κάθε peer δημιουργεί φόρτο εργασίας ζητώντας αρχεία, κάθε peer προσθέτει επίσης δυνατότητα εξυπηρέτησης στο σύστημα, διανέμοντας αρχεία σε άλλους ομοτίμους.
- (+) οικονομικά αποδοτικές, (-προκλήσεις ασφάλειας, απόδοσης και αξιοπιστίας)

4. Πότε ο πελάτης web και ο εξυπηρετητής Web χρησιμοποιούν παραμένουσες συνδέσεις (persistent connections) και πότε μη παραμένουσες συνδέσεις (non- persistent connections). (ΣΕΛ 98)

το HTTP χρησιμοποιεί μόνιμες συνδέσεις στην προεπιλεγμένη λειτουργία του, αλλά οι πελάτες και οι διακομιστές HTTP μπορούν να ρυθμιστούν ώστε να χρησιμοποιούν μη μόνιμες συνδέσεις

Όταν σε μια αλληλεπίδραση client-server κάθε ζεύγος αιτήματος/απόκρισης αποστέλλεται μέσω ξεχωριστής σύνδεσης TCP η οποία κλείνει κατά την ολοκλήρωση της: λέγεται **μη παραμενουσα**, αντιθετα αν όλα τα αιτήματα και οι αντίστοιχες απαντήσεις τους αποστέλλονται την ίδια σύνδεση λέγεται **παραμενουσα**.

5. Αναφέρετε μια σημαντική ομοιότητα και μια σημαντική διαφορά στη λειτουργία των πρωτοκόλλων SMTP & HTTP. (smtp: σελ 122, http: σελ 330)

Ομοιότητες :

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

Διαφορές :

- Το **HTTP** είναι κυρίως ένα πρωτόκολλο προσέλκυσης (**pull protocol**)

μεταφέρει αρχεία από έναν server WEB σε έναν client Web ενώ το

- Το **SMTP** είναι κυρίως ένα πρωτόκολλο προώθησης (**push protocol**) .μεταφέρει αρχεία από έναν server ταχυδρομείου σε έναν άλλο server Ταχυδρομείου.
- Στο SMTP, ο περιορισμός ASCII 7 - Bit, απαιτεί τα δυαδικά δεδομένα πολυμέσων να κωδικοποιούνται σε ASCII πριν σταλούν μέσω του SMTP, και το αντίστοιχο μήνυμα ASCII να αποκωδικοποιείται πάλι σε δυαδικό μετά τη μεταφορά μέσω SMTP.
- Το HTTP, δεν απαιτεί τα δεδομένα πολυμέσων να είναι κωδικοποιημένα σε ASCII πριν τη μεταφορά τους.
- Και οι δύο πλευρές του SMTP εκτελούνται σε κάθε εξυπηρετή ταχυδρομείου. Όταν ένας εξυπηρετής ταχυδρομείου στέλνει αλληλογραφία σε άλλους εξυπηρετές ταχυδρομείου, ενεργεί ως πελάτης SMTP. Όταν ένας εξυπηρετής ταχυδρομείου δέχεται αλληλογραφία από άλλους εξυπηρετές ταχυδρομείου, ενεργεί ως εξυπηρετής SMTP.
-

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

(σελ 310)

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**

7. Για ποιους λόγους μια εφαρμογή θα επέλεγε το UDP και όχι το TCP πρωτόκολλο?

(σελ 200 εκδ 7, σελ 195 εκδ 8)

A) Καλύτερος έλεγχος επιπέδου εφαρμογής σε ότι αφορά στο ποια δεδομένα αποστέλλονται και πότε

B) Μη εγκαθίδρυση σύνδεσης(το TCP μια τριμερη χειραψια ενώ το udp όχι, έτσι δεν εισαγει καμια καθυστερηση)

Γ) Ανύπαρκτη κατάσταση σύνδεσης(μπορει τυπικα να υποστηριζει πολυ περισσοτερους πελατες οταν η εφαρμογη εκτελειται πανω απο UDP)

Δ) Μικρή καθυστέρηση κεφαλίδας πακέτου (UDP κεφαλιδα 8 bytes < TCP κεφαλιδα 20 bytes).

8. Αναφέρετε 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>>? (σελ 204, 186, 238, 200, ρδτ2 207,208 , πεδία tcp 230)

Αθροισμα ελέγχου διαδικτύου: (σελ 332 8η εκδ)

Το άθροισμα ελέγχου κεφαλίδας βοηθά έναν δρομολογητή για την ανίχνευση σφαλμάτων bit σε ένα λαμβανόμενο datagram IP. Υπολογίζεται λαμβάνοντας κάθε 2 byte μέσα στην κεφαλίδα, ως έναν αριθμό και αθροίζοντας αυτούς τους αριθμούς χρησιμοποιώντας αριθμητική συμπληρώματος ως προς 1.

Αθροισμα ελέγχου μεταφοράς: (σελ 232 8η)

Το TCP/UDP στην πλευρά αποστολής βρίσκει το 1-συμπλήρωμα 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. Επειδή το TCP αναγνωρίζει μόνο byte μέχρι το πρώτο byte που λείπει στη ροή, το TCP λέγεται ότι παρέχει αθροιστικές επιβεβαιώσεις.

Χρησιμοποιούνται και τα 2 επειδή (σελ 333 8η):

- 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 πάνω από ένα διαφορετικό πρωτόκολλο δικτύου. (πχ το ATM) και το IP μπορεί να μεταφέρει δεδομένα που δεν θα περνούν στο TCP/UDP.

9. Τι ορίζει ένα πρωτόκολλο στην δικτύωση υπολογιστών? (σελ 9 7η εκδ, σελ 9 8η εκδ)

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.

10. Αναφέρετε και περιγράψτε εν συντομία τις υπηρεσίες που περιλαμβάνει το μοντέλο υπηρεσίας TCP.

(σελ 92 8η, αναφέρεται και η συνδεσμική υπηρεσία)

- 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 **πολύπλεξη και αποπολύπλεξη** επιπέδου μεταφοράς παρέχουν επίσης έλεγχο ακεραιότητας συμπεριλαμβάνοντας πεδία ανίχνευσης σφαλμάτων στις κεφαλίδες των τμημάτων τους. **(σελ 186)**
- Το TCP δημιουργεί μια αξιόπιστη υπηρεσία μεταφοράς δεδομένων πάνω από την αναξιόπιστη υπηρεσία βέλτιστης προσπάθειας του IP, διασφαλίζοντας ότι η ροή δεδομένων που διαβάζει μια διεργασία από την προσωρινή μνήμη λήψης TCP της δεν είναι κατεστραμμένη, χωρίς κενά, χωρίς διπλασιασμούς και με τη σειρά **(σελ 238 8η)**
- ο TCP παρέχει επίσης υπηρεσία ελέγχου ροής (ταιριάζει το ρυθμό με τον οποίο ο αποστολέας στέλνει, με τον ρυθμό που ο παραλήπτης διαβάζει). Πετυχαίνει τον έλεγχο ροής κανοντας τον αποστολέα να διατηρεί μια δυναμική μεταβλητή **rwnd** (παράθυρο λήψης) , όπου ο ρολος της είναι να δίνει στον αποστολέα μια ιδέα του ελευθερού χωρου που μενει. **(σελ 247 8η, σελ 252 7η)**

Αν ο αποστολέας TCP επιβραδυνει εξαιτίας της συμφορησης μεσα στο δικτυο IP, αυτη η μορφη ελεγχου λεγεται ελεγχος συμφορησης (αλλα αν και οι ενεργειες του ελεγχου ροης, και του ελεγχου συμφορησης ειναι ιδιες, δηλαδη η επιβραδυνση, γινονται για διαφορετικους σκοπους)

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

(σελ 247 8η, σελ 252 7η)

Αν ο αποστολέας TCP επιβραδυνει εξαιτίας της συμφορησης μεσα στο δικτυο IP, αυτη η μορφη ελεγχου λεγεται ελεγχος συμφορησης (αλλα αν και οι ενεργειες του ελεγχου ροης, και του ελεγχου συμφορησης ειναι ιδιες, δηλαδη η επιβραδυνση, γινονται για διαφορετικους σκοπους)

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

12. Ποιος είναι ο χρόνος διαδρομής (RTT) στο TCP πρωτόκολλο και ποιος ο χρόνος επαναμετάδοσης(time out) ?

(σελ 99 8η, σελ 102 7η) (σελ 235 8η, σελ 242 7η)

Το δείγμα **RTT** είναι ο χρόνος που χρειάζεται για να ταξιδέψει ένα μικρό πακέτο από πελάτη σε διακομιστή και μετά να επιστρέψει στον πελάτη. Το RTT περιλαμβάνει καθυστερήσεις διάδοσης πακέτων, καθυστερήσεις ουράς πακέτων σε ενδιάμεσους δρομολογητές και μεταγωγείς και καθυστερήσεις επεξεργασίας πακέτων. 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.

(σελ 235 8η)

Ο χρόνος επαναμετάδοσης **time out** αφορά έναν χρονομετρητή, όπου το TCP αποκρίνεται στο συμβαν λήξης χρόνου, επανα μεταδίδοντας το τμήμα που προκάλεσε την λήξη χρόνου. Το TCP κατοπιν επανεκκινεί τον χρονομετρητή. (πρέπει να είναι μεγαλύτερος από το χρόνο διαδρομής μετ' επιστροφής (RTT), αλλιώς θα γίνονται άχρηστες αναμεταδόσεις)

13. Πώς λειτουργεί η αργή εκκίνηση (slow start) στο TCP πρωτόκολλο πως η αποφυγή συμφόρησης? (σελ 272 7η, σελ 266 8η)

Όταν ξεκινήσει μια σύνδεση TCP , η τιμή της **cwnd** **αρχικοποιείται** σε μια μικρή τιμή του **1 MSS**, γεγονός που έχει ως αποτέλεσμα έναν αρχικό ρυθμό αποστολής περίπου MSS/RTT .

Δεδομένου ότι το διαθέσιμο εύρος ζώνης στον αποστολέα TCP μπορεί να είναι πολύ **μεγαλύτερο** από το MSS/RTT , ο αποστολέας TCP θα ήθελε να βρει

γρήγορα το ποσό του **διαθέσιμου εύρους ζώνης**.

Έτσι, στην κατάσταση **αργής εκκίνησης**, η τιμή του cwnd ξεκινά από 1 MSS και **αυξάνεται κατά 1 MSS** κάθε φορά που ένα μεταδιδόμενο τμήμα επιβεβαιώνεται για πρώτη φορά. Αυτή η διαδικασία έχει ως αποτέλεσμα τον διπλασιασμό του ρυθμού αποστολής κάθε RTT. Έτσι, ο ρυθμός αποστολής TCP ξεκινά αργά αλλά **αυξάνεται εκθετικά** κατά τη φάση αργής εκκίνησης.

Όταν γίνεται είσοδος στην κατάσταση **αποφυγής συμφόρησης** αποστολέας TCP ορίζει την τιμή του **cwnd** περίπου στην μιση που είχε προ συμφόρησης. **αυξάνει την cwnd κατά 1 MSS / CWND** (ΓΡΑΜΜΙΚΗ ΑΥΞΗΣΗ). Ορίζει επίσης την τιμή μιας δεύτερης μεταβλητής κατάστασης, ssthresh (σύντομο χέρι για "οριακό όριο αργής έναρξης") σε $cwnd/2$ — το μισό της τιμής της τιμής του παραθύρου συμφόρησης όταν εντοπίστηκε συμφόρηση

Έτσι αντί να διπλασιάζει 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.

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

(σελ 331 7η, 332 8η)

Αυτό το πεδίο χρησιμοποιείται μόνο όταν ένα δεδομένογραμμα 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. Ο αριθμός πρωτοκόλλου είναι η κόλλα που **συνδέει τα στρώματα δικτύου και μεταφοράς** μεταξύ τους.

15. 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. (σελιδα 91 8η, σελ 93 7η)

- **(ΣΥΝΔΕΣΜΙΚΗ)** Το TCP κάνει τον πελάτη και τον εξυπηρετητή να ανταλλάσσουν 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 (σελ 252 7η, σελ 247 8η)

- Ο έλεγχος συμφόρησης του TCP παρέχεται μέσω της υπηρεσία ελέγχου ροής (ταιριάζει το ρυθμο με τον οποίο ο αποστολέας στέλνει, με τον ρυθμο που ο παραληπτής διαβάσει).Αν ο αποστολέας TCP επιβραδυνει εξαιτίας της συμφορησης μεσα στο δικτυο IP, αυτη η μορφη ελεγχου λεγεται ελεγχος συμφορησης (αλλα αν και οι ενεργειες του ελεγχου ροης, και του ελεγχου συμφορησης ειναι ιδιες, δηλαδη η επιβραδυνση, γινονται για διαφορετικους σκοπους)
- Το μοντέλο TCP υλοποιεί συνδεσμική υπηρεσία και έλεγχο συμφόρησης ενώ το μοντέλο UDP όχι. (σελ 197 8η)

16. 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?

- Επειδή ένας εξυπηρετητής HTTP δεν κρατά πληροφορίες για τους πελάτες(δε χρειάζεται συνδεση/αυθεντικοποίηση) θεωρείται ένα ακαταστατικό πρωτόκολλο.
- Κατά τη διάρκεια μιας συνόδου , ο εξυπηρετητής FTP πρέπει να διατηρεί την κατάσταση (state) για τον χρήστη.
- 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.

17. 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?
(σελ 237 7η, σελ 231,232 8η)

- 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.
- Το TCP είναι αμφίδρομο, οπότε ο υπολογιστής A μπορεί να λαμβάνει δεδομένα από τον υπολογιστή B , ενώ στέλνει δεδομένα στον υπολογιστή B ως τμήμα της ίδιας σύνδεσης TCP . Καθένα από τα τμήματα που φτάνουν από τον υπολογιστή B έχει έναν αριθμό ακολουθίας για τα δεδομένα που ρέουν από τον β προς τον A. Ο **αριθμός επιβεβαίωσης** που θέτει ο υπολογιστής A στο τμήμα του είναι ο αριθμός ακολουθίας του επόμενου byte που περιμένει ο υπολογιστής A από τον υπολογιστή B.
- Επειδή το TCP επιβεβαιώνει μόνο byte μέχρι το πρώτο ελλείπον byte στο ρεύμα, λέγεται ότι παρέχει **συσσωρευτικές επιβεβαιώσεις**.

18. Αναφέρετε μια σημαντική ομοιότητα και σημαντική διαφορά στη λειτουργία των πρωτοκόλλων FTP & HTTP. [NOT SURE]

Ομοιότητες:

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

Διαφορές:

- Η πιο χτυπητή διαφορά είναι ότι το FTP χρησιμοποιεί δύο παράλληλες συνδέσεις TCP 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.
- 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.

19. Στην εγκαθίδρυση σύνδεσης TCP, μπορεί και αν ναι σε ποιο βήμα να μεταφέρει δεδομένα ο πελάτης; Επίσης, μπορεί και αν ναι σε ποιο βήμα να μεταφέρει δεδομένα ο εξυπηρέτης; (σελ 228 8η)

Ο πελάτης στέλνει πρώτα ένα ειδικό τμήμα TCP. ο διακομιστής ανταποκρίνεται με ένα δεύτερο ειδικό τμήμα TCP. και τελικά ο πελάτης απαντά ξανά με ένα τρίτο ειδικό τμήμα. Τα δύο πρώτα τμήματα δεν φέρουν ωφέλιμο φορτίο, δηλαδή δεν φέρουν δεδομένα επιπέδου εφαρμογής. το τρίτο από αυτά τα τμήματα μπορεί να φέρει ωφέλιμο φορτίο. Επειδή τρία τμήματα αποστέλλονται μεταξύ των δύο κεντρικών υπολογιστών, αυτή η διαδικασία δημιουργίας σύνδεσης αναφέρεται συχνά ως χειραψία τριών κατευθύνσεων. Μόλις δημιουργηθεί μια σύνδεση TCP, οι δύο διαδικασίες εφαρμογής μπορούν να στείλουν δεδομένα η μία στην άλλη.

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

(σελ 135 7η, σελ 132 8η)

Το **TTL** είναι ο χρόνος που θα ζησει μια εγγραφή πόρου. Καθορίζει πότε ένας πόρος πρέπει να αφαιρεθεί από μια κρυφή μνήμη. Το πεδίο χρόνου ζωής time to live περιλαμβάνεται για να διασφαλίσει ότι τα δεδομενογράμματα δεν κυκλοφορούν για πάντα μέσα στο δίκτυο.

(σελ 331 7η, σελ 332 8η)

• Χρόνος ζωής. Το πεδίο **time-to-live** (TTL) περιλαμβάνεται για να διασφαλιστεί ότι τα datagrams δεν θα κυκλοφορούν για πάντα (λόγω, για παράδειγμα, ενός βρόχου δρομολόγησης μεγάλης διάρκειας) στο δίκτυο. Αυτό το πεδίο μειώνεται κατά ένα κάθε φορά που το datagram υποβάλλεται σε επεξεργασία από έναν δρομολογητή. Εάν το πεδίο TTL φτάσει στο 0, ένας δρομολογητής πρέπει να απορρίψει αυτό το datagram.

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

(σελ 108 7η, σελ 107 8η)

- 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.

(σελ 110 7η, σελ 108 8η)

- Αν και τα cookies συχνά απλοποιούν τις αγορές στο διαδίκτυο για τον

χρήστη, παραμένουν άκρως αμφισβητήσιμα, επειδή μπορούν να θεωρηθούν ως παραβίαση της ιδιωτικότητας. 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? (σελ 244 7η , σελ 238 8η)

Το TCP δημιουργεί μια 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 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 **ληξεις χρόνου** (time out) ώστε να ανακάμψει από χαμένα τμήματα. κατόπιν παρουσιάζουμε μια πληρέστερη περιγραφή , που χρησιμοποιεί διπλότυπες επιβεβαιώσεις εκτός των λήξεων χρόνου.

23. ΣΥΣΤΑΣΗ ΠΑΡΑΓΩΓΗΣ TCP ACK:

Συμβάν	Ενέργεια παραλήπτη TCP
Αφίξη τμήματος στη σωστή σειρά, με τον αναμενόμενο αριθμό ακολουθίας. Όλα τα τμήματα μέχρι τον αναμενόμενο αριθμό ακολουθίας έχουν ήδη επιβεβαιωθεί.	Καθυστερημένο ACK. Αναμονή έως 500 ms για την άφιξη ενός άλλου τμήματος σε σωστή σειρά. Εάν το επόμενο τμήμα στη σωστή σειρά δεν φτάσει μέσα σε αυτό το χρονικό διάστημα, αποστολή ενός ACK.
Αφίξη τμήματος στη σωστή σειρά, με τον αναμενόμενο αριθμό ακολουθίας. Ένα άλλο τμήμα με τη σωστή σειρά περιμένει για μετάδοση ACK.	Άμεση αποστολή ενός μόνο συσσωρευτικού ACK, που επιβεβαιώνει και τα δύο τμήματα με τη σωστή σειρά.
Αφίξη τμήματος εκτός σειράς με μεγαλύτερο απ' τον αναμενόμενο αριθμό ακολουθίας. Ανίχνευση χάσματος.	Άμεση αποστολή διπλότυπου ACK, που υποδεικνύει τον αριθμό ακολουθίας του επόμενου αναμενόμενου byte (το οποίο είναι το κάτω άκρο του χάσματος).
Αφίξη τμήματος που συμπληρώνει, μερικώς ή πλήρως, το χάσμα στα ληφθέντα δεδομένα.	Άμεση αποστολή ACK, αρκεί το τμήμα αυτό να αρχίζει απ' το κάτω άκρο του χάσματος.

Παράδειγμα 3.2 ♦ Σύσταση Πακέτων

24. Το Traceroute υλοποιείται με μηνύματα ICMP. Ποιος είναι ο σκοπός του Traceroute; Πώς λειτουργεί; (σελ 420 7η εκδ, σελ 424 8η)

Το Traceroute μας επιτρέπει να εντοπίσουμε μια διαδρομή από έναν κεντρικό υπολογιστή σε οποιονδήποτε άλλο οικοδεσπότη στον κόσμο, αρα και να μετρήσουμε την καθυστέρηση από άκρο σε άκρο σε ένα δίκτυο υπολογιστών

Υλοποιείται με μηνύματα ICMP, για να προσδιορίσει τα ονόματα και τις διευθύνσεις των δρομολογητών μεταξύ της πηγής και του προορισμού.

Εστω 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.

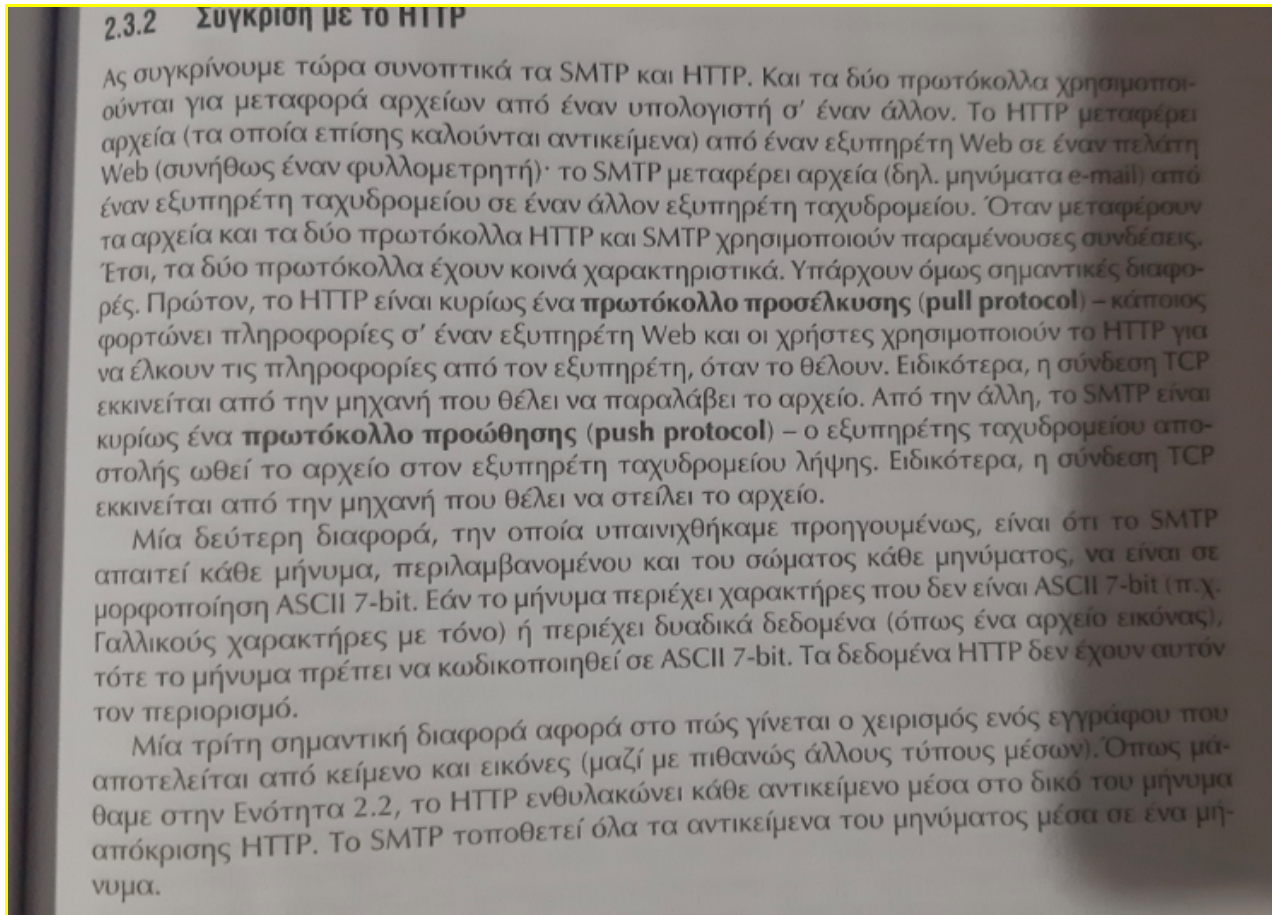
Επίσης, όταν ο υπολογιστής προορισμού λάβει το N-οστό πακέτο, και αυτός επίσης στέλνει ένα μήνυμα πίσω στην προέλευση.

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 προορισμό.

25. Ποιες είναι οι τρεις διαφορές ανάμεσα στο HTTP και SMTP;

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

(σελ. 121 εκδ 7 , smtp)



2. Το HTTP είναι stateless. (σελ.100 7η έκδοση)

Επειδή ένας εξυπηρετής HTTP δεν κρατά πληροφορίες για τους πελάτες, το HTTP λέγεται ότι είναι ένα ακαταστασικό πρωτόκολλο

(stateless : κάθε αιτημα γίνεται μεμονωμενα χωρις αναφορα στο ιστορικο προηγουμενων συνεδριων αντιθετα stateful : οταν κραται συνεδρια απο προηγουμενα request)

Το **HTTP** είναι κυρίως ένα πρωτόκολλο προσέλκυσης (pull protocol) μεταφέρει αρχεία από έναν server WEB σε έναν client Web χωρίς να χρειάζεται κωδικοποίηση ενώ το

Το **SMTP** είναι κυρίως ένα πρωτόκολλο προώθησης (push protocol) .μεταφέρει αρχεία από έναν server ταχυδρομείου σε έναν άλλο server Ταχυδρομείου & χρειάζεται κωδικοποίηση

26. , Ποια πεδία του IP δεδομενογράμματος/πακέτου εξετάζει ο υπολογιστής προορισμού και πως καθορίζει ότι δύο δεδομενογράμματα που καθορίστηκε ότι ανήκουν στο ίδιο μεγαλύτερο δεδομενόγραμμα είναι ή όχι συνεχόμενα τεμάχια του μεγαλύτερου δεδομενογράμματος; (σελ. 333 7η εκδ. / σελ. 332 8η εκδ)

Ταυτότητα, σημαίες, μετατόπιση κατάτμησης.

- Για την επίτευξη αυτού του σκοπού φροντίζει ο υπολογιστής **προέλευσης** όπου σε κάθε δεδομένογραμμα προς αποστολή αυξάνει κατά ένα τον αριθμό ταυτότητας τους.
- Στην συνέχεια όταν ο **δρομολογητής** πρέπει να μεταφέρει ένα δεδομένογραμμα το τεμαχίζει και σφραγίζει κάθε ένα από τα επιμερους δίνοντας στο κάθε ένα : 1. διεύθυνση προέλευσης & προορισμού, & 2. τον αριθμό ταυτότητας του αρχικού πακέτου.
- Τέλος, για να μπορέσει ο υπολογιστής **προορισμού** να ναι σίγουρος ότι ελαβε και το τελευταίο τεμαχίο, το τελευταίο τεμαχίο έχει flag=0.Ενώ όλα τα άλλα έχουν flag=1. Επίσης για να μπορέσει να καθορίσει αν λείπει ένα τεμαχίο, αλλά και να τα ανασυνθέσει με την σωστή σειρά χρησιμοποιεί το πεδίο μετατόπισης για να καθορίσει που μπαίνει το κάθε τεμαχίο στο αρχικό πακέτο.

ποια από τα δεδομενογράμματα είναι τεμάχια του ίδιου μεγαλύτερου δεδομενογράμματος. Επειδή το IP είναι μία αναξιόπιστη υπηρεσία, ένα ή 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 σ' αυτό το bit-σημαία την τιμή 1. Επίσης, για να μπορεί να καθορίσει ο υπολογιστής προορισμού εάν λείπει ένα τεμάχιο (και επίσης να μπορέσει να ανασυνθέσει τα τεμάχια με την σωστή τους σειρά), το πεδίο μετατόπισης χρησιμοποιείται για να καθορίσει πού μπαίνει το τεμάχιο μέσα στο αρχικό δεδομένογραμμα IP.

27. Τι είναι το παράθυρο λήψης (receive window) στο TCP πρωτόκολλο; Τι είναι το παράθυρο συμφόρησης (congestion window); Πιο παράθυρο χρησιμοποιεί ο αποστολέας TCP;
(σελ 247, σελ. 264)

Το TCP παρέχει έλεγχο ροής ζητώντας από τον **αποστολέα** να διατηρεί μια μεταβλητή που ονομάζεται παράθυρο λήψης(**cwnd**). Ανεπίσημα, το παράθυρο λήψης χρησιμοποιείται για να δώσει στον αποστολέα μια ιδέα για το πόσο ελεύθερο χώρο προσωρινής αποθήκευσης είναι διαθέσιμος στον δέκτη

Ο μηχανισμός ελέγχου συμφόρησης TCP που λειτουργεί στον αποστολέα παρακολουθεί μια πρόσθετη μεταβλητή, το παράθυρο συμφόρησης(**rwnd**). Το παράθυρο συμφόρησης, που συμβολίζεται cwnd, επιβάλλει έναν περιορισμό στον ρυθμό με τον οποίο ένας αποστολέας TCP μπορεί να στείλει κίνηση στο δίκτυο.

Ο αποστολέας έχει και το rwnd και το cwnd.

28. 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;
(σελ 243,244)

Όταν λαμβάνει ένας δέκτης TCP ένα τμήμα με έναν αριθμό ακολουθίας μεγαλύτερο από τον επόμενο, αναμενόμενο, κατά σειρά αριθμό σειράς, ανιχνεύει ένα κενό στη ροή δεδομένων—δηλαδή, ένα τμήμα που λείπει.

Αυτό το κενό μπορεί να είναι αποτέλεσμα απώλειας ή αναδιάταξης τμημάτων εντός του δικτύου. Εφόσον το TCP δεν χρησιμοποιεί αρνητικές επιβεβαιώσεις, ο παραλήπτης δεν μπορεί να στείλει μια ρητή αρνητική επιβεβαίωση πίσω στον αποστολέα. Αντίθετα, απλώς αναγνωρίζει ξανά (δηλαδή, δημιουργεί ένα διπλότυπο ACK για) το τελευταίο κατά σειρά byte δεδομένων που έχει λάβει.

Επειδή ένας αποστολέας συχνά στέλνει μεγάλο αριθμό τμημάτων, εάν χαθεί ένα τμήμα, πιθανότατα θα υπάρχουν πολλά διπλότυπα ACK. Εάν ο αποστολέας TCP λάβει τρία διπλά ACK για τα ίδια δεδομένα, το λαμβάνει ως ένδειξη ότι το τμήμα που ακολουθεί το τμήμα που έχει λάβει ACK τρεις φορές έχει χαθεί.

Στην περίπτωση που ληφθούν τρία διπλότυπα ACK, ο αποστολέας TCP εκτελεί μια γρήγορη αναμετάδοση, αναμεταδίδοντας το τμήμα που λείπει πριν λήξει ο χρονοδιακόπτης αυτού του τμήματος.

29. 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;

- Για την επίτευξη αυτού του σκοπού φροντίζει ο υπολογιστής **προέλευσης** όπου σε κάθε δεδομένογραμμα προς αποστολή αυξάνει κατά ένα τον αριθμό ταυτότητας τους.
- Στην συνέχεια όταν ο **δρομολογητής** πρέπει να μεταφέρει ένα δεδομένογραμμα το τεμαχίζει και σφραγίζει κάθε ένα από τα επιμερους δίνοντας στο κάθε ένα :
1. διεύθυνση προέλευσης & προορισμού, & 2. **τον αριθμό ταυτότητας του αρχικού πακέτου.**

Τελος, για να μπορεσει ο υπολογιστής **προορισμού** να καταλαβει **είναι τεμάχια του ίδιου μεγαλύτερου δεδομενογράμματος** ελεγχει τη ταυτοτητα με τα οποια τα σφραγισε ο **δρομολογητής** πριν τα τεμαχισει.

30. 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; (σελ 470 8η)

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 , ξεκινά 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 **δυναμικής εκθετικής υποχώρησης**. Δηλαδή, περιμένει ένα διάστημα μέχρι να ξαναστείλει, το οποίο αυξάνεται κάθε φορά που εντοπίζεται σύγκρουση

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

Εάν ένα πακέτο χαθεί στη διαδρομή από τον διακομιστή προς τον πελάτη, τότε ο διακομιστής θα μεταδώσει ξανά το πακέτο

- **rdt2** : το βάρος του εντοπισμού και της ανάκτησης από χαμένα πακέτα πεφτει στον αποστολέα. είτε το πακέτο είτε το ACK του παραλήπτη αυτού του πακέτου χαθούν και στις δύο περιπτώσεις, **δεν υπάρχει απάντηση στον αποστολέα από τον παραλήπτη**. Εάν ο αποστολέας είναι διατεθειμένος να περιμένει αρκετό καιρό ώστε να είναι σίγουρο ότι ένα πακέτο έχει χαθεί, μπορεί απλώς να επαναμεταδώσει το πακέτο δεδομένων.
- **GNB** : Σε ένα πρωτόκολλο GNB ο παραληπτης πρέπει να αποκριθει σε 2 συμβαντα:
 1. Όταν λαμβάνει στη **σωστή σειρά** ένα πακέτο n : (δηλαδή, τα δεδομένα που παραδόθηκαν τελευταία στο ανώτερο στρώμα προήλθαν από ένα πακέτο με αριθμό σειράς $n - 1$), ο παραληπτης στέλνει ένα ACK για το πακέτο n και παραδίδει τα δεδομένα τμήμα του πακέτου στο ανώτερο στρώμα.
 2. Όταν **ΔΕΝ** λαμβάνει στη σωστή σειρά ένα πακέτο n ο παραλήπτης **απορρίπτει το πακέτο** και στέλνει ξανά ένα ACK για το πιο πρόσφατα ληφθέν πακέτο παραγγελίας.
- **επιλεκτική επαναληψη SR**: (τα πρωτόκολλα επιλεκτικής επανάληψης αποφεύγουν τις περιττές αναμεταδόσεις βάζοντας τον αποστολέα να επαναμεταδίδει μόνο εκείνα τα πακέτα που υποψιάζεται ότι χάθηκαν ή καταστράφηκαν) στον δέκτη.
 - θα απαιτήσει από τον παραλήπτη να αναγνωρίσει μεμονωμένα τα σωστά ληφθέντα πακέτα
 - ο παραληπτης SR θα επιβεβαιώνει ένα σωστά ληφθέν πακέτο, είτε είναι με ορθη σειρά είτε όχι. Τα πακέτα εκτός σειράς αποθηκεύονται στην προσωρινή μνήμη μέχρι να ληφθούν οποιαδήποτε χαμένα πακέτα (δηλαδή πακέτα με μικροτερους αριθμους ακολουθιας), οπότε μια δέσμη πακέτων μπορεί να παραδοθεί στο ανώτερο στρώμα **(σελ 221 8η)**

32. Το CSMA/CD πως μοιάζει με ανθρώπινη συμπεριφορά; **(σελ 469 8η)**

Ως άνθρωποι έχουμε πρωτόκολλα, μεσω των οποιων 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.

33. Ποιά είναι τα κοινά χαρακτηριστικά των κεφαλίδων των πρωτοκόλλων 2ου, 3ου 4ου επιπέδου.Ως παράδειγμα συγκρίνετε το Ethernet - IP - TCP

κεφαλίδα 2ου επιπέδου/ζευξης (Ethernet)(σελ 486 8η)

- (δεδομένα) περιέχει τα δεδομένα του δεδομενογράμματος IP
- (προελευση) MAC ADDRESS προσαρμογέα προορισμού
- (προορισμός) MAC ADDRESS προσαρμογέα που εκπέμπει το πλαίσιο πάνω στο LAN
- (πολυπλεξη/αποπολυπλεξη πρωτοκόλλου επιπέδου δικτύου : που θα μεταβιβασθούν τα περιεχόμενα του πεδίου δεδομένων του ενός πλαισίου ETHERNET)

ΠΕΔΙΟ ΤΥΠΟΥ (συνδεση επιπεδων ζευξης και δικτυου)

κεφαλίδα 3ου επιπέδου/δικτύου (IP) (σελ 331 8η)

- (εκδοση πρωτοκόλλου) αριθμός εκδόσης
- (καθορισμός μήκους κεφαλίδας IP) μήκος κεφαλίδας μεταβλητό, λόγω επιλογών που περιλαμβάνονται στη κεφαλίδα
- (ειδοποίηση συμφορησης & διακριση τυπων δεδομενογραμματος) ΤΟΣ ΤΥΠΟΣ ΥΠΗΡΕΣΙΑΣ
- (μήκος δεδομενογραμματος) συνολικό μήκος δεδομενογραμματος
- (μετατοπιση κατατμησης IP), σειρά επανασυνθεσης μικροτερων datagrams
- flags (0:last, 1:rest)
- ID
- (χρονο σφραγιση/διαρκεια ζωης) TTL
- (πολυπλεξη/αποπολυπλεξη πρωτοκόλλου μεταφορας : που θα μεταβιβασθούν τα περιεχόμενα του πεδίου δεδομένων ενός datagram)
- **ΑΡΙΘΜΟΣ ΠΡΩΤΟΚΟΛΛΟΥ(συνδεση επιπεδων δικτυου και μεταφορας)** 17 -> UDP 6->TCP
- (ανιχνευση σφαλματος)_αθροισμα ελεγχου κεφαλίδας
- (προελευση-προορισμός)_διευθυνση προελευσης και διευθυνση προορισμου
- (επεκταση κεφαλίδας ip) πεδίο επιλογών
- (δεδομένα)_περιέχει τα δεδομένα/ωφέλιμο φορτίο του TCP, & ICMP μηνυματα

κεφαλίδα 4ου επιπέδου/μεταφορας (TCP) (σελ 230 8η)

- (πολυπλεξη/αποπολυπλεξη, προελευση-προορισμός:)

ΑΡΙΘΜΟΙ ΘΥΡΩΝ ΠΡΟΕΛΕΥΣΗΣ/ΠΡΟΟΡΙΣΜΟΥ(συνδεση επιπεδων μεταφορας και εφαρμογης)

- (αξιοπιστη μεταφορα) αριθμο ακολουθιας, αριθμου επιβεβαιωσης
- (διαθεσιμος χωρος παραληπτη) παραθυρο ληψης,
- (καθορισμος μηκους κεφαλιδας TCP)_μηκος κεφαλιδας,
- (χρονο σφραγιση/διαπραγματευση ακρων για max size του MSS) πεδιο επιλογων
- (flags)
- (επιβεβαιωση εγκυροτητας) ACK
- (εγκαθιδρυση/διακοπη συνδεσης) RST , SYN, FIN
- (ειδοποιηση συμφορησης) CWR , ECE
- (μεταβιβαση σε ανωτερο επιπεδο) PSH
- (προτεραιότητα) URG
- (δεδομενα)

(αρα κοινα πεδια πεδια ειναι ολα οσα εχει το ethernet)

34. Περιγράψτε τους μηχανισμούς TCP που ελέγχουν το παράθυρο συμφόρησης.

Ο έλεγχος συμφόρησης του TCP ως μηχανισμός που λειτουργεί στον αποστολέα παρακολουθεί μια πρόσθετη μεταβλητή, το παράθυρο συμφόρησης. Το παράθυρο συμφόρησης, που συμβολίζεται cwnd, επιβάλλει έναν περιορισμό στον ρυθμό με τον οποίο ένας αποστολέας TCP μπορεί να στείλει κίνηση στο δίκτυο.

Συγκεκριμένα, η ποσότητα των μη επιβεβαιωμένων δεδομένων(=LastByteSent – LastByteAcked) σε έναν αποστολέα δεν μπορεί να υπερβαίνει το ελάχιστο των cwnd και rwnd, δηλαδή: LastByteSent – LastByteAcked ... min{cwnd, rwnd}

35. Το DNS αποκαλείται σύστημα. Απο τι αποτελείται; Γιατί χρησιμοποιείται το UDP ως υποκείμενο πρωτόκολλο και όχι το TCP.

36. Ποιά είναι η διαφορά μεταξύ UDP-TCP σε σχέση με την πολύπλεξη και αποπολύπλεξη; Ποιές άλλες διαφορές έχουν σε σχέση με την υπηρεσία στην καλούσα εφαρμογή; Ποια είναι η ομοιότητα των POP3 και IMAP; Ποιά είναι η κοινή διαφορά τους σε σχέση με το SMTP;

Σ/Λ

37. Το TCP Reno αποφεύγει τους χαμηλούς ρυθμούς μετάδοσης της αργής εκκίνησης χάρη στο μηχανισμό «ταχείας επαναμετάδοσης».

[ΛΑΘΟΣ] ο μηχανισμός λέγεται ταχεία ανάκαμψη (σελ 270 8η εκδ)

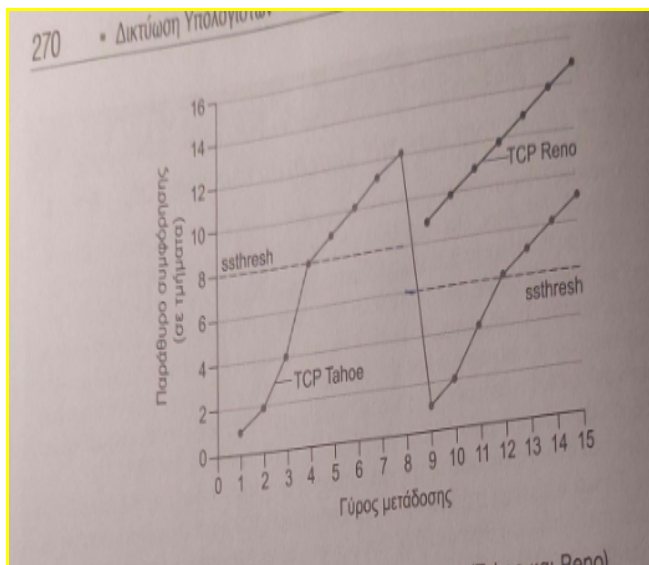
38. Το TCP σχεδιάστηκε για να υποστηρίξει μεταδόσεις σε σταθερά και ασύρματα δίκτυα.

[ΛΑΘΟΣ] σχεδιάστηκε το 1970 επειδή υπήρχαν πολλά δίκτυα. Κάθε ένα από αυτά τα δίκτυα είχε το δικό του πρωτόκολλο, οπότε αναγνωρίστηκε η σημασία διασυνδεσης των δικτύων μέσω ενός ενιαίου πρωτοκόλλου και δημιουργήθηκε το tcp.

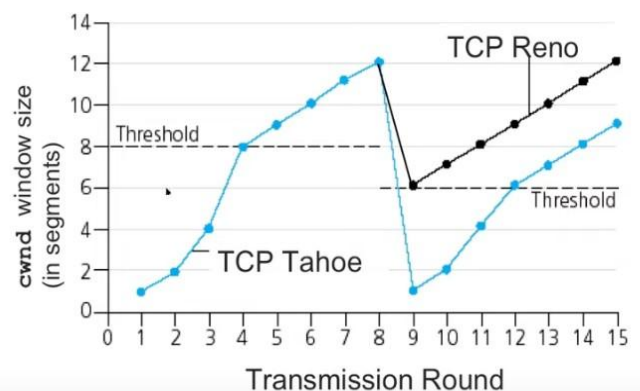
(σελ 228 8η εκδ)

39. Η «ταχεία ανάκαμψη» οδηγεί γενικά σε υψηλότερη μέση τιμή του παραθύρου συμφορήσης. (σελ 268 8η εκδ)

[ΛΑΘΟΣ] επειδή μετά την ενεργοποίηση του μηχανισμού αποφυγής συμφορήσης η νέα μέση τιμή παραθύρου συμφορήσης ($ssthresh = cwnd/2$) ανανεώνει τη τιμή της $ssthresh$ σε $cwnd/2$ για το $cwnd$ κατά το οποίο προκλήθηκε η συμφορήση και τότε εισέρχεται σε ταχεία ανάκαμψη (προφανώς με μικρότερο $ssthresh$).



Popular “Flavors” of TCP



40. Ένας υπολογιστής με μια διεύθυνση IP μπορεί να έχει μέχρι 65536 ταυτοχρονες συνδέσεις TCP (σελ 188 8η εκδ) [NOT SURE]

[ΣΩΣΤΟ] μπορεί να έχει μέχρι $2^{16}=65535$ tcp connection(όσα είναι και τα ports)

41. Το UDP θεωρείται connectionless πρωτόκολλο διότι δεν εγγυάται την παράδοση των πακέτων. (σελ 247)

[ΛΑΘΟΣ] το UDP θεωρείται connectionless επειδή δε διατηρεί κατάσταση συνδεσης, αφού δε κάνει χειραψία μεταξύ των τερματικών. ΧΩΡΙΣ να αναιρείται το δεύτερο σκελος της προτασης, αποτέλεσμα του "connectionless" είναι η μη εγγυημένη παράδοση πακέτων.

42. Τα παράθυρα συμφόρησης & λήψης (cwnd/rwnd) υπολογίζονται από τον παραλήπτη του TCP. (σελ 247 & σελ 264 8η)

[ΛΑΘΟΣ] Το cwnd υπολογίζεται από τον αποστολέα, όπου προσαρμόζοντας την τιμή της cwnd μπορεί να ρυθμίσει τον ρυθμό με τον οποίο στέλνει data μες στην συνδεση του.(tcp)

Το rwnd, υπολογίζεται και αυτο απο τον αποστολέα.

43. Η επικεφαλίδα TCP διαθέτει πεδίο για την ενημέρωση σχετικά με το παράθυρο λήψης (rwnd). (σελ 230 8η)

[ΣΩΣΤΟ] διότι είναι πεδίο που χρειάζεται για τον έλεγχο ροής(δειχνει ποσα bytes προτιθεται να δεχτει ένας παραληπτης.

44. Η επικεφαλίδα TCP διαθέτει πεδίο για την ενημέρωση σχετικά με το παράθυρο συμφορησης (cwnd). (σελ 230 8η)

[ΛΑΘΟΣ] δεν διαθετει πεδιο για την ενημερωση σχετικά με το παράθυρο συμφόρησης.

45. Το TCP Reno αποφεύγει τους χαμηλούς ρυθμούς μετάδοσης της αργής εκκίνησης χάρη στο μηχανισμό «ταχείας επαναμετάδοσης».

ΙΣΧΥΕΙ ΟΤΙ ΤΟ TCP RENO ΑΠΟΦΕΥΓΕΙ ΤΟΥΣ ΧΑΜΗΛΟΥΣ ΡΥΘΜΟΥΣ ΜΕΤΑΔΟΣΗΣ ΤΗΣ ΑΡΓΗΣ ΕΚΚΙΝΗΣΗΣ

αλλα

[ΛΑΘΟΣ] επειδη ο μηχανισμος δε λεγεται ταχειας επαναμεταδοσης, λεγεται ταχεία ανάκαμψης

και τον ενσωμάτωσε ο TCP RENO, όπου μετά το γεγονός που προκάλεσε συμφορηση, ενώ το TCP πηγαινε σε κατασταση αργης εκκινησης(χαμηλοι ρυθμοι μεταδοσης αφου θετει $cwnd=1MSS$), το **TCP RENO πηγαινει σε κατασταση ταχειας ανακαμψης(υψηλοτεροι ρυθμοι μεταδοσης** αφου θετει($cwnd=ssthresh+3 MSS$) τιμη προφανως μεγαλυτερη απο αυτην της αργης εκκινησης. **(σελ 268 8η)**

σειρα: 3 διπλότυπα ACK -> ταχεια αναμετάδοση- >ταχεία ανάκαμψη

46. 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 **(σελ 278 8η)**

[ΣΩΣΤΟ] τα υψηλά ποσοστά απώλειας που προκαλούνται από τους μη ελεγχόμενους αποστολές UDP θα αναγκάσουν τους αποστολές TCP (οι οποίοι, μειώνουν τα ποσοστά αποστολής τους ενόψει της συμφόρησης) να μειώσουν δραματικά τους ρυθμούς τους. Έτσι, **η έλλειψη ελέγχου συμφόρησης στο UDP** μπορεί να έχει ως αποτέλεσμα υψηλά ποσοστά απώλειας μεταξύ ενός αποστολέα και παραλήπτη UDP και τον **παραγκωνισμό των συνεδριών TCP**.

47. Στον μηχανισμό ελέγχου συμφόρησης του TCP, όταν ο μετρητής (timer) ληξει στον αποστολέα, το κατώφλι (threshold) παίρνει τιμή ίση με το μισό της τιμής που είχε πριν. **[ΛΑΘΟΣ]**

Ο αλγόριθμος αποφυγής συμφόρησης του TCP συμπεριφέρεται το ίδιο όταν εμφανίζεται ένα γεγονός ληξης χρονου, όπως στην περίπτωση αργής εκκίνησης: Η τιμή του **cwnd ορίζεται σε 1 MSS** και η τιμή του ssthresh ενημερώνεται στο μισό της τιμής του cwnd όταν συνέβη το συμβάν απώλειας **(σελ 267 8η)**

48. Η μεταγωγή πακέτου υποστηρίζει ευρέως διαφορετικούς τύπους σύνδεσης και ρυθμούς ζεύξης. **[ΣΩΣΤΟ] [!]**

49. Το "BEST EFFORT" σημαίνει ότι τα δεδομενογράμματα παραδόθηκαν στους προορισμούς όσο πιο γρήγορα γίνεται. **[ΛΑΘΟΣ]**

το βασικό μοντέλο υπηρεσιών βέλτιστης προσπάθειας **δεν είναι αξιόπιστο**. Δεν εγγυάται την ληψη των πακετων με τη σειρα που σταλθηκαν

δεν εγγυάται την τελικη παράδοση τους

δεν εγγυάται την απο ακρο σε ακρο καθυστέρηση

ουτε υπάρχει εγγυηση ελαχιστου ευρους ζωνης

50. Μια συσκευή Α στέλνει δύο TCP segments το ένα αμέσως μετά το άλλο στην συσκευή Β πάνω από μια TCP σύνδεση. Αν το πρώτο έχει αριθμό ακολουθίας 80, ενώ το δεύτερο 120, τα δεδομένα στο πρώτο segment είναι 30 bytes. (σελ. 232)

[ΛΑΘΟΣ] Επειδη Τα δεδομενα στο πρωτο segment ειναι 40 bytes.
(20 κεφαλιδα TCP+20bytes της κεφαλιδας IP)

51. Σε ένα πρωτόκολλο Go-Back-N ο παραληπτής πρέπει να αποκριθεί σε διάφορα συμβάντα. (σελ. 216 8η)

[ΣΩΣΤΟ]

Σε ενα πρωτόκολλο GNB ο παραληπτης πρεπει να αποκριθει σε 2 συμβαντα:

1. Όταν λαμβάνει στη σωστή σειρά ένα πακέτο n : (δηλαδή, τα δεδομένα που παραδόθηκαν τελευταία στο ανώτερο στρώμα προήλθαν από ένα πακέτο με αριθμό σειράς $n - 1$), ο δέκτης στέλνει ένα ACK για το πακέτο n και παραδίδει τα δεδομένα τμήμα του πακέτου στο ανώτερο στρώμα.

2. Όταν ΔΕΝ λαμβάνει στη σωστή σειρά ένα πακέτο n ο παραλήπτης απορρίπτει το πακέτο και στέλνει ξανά ένα ACK για το πιο πρόσφατα ληφθέν πακέτο παραγγελίας.

52. Το πρωτόκολλο ICMP λειτουργεί στο 2ο επίπεδο(ζεύξης). (σελ. 423 8η)

[ΛΑΘΟΣ] Το ICMP ειναι πρωτόκολλο ελέγχου μηνυμάτων δικτύου και χρησιμοποιείται από υπολογιστές & δρομολογητές για ανταλλαγή πληροφοριών ΣΕ ΕΠΊΠΕΔΟ ΔΙΚΤΥΟΥ(3ο).

53. Έστω ότι ο Host A στέλνει μέσω μιας TCP σύνδεσης στον host B ένα segment με αριθμό ακολουθίας 38 και 4 bytes δεδομένων. Σε αυτο το ίδιο segment acknowledgment number θα είναι απαραίτητα 42. [ΛΑΘΟΣ]

54. Το SMTP είναι πρωτόκολλο προώθησης. (σελ. 121 7η έκδοση)

[ΣΩΣΤΟ], γιατί ο εξυπηρέτης ταχυδρομείου αποστολής ωθεί το αρχείο στον εξυπηρέτη ταχυδρομείου λήψης. Ειδικότερα, η σύνδεση TCP εκκινείται από

την μηχανή που θέλει να στείλει το αρχείο.

55. Το διπλότυπο ACK εκκινεί τη διαδικασία ταχείας ανάκαμψης.

(σελ 270 8η) [NOT SURE]

[ΣΩΣΤΟ] Για να ενεργοποιηθεί η ταχεία ανάκαμψη πρέπει να υπάρχει συμβάν απώλειας (δηλαδή 3 διπλοτυπα ACK που υπονοούν συμφόρηση που υποδηλώνεται από μια λήξη χρόνου). Κάθε αφικνουμένο ACK στη διαδικασία αποφυγής συμφόρησης, αυξάνει το cwnd με αποτέλεσμα ένα απολεσθέν τμήμα, δίνοντας εναυσμα για ταχεία ανακαμψη. Εισέρχεται σε κατάσταση συμφορησης. Αυτό έχει ως αποτέλεσμα να εισελθει επειτα σε κατασταση ταχειας ανάκαμψης.

56. Το διπλότυπο ACK εκκινεί τη διαδικασία ταχείας επαναμετάδοσης. (σελ. 243)

[ΛΑΘΟΣ] ένα διπλοτυπο ACK είναι ένα ACK που επιβεβαιώνει την εκ νέου την ληψη ενός τμηματος, για το οποίο ο αποστολεας έχει ήδη λαβει μια προηγουμενη επιβεβαιωση.

57. Έστω ότι ένας HOST A στέλνει ένα αρχείο στον HOST B μέσω μιας TCP ροής. Ο αριθμός των bytes που στέλνει ο A αλλά δεν έχουν επιβεβαιωθεί δεν μπορεί να υπερβαίνει το μέγεθος του παραθύρου λήψης. (σελ. 247, 248 8η εκδ)

[ΣΩΣΤΟ]

58. Η αρχή του end-to-end είναι μια ομάδα από κανόνες που εγγυάται την ποιότητα των συνδέσεων .

[NOT Sure]

(σελ. 199 , 363, 8η εκδ)

η αρχη του end to end δηλώνει ότι εφόσον καποια λειτουργια (πχ ανίχνευση σφαλμάτων επιπεδου μεταφορας) πρέπει να υλοποιηθει απο ακρο σε ακρο: «λειτουργίες τοποθετημένες στα χαμηλότερα επίπεδα μπορεί να είναι περιττες ή μικρής αξίας σε σύγκριση με το κόστος παροχής τους στο υψηλότερο επίπεδο.»

Επειδή το IP υποτίθεται ότι εκτελείται σε σχεδόν οποιοδήποτε πρωτόκολλο επιπέδου-2, είναι χρήσιμο για το επίπεδο μεταφοράς να παρέχει έλεγχο σφαλμάτων ως μέτρο ασφαλείας.

59. Τα switches εμφανίζουν χαμηλότερη καθυστέρηση σε σχέση με τους routers. (σελ. 497 8η εκδ)

[ΣΩΣΤΟ] οι δρομολογητές, έχουν συχνά μεγαλύτερο χρόνο επεξεργασίας ανά πακέτο από τους μεταγωγείς, οπότε είναι σωστή η πρόταση ότι τα switches εμφανίζουν χαμηλότερη καθυστέρηση από τους δρομολογητές.

Αυτό ισχύει επειδή:

- οι δρομολογητές δεν είναι συσκευές σύνδεσης και άμεσης λειτουργίας (γίνεται διαμορφωση των IP των υπολογιστών που συνδέονται στους δρομολογητές) και πρέπει να επεξεργάζονται πακέτα μέχρι και το **επίπεδο 3** προς τα πάνω.
- οι μεταγωγείς είναι συσκευές σύνδεσης και άμεσης λειτουργίας, και επεξεργάζονται πακέτα μόνο μέχρι το **επίπεδο 2**.

60. Στο HTTP με διοχέτευση τα αιτήματα έχουν μικρότερο χρόνο απόκρισης.

[ΛΑΘΟΣ] (σελ 114 ,8η εκδ) Head of Line [HOL] blocking

61. Μια συσκευή Α στέλνει δύο TCP segments το ένα αμέσως μετά το άλλο στην συσκευή Β πάνω από μια TCP σύνδεση. Αν το πρώτο έχει αριθμό ακολουθίας 90, ενώ το δεύτερο 110, στη περίπτωση που το πρώτο χάνεται ενώ το δεύτερο φτάνει κανονικά το acknowledgment number που στέλνει ο Β είναι 90. **[ΣΩΣΤΟ]**

62. Η UDP κεφαλίδα περιλαμβάνει το πεδίο “more-fragments”

(σελ 198 & σελ 332 8η εκδ)

[ΛΑΘΟΣ] το UDP δεν έχει το more-fragments στην κεφαλίδα, το IP περιλαμβάνει στη κεφαλίδα του το MF (more-fragments) που αναφέρεται στη μετατόπιση κατατμήσης.

63. Το πρωτόκολλο ICMP λειτουργεί στο 3ο επίπεδο(δικτύου).(σελ. 423 8η)

[ΣΩΣΤΟ] Το ICMP είναι πρωτόκολλο ελέγχου μηνυμάτων δικτύου και χρησιμοποιείται από υπολογιστές & δρομολογητές για ανταλλαγή πληροφοριών **ΣΕ ΕΠΙΠΕΔΟ ΔΙΚΤΥΟΥ(3ο)**.

64. Στην κεφαλίδα του TCP υπάρχει πεδίο που σηματοδοτεί την συμφόρηση(network congestion).(σελ. 236-237, 7η έκδοση)

[ΣΩΣΤΟ] Στο πεδίο σημαίας (flag field), της κεφαλίδας του TCP, τα bits CWR και ECE χρησιμοποιούνται για ρητή ειδοποίηση συμφόρησης.

65. Το SMTP είναι πρωτόκολλο προσέλκυσης.(σελ. 121 7η έκδοση)

[ΛΑΘΟΣ], γιατί το SMTP είναι ένα πρωτόκολλο **προώθησης**(push protocol). Ο εξυπηρέτης ταχυδρομείου αποστολής ωθεί το αρχείο στον εξυπηρέτη ταχυδρομείου λήψης. Ειδικότερα, η σύνδεση TCP εκκινείται από την μηχανή που θέλει να στείλει το αρχείο.(

66. Στο TCP η σύνδεση κλείνει μόνο από τον παραλήπτη. (σελ 251 8η)

[ΛΑΘΟΣ] Οποιαδήποτε από τις δύο διεργασίες που συμμετέχουν σε μια σύνδεση TCP μπορεί να τερματίσει τη σύνδεση.

(εξήγηση: Όταν τελειώνει μια σύνδεση, οι "πόροι" (δηλαδή οι buffer και οι μεταβλητές) απελευθερώνονται. Ένα από τα 2 άκρα εστω Α εκδίδει μια εντολή κλεισίματος. Αυτό αναγκάζει το TCP του Α να στείλει ένα ειδικό τμήμα TCP στη διαδικασία Β. Αυτό το ειδικό τμήμα έχει ένα bit σημαίας στην κεφαλίδα του τμήματος, το bit FIN, που έχει οριστεί σε 1. Όταν ο Β λάβει αυτό το τμήμα, στέλνει στον Α ένα τμήμα επιβεβαίωσης σε αντάλλαγμα. Στη συνέχεια, ο Β στέλνει το δικό του τμήμα τερματισμού λειτουργίας, στο οποίο το bit FIN έχει οριστεί σε 1. Τέλος, ο Α αναγνωρίζει το τμήμα τερματισμού λειτουργίας του Β. Σε αυτό το σημείο, όλοι οι πόροι στους δύο οικοδεσπότες έχουν απελευθερωθεί.)

67. Το UDP υποστηρίζει εγγυημένη παράδοση με τη σωστή σειρά. (σελ 197 8η)

[ΛΑΘΟΣ] το UDP δεν διατηρεί κατάσταση σύνδεσης στα τερματικά συστήματα (αρα δεν περιλαμβάνει ενταμιευτές αποστολής και λήψης, παραμετρους ελέγχου συμφορησης, παραμετρους αριθμων ακολουθιας και επιβεβαιωσης)
Συνεπώς, δεν κρατάει πληροφορίες απαραίτητες για την αξιοπιστη μεταφορα δεδομενων και δεν εγγυάται την παραδοση ολων των πακετων, ποσο μαλλον την παραδοση τους με τη σωστη σειρα.

68. Υπάρχει prefix(ποσα bit ανηκουν στην network ip) που αντιστοιχίζεται σε 96 IPv4 διευθύνσεις. Αν είναι σωστό ποιό είναι. Αν είναι λάθος με ποιο συνδυασμό απο prefix (το μικρότερο πλήθος) το πετυχαίνουμε;

(/25 -> $2^7=128$) ή (/26 -> $2^6=64$ και /27-> $2^5=32$ που δινουν 96 ως ΣΥΝΔΥΑΣΜΟΣ)

69. Το TCP υποστηρίζει αμφίδρομη επικοινωνία μεταξύ αποστολέα και παραλήπτη.

[ΣΩΣΤΟ] Η σύνδεση είναι μια πλήρης αμφίδρομη σύνδεση, καθώς οι δύο διεργασίες μπορούν να στέλνουν μηνύματα η μία στην άλλη μέσω της σύνδεσης ταυτόχρονα (σελ 91 8η)

70. Υπάρχει prefix που αντιστοιχίζεται σε 100 IPv4 διευθύνσεις. Αν είναι σωστό ποιό είναι. Αν είναι λάθος με ποιο συνδυασμό απο prefix (το μικρότερο πλήθος) το πετυχαίνουμε;

71. Ο κεντρικός υπολογιστής A στέλνει στον κεντρικό υπολογιστή B ένα μεγάλο αρχείο μέσω μιας σύνδεσης TCP. Ας υποθέσουμε ότι ο κεντρικός υπολογιστής B δεν έχει δεδομένα για αποστολή στον κεντρικό υπολογιστή A. Ο κεντρικός υπολογιστής B δεν θα στείλει επιβεβαιώσεις στον κεντρικό υπολογιστή A επειδή ο κεντρικός υπολογιστής B δεν μπορεί να επιστρέψει τις επιβεβαιώσεις στα δεδομένα. **[ΛΑΘΟΣ]**

72. Το μέγεθος του TCP rwnd δεν αλλάζει ποτέ καθ' όλη τη διάρκεια του σύνδεση. **[ΛΑΘΟΣ]**

73. Ας υποθέσουμε ότι ο κεντρικός υπολογιστής A στέλνει στον κεντρικό

υπολογιστή B ένα μεγάλο αρχείο μέσω μιας σύνδεσης TCP. Ο αριθμός των μη επιβεβαιωμένων byte που στέλνει ο A δεν μπορεί να υπερβαίνει το μέγεθος του buffer λήψης. **[ΣΩΣΤΟ]**

74. Ας υποθέσουμε ότι ο κεντρικός υπολογιστής A στέλνει ένα μεγάλο αρχείο στον κεντρικό υπολογιστή B μέσω μιας σύνδεσης TCP. Εάν ο αύξων αριθμός για ένα τμήμα αυτής της σύνδεσης είναι m , τότε ο αύξων αριθμός για το επόμενο τμήμα θα είναι απαραίτητα $m + 1$. **[ΛΑΘΟΣ]**

75. Το τμήμα TCP έχει ένα πεδίο στην κεφαλίδα του για `rwnd`. **[ΣΩΣΤΟ]**

76. Ας υποθέσουμε ότι το τελευταίο `SampleRTT` σε μια σύνδεση TCP είναι ίσο με 1 δευτερόλεπτο. Η τρέχουσα τιμή του `TimeoutInterval` για τη σύνδεση θα είναι αναγκαστικά ≥ 1 sec. **[ΛΑΘΟΣ]**

77. Με το πρωτόκολλο SR, είναι δυνατό για τον αποστολέα να λάβει ένα ACK για ένα πακέτο που βρίσκεται εκτός του τρέχοντος παραθύρου του. **[ΣΩΣΤΟ]**

Ας υποθέσουμε ότι ο αποστολέας έχει μέγεθος παραθύρου 3 και στέλνει πακέτα 1, 2, 3 σε $0t$. Στο $1t$ ο παραλήπτης ACKs 1, 2, 3. Στο $2t$ ο αποστολέας λήγει και στέλνει ξανά 1, 2, 3. Στο $3t$ ο παραλήπτης λαμβάνει τα διπλότυπα και επιβεβαιώνει ξανά 1, 2, 3. Στο $4t$ ο αποστολέας λαμβάνει τα ACK που έστειλε ο παραλήπτης στο $1t$ και προωθεί το παράθυρό του σε 4, 5, 6. Στις $5t$ ο αποστολέας λαμβάνει τα ACKs 1, 2, 3 ο δέκτης που αποστέλλεται σε $2t$. Αυτά τα ACK βρίσκονται έξω από το παράθυρό του.

78. Με το GBN, είναι δυνατό για τον αποστολέα να λάβει ένα ACK για ένα πακέτο εκτός του τρέχοντος παραθύρου. **[ΣΩΣΤΟ]**

79. Το πρωτόκολλο εναλλασσόμενων bit είναι το ίδιο με το πρωτόκολλο SR με μέγεθος παραθύρου αποστολέα και παραλήπτη 1. **[ΣΩΣΤΟ]**

80. Το πρωτόκολλο εναλλασσόμενων bit είναι το ίδιο με το πρωτόκολλο GBN με μέγεθος παραθύρου αποστολέα και παραλήπτη 1. **[ΣΩΣΤΟ]**

με μέγεθος παραθύρου 1, τα SR, GBN και το πρωτόκολλο εναλλασσόμενου bit είναι λειτουργικά ισοδύναμα. Το μέγεθος παραθύρου 1 αποκλείει τη δυνατότητα πακέτων εκτός σειράς (εντός του παραθύρου). Ένα αθροιστικό ACK είναι απλώς ένα συνηθισμένο ACK σε αυτήν την περίπτωση, καθώς μπορεί να αναφέρεται μόνο στο μεμονωμένο πακέτο μέσα στο παράθυρο

10

Over a TCP connection, suppose host A sends two segments to host B, host B sends an acknowledgement for each segment, the first acknowledgement is lost, but the second acknowledgement arrives before the timer for the first segment expires.

- ☐ Host A will retransmit both segments
- ☒ Host A will retransmit neither segments
- ☐ Host A will retransmit the second segment
- ☐ Host A will retransmit the first segment

Correct.

81. Πως γίνεται η μετάφραση διευθύνσεων δικτύου; (σελ 345&346, 8η εκδ.)

- 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. Μπορούν να ανακτούν οι διευθύνσεις των συσκευών στο τοπικό δίκτυο χωρίς να ειδοποιηθεί ο έξω κόσμος.
 - ii. Μπορεί να αλλάξει ο ISP χωρίς να αλλάξουν οι IP στο τοπικό δίκτυο.
 - iii. 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 δόθηκε.

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

ΑΠΑΝΤΗΣΕΙΣ ΣΤΙΣ ΕΡΩΤΗΣΕΙΣ ΤΟΥ ΒΙΒΛΙΟΥ

Κεφ 1 απαντήσεις στις επαναληπτικές ερωτήσεις βιβλίου

4. Αναφέρετε 4 τεχνολογίες προσβασης,Καταταξτε καθε μια ως οικιακη προσπελαση, εταιρική προσπελαση ή ασυρματη προσπελαση ευρειας περιοχης.

- μοντεμ μεσω τηλεφωνικης γραμμης,
- DSL μεσω τηλεφωνικής γραμμης
- καλωδιο σε HFC
- 100Mbps μεταγωγεας Ethernet
- wifi
- 3G,4G (wide area wireless)

7. Ποιος ειναι ο ρυθμος μεταδοσης Ethernet LAN;

Ethernet LANs have transmission rates of 10 Mbps, 100 Mbps, 1 Gbps and 10 Gbps.

8. Ποια είναι μερικά από τα φυσικά μέσα που μπορεί να τρέξει το Ethernet;

Σήμερα, το Ethernet περνάει συνήθως πάνω από σύρμα χαλκού συνεστραμμένου ζεύγους. Μπορεί επίσης να περάσει πάνω από συνδέσμους οπτικών ινών.

10. Περιγράψτε τις πιο δημοφιλείς τεχνολογίες ασύρματης πρόσβασης στο Διαδίκτυο σήμερα. Συγκρίνετε και αντιπαραβάλλετε τα.

a) **Wifi (802.11)** In a wireless LAN, wireless users transmit/receive packets to/from an base station (i.e., wireless access point) within a radius of a few tens of meters. The base station is typically connected to the wired Internet and thus serves to connect wireless users to the wired network.

b) **3G and 4G wide-area wireless access networks.** In these systems, packets are transmitted over the same wireless infrastructure used for cellular telephony, with the base station thus being managed by a telecommunications provider. This provides wireless access to users within a radius of tens of kilometers of the base station.

12. Τι πλεονέκτημα έχει ένα δίκτυο μεταγωγής κυκλώματος έναντι ενός δικτύου μεταγωγής πακέτων εργασία? Ποια πλεονεκτήματα έχει το TDM έναντι του FDM σε ένα δίκτυο μεταγωγής κυκλώματος;

Ένα δίκτυο μεταγωγής κυκλώματος μπορεί να εγγυηθεί ένα συγκεκριμένο ποσό εύρους ζώνης από άκρο σε άκρο για τη διάρκεια μιας συνδεσης.

Τα περισσότερα δίκτυα μεταγωγής πακέτων σήμερα (συμπεριλαμβανομένου του Διαδικτύου) δεν μπορούν να παρέχουν εγγυήσεις από άκρο σε άκρο για το εύρος ζώνης.

14. Γιατί δύο πάροχοι ISP που βρίσκονται στο ίδιο επίπεδο μέσα στην ιεραρχία συχνά λειτουργούν ως ομοτιμοί μεταξύ τους;

Εάν οι δύο ISP δεν κάνουν peer μεταξύ τους, τότε όταν στέλνουν κίνηση ο ένας στον άλλο πρέπει να στείλουν την κίνηση μέσω ενός παρόχου ISP (διαμεσολαβητής), στον οποίο πρέπει να πληρώσουν για τη μεταφορά της κίνησης.

Με την άμεση ανταλλαγή μεταξύ τους, οι δύο ISP μπορούν να μειώσουν τις πληρωμές τους στους παρόχους ISP τους. Τα σημεία ανταλλαγής Διαδικτύου (IXP) (συνήθως σε ένα αυτόνομο κτίριο με τους δικούς του διακόπτες) είναι ένα σημείο συνάντησης όπου πολλοί πάροχοι υπηρεσιών Internet μπορούν να συνδεθούν και/ή να κάνουν ομότιμη σύνδεση. Ένας ISP κερδίζει τα χρήματά του χρεώνοντας σε κάθε έναν από τους ISP που συνδέονται με το IXP μια σχετικά μικρή χρέωση, η οποία μπορεί να εξαρτάται από

το ποσό της κίνησης που αποστέλλεται ή λαμβάνεται από το IXP.

16.Εξετάστε το ενδεχόμενο αποστολής ενός πακέτου από έναν κεντρικό υπολογιστή προέλευσης σε έναν κεντρικό υπολογιστή προορισμού μέσω μιας σταθερής διαδρομής. Καταχωρίστε τα στοιχεία καθυστέρησης στην καθυστέρηση από άκρο σε άκρο. Ποιες από αυτές τις καθυστερήσεις είναι σταθερές και ποιες μεταβλητές;

Τα στοιχεία καθυστέρησης είναι οι καθυστερήσεις κομβικής επεξεργασίας, οι καθυστερήσεις μετάδοσης, οι καθυστερήσεις διάδοσης και οι καθυστερήσεις στην ουρά. Όλες αυτές οι καθυστερήσεις είναι σταθερές, εκτός από τις καθυστερήσεις στην ουρά, οι οποίες είναι μεταβλητές

20.Ας υποθέσουμε ότι το τελικό σύστημα Α θέλει να στείλει ένα μεγάλο αρχείο στο τέλος του συστήματος Β. Σε πολύ υψηλό επίπεδο, περιγράψτε πώς το τελικό σύστημα Α δημιουργεί πακέτα από το αρχείο. Όταν ένα από αυτά τα πακέτα φτάνει σε έναν δρομολογητή, ποιες πληροφορίες στο πακέτο χρησιμοποιεί ο δρομολογητής για να προσδιορίσει τη σύνδεση στην οποία προωθείται το πακέτο;

Το σύστημα τερματισμού Α χωρίζει το μεγάλο αρχείο σε κομμάτια. Προσθέτει κεφαλίδα σε κάθε κομμάτι, δημιουργώντας έτσι πολλαπλά πακέτα από το αρχείο. Η κεφαλίδα σε κάθε πακέτο περιλαμβάνει τη διεύθυνση IP του προορισμού (τελικό σύστημα Β). Ο διακόπτης πακέτων χρησιμοποιεί τη διεύθυνση IP προορισμού στο πακέτο για να προσδιορίσει την εξερχόμενη σύνδεση.

22. Καταγράψτε πέντε εργασίες που μπορεί να εκτελέσει ένα επίπεδο. Είναι δυνατόν μία (ή περισσότερες) από αυτές τις εργασίες να εκτελούνται από δύο (ή περισσότερα) επίπεδα;

Πέντε γενικές εργασίες είναι ο έλεγχος σφαλμάτων, ο έλεγχος ροής, η τμηματοποίηση και η επανασυναρμολόγηση, η πολυπλεξία και η ρύθμιση σύνδεσης. Ναι, αυτές οι εργασίες μπορούν να εκτελεστούν σε διαφορετικά επίπεδα. Για παράδειγμα, ο έλεγχος σφαλμάτων παρέχεται συχνά σε περισσότερα από ένα επίπεδα.

23. Ποια είναι τα πέντε επίπεδα στη στοίβα πρωτοκόλλου Διαδικτύου; Ποια είναι τα κύρια τις ευθύνες καθενός από αυτά τα επίπεδα;

Τα πέντε επίπεδα στη στοίβα πρωτοκόλλου Διαδικτύου είναι – από πάνω προς τα κάτω – το επίπεδο εφαρμογής, το επίπεδο μεταφοράς, το επίπεδο δικτύου, το επίπεδο σύνδεσης και το φυσικό επίπεδο

25. Ποια επίπεδα στη στοίβα πρωτοκόλλου Διαδικτύου επεξεργάζεται ένας δρομολογητής; Ποια στρώματα επεξεργάζεται μια εναλλαγή επιπέδου σύνδεσης; Ποια επίπεδα επεξεργάζεται ένας κεντρικός υπολογιστής;

- Οι δρομολογητές επεξεργάζονται το δίκτυο, τη σύνδεση και τα φυσικά επίπεδα (επίπεδα 1 έως 3). (Αυτό είναι λίγο λευκό ψέμα, καθώς οι

σύγχρονοι δρομολογητές μερικές φορές λειτουργούν ως τείχη προστασίας ή στοιχεία προσωρινής αποθήκευσης και επεξεργάζονται επίσης το επίπεδο μεταφοράς.)

- Το επίπεδο σύνδεσης επεξεργάζεται τη σύνδεση και τα φυσικά επίπεδα επεξεργασίας (επίπεδα 1 έως 2).
- Οι κεντρικοί υπολογιστές επεξεργάζονται και τα πέντε επίπεδα.

Κεφ 2 απαντήσεις στις επαναληπτικές ερωτήσεις βιβλίου

2. Ποια είναι η διαφορά μεταξύ της αρχιτεκτονικής δικτύου και της αρχιτεκτονικής εφαρμογών;

- Η αρχιτεκτονική δικτύου αναφέρεται στην οργάνωση της διαδικασίας επικοινωνίας σε επίπεδα (π.χ. η αρχιτεκτονική Διαδικτύου πέντε επιπέδων).
- Η αρχιτεκτονική εφαρμογών, από την άλλη πλευρά, σχεδιάζεται από έναν προγραμματιστή εφαρμογών και υπαγορεύει την ευρεία δομή της εφαρμογής (π.χ. πελάτης-διακομιστής ή P2P)

3. Για μια συνεδρία επικοινωνίας μεταξύ ενός ζεύγους διεργασιών, ποια διεργασία είναι ο πελάτης και ποια ο διακομιστής;

Η διαδικασία που ξεκινά την επικοινωνία είναι ο πελάτης. η διαδικασία που περιμένει να επικοινωνήσει είναι ο διακομιστής

4. Για μια εφαρμογή κοινής χρήσης αρχείων P2P, συμφωνείτε με τη δήλωση, "Δεν υπάρχει έννοια των πλευρών πελάτη και διακομιστή μιας περιόδου σύνδεσης επικοινωνίας"; Γιατί ή γιατί όχι?

Όχι. Σε μια εφαρμογή κοινής χρήσης αρχείων P2P, ο ομότιμος που λαμβάνει ένα

αρχείο είναι συνήθως ο πελάτης και ο ομότιμος που στέλνει το αρχείο είναι συνήθως ο διακομιστής.

5. Ποιες πληροφορίες χρησιμοποιούνται από μια διεργασία που εκτελείται σε έναν κεντρικό υπολογιστή για να προσδιορίσει μια διαδικασία που εκτελείται σε έναν άλλο κεντρικό υπολογιστή;

Η διεύθυνση IP του κεντρικού υπολογιστή προορισμού και ο αριθμός θύρας της υποδοχής στη διαδικασία προορισμού.

6. Ας υποθέσουμε ότι θέλετε να κάνετε μια συναλλαγή από έναν απομακρυσμένο πελάτη σε έναν διακομιστή όσο το δυνατόν γρηγορότερα. Θα χρησιμοποιούσατε UDP ή TCP; Γιατί;

Θα χρησιμοποιούσατε UDP. Με το UDP, η συναλλαγή μπορεί να ολοκληρωθεί σε ένα χρόνο μετ' επιστροφής (RTT) - ο πελάτης στέλνει το αίτημα συναλλαγής σε μια υποδοχή UDP και ο διακομιστής στέλνει την απάντηση πίσω στην υποδοχή UDP του πελάτη. Με το TCP, απαιτούνται τουλάχιστον δύο RTT - ένα για τη ρύθμιση της σύνδεσης TCP και ένα άλλο για τον πελάτη για να στείλει το αίτημα και για τον διακομιστή για να στείλει πίσω την απάντηση.

8. Καταγράψτε τις τέσσερις ευρείες κατηγορίες υπηρεσιών που μπορεί να παρέχει ένα πρωτόκολλο μεταφοράς. Για καθεμία από τις κλάσεις υπηρεσιών, υποδείξτε εάν είτε το UDP είτε το TCP (ή και τα δύο) παρέχουν μια τέτοια υπηρεσία. [NOT SURE]

α) Η αξιόπιστη μεταφορά δεδομένων

- TCP παρέχει μια αξιόπιστη ροή byte μεταξύ πελάτη και διακομιστή, αλλά το UDP όχι.

β) Εγγύηση ότι θα διατηρηθεί μια συγκεκριμένη τιμή απόδοσης (κανένα)

γ) Εγγύηση ότι τα δεδομένα θα παραδοθούν εντός καθορισμένου χρονικού διαστήματος (κανένα)

δ) Εμπιστευτικότητα (μέσω κρυπτογράφησης) (κανένα)

10. Τι σημαίνει πρωτόκολλο χειραψίας;

ένα πρωτόκολλο χρησιμοποιεί χειραψία εάν οι δύο οντότητες που επικοινωνούν ανταλλάσσουν πρώτα πακέτα ελέγχου πριν στείλουν δεδομένα ή μία στην άλλη. Το SMTP χρησιμοποιεί χειραψία στο επίπεδο εφαρμογής, ενώ το HTTP όχι.

11. Γιατί τα HTTP, SMTP και IMAP τρέχουν πάνω από το TCP και όχι στο UDP;

Οι εφαρμογές που σχετίζονται με αυτά τα πρωτόκολλα απαιτούν όλα τα δεδομένα της εφαρμογής να λαμβάνονται με τη σωστή σειρά και χωρίς κενά. Το TCP παρέχει αυτήν την υπηρεσία ενώ το UDP όχι.

13. Περιγράψτε πώς η προσωρινή αποθήκευση Ιστού μπορεί να μειώσει την καθυστέρηση στη λήψη ενός αιτήματος. Η προσωρινή αποθήκευση Ιστού θα μειώσει την καθυστέρηση για όλα τα αντικείμενα που ζητούνται από έναν χρήστη ή μόνο για ορισμένα από τα αντικείμενα; Γιατί

Η προσωρινή αποθήκευση Ιστού μπορεί να φέρει το επιθυμητό περιεχόμενο «πιο κοντά» στον χρήστη, πιθανώς στο ίδιο LAN στο οποίο είναι συνδεδεμένος ο κεντρικός υπολογιστής του χρήστη.

Η προσωρινή αποθήκευση στο Web μπορεί να μειώσει την καθυστέρηση για όλα τα αντικείμενα, ακόμη και για αντικείμενα που δεν αποθηκεύονται προσωρινά, καθώς η προσωρινή αποθήκευση μειώνει την επισκεψιμότητα σε συνδέσμους

26. Στην Ενότητα 2.7, ο διακομιστής UDP που περιγράφεται χρειάζεται μόνο μία υποδοχή, ενώ ο διακομιστής TCP χρειαζόταν δύο υποδοχές. Γιατί; Εάν ο διακομιστής TCP υποστήριζε η ταυτόχρονες συνδέσεις, καθεμία από διαφορετικό κεντρικό υπολογιστή πελάτη, πόσες υποδοχές θα χρειαζόταν ο διακομιστής TCP;

Με τον διακομιστή UDP, δεν υπάρχει υποδοχή “καλωσορισματος” και όλα τα δεδομένα από διαφορετικούς πελάτες εισέρχονται στον διακομιστή μέσω αυτής της μίας υποδοχής.

Με τον διακομιστή TCP, υπάρχει μια υποδοχή υποδοχής και κάθε φορά που ένας πελάτης ξεκινά μια σύνδεση με τον διακομιστή, δημιουργείται μια νέα υποδοχή. Έτσι, για να υποστηρίξει η ταυτόχρονες συνδέσεις, ο διακομιστής θα χρειαζόταν $n+1$ υποδοχές.

Κεφ 3 απαντήσεις στις επαναληπτικές ερωτήσεις βιβλίου

3. Θεωρήστε μια σύνδεση TCP μεταξύ του κεντρικού υπολογιστή A και του κεντρικού υπολογιστή B. Ας υποθέσουμε ότι τα τμήματα TCP που ταξιδεύουν από τον κεντρικό υπολογιστή A στον κεντρικό υπολογιστή B έχουν τον αριθμό θύρας προέλευσης x και τον αριθμό θύρας προορισμού y .

Ποιοι είναι οι αριθμοί θύρας προέλευσης και προορισμού για τα τμήματα που ταξιδεύουν από τον κεντρικό υπολογιστή B στον κεντρικό υπολογιστή A;

Αριθμός θύρας προέλευσης y και αριθμός θύρας προορισμού x

4. Περιγράψτε γιατί ένας προγραμματιστής εφαρμογών μπορεί να επιλέξει να εκτελέσει μια εφαρμογή μέσω UDP αντί TCP.

Ένας προγραμματιστής εφαρμογών μπορεί να μην θέλει η εφαρμογή του να

χρησιμοποιεί τον έλεγχο συμφόρησης του TCP, ο οποίος μπορεί να μειώσει τον ρυθμό αποστολής της εφαρμογής σε περιόδους συμφόρησης.

Συχνά, οι σχεδιαστές εφαρμογών τηλεφωνίας IP και τηλεδιάσκεψης IP επιλέγουν να εκτελούν τις εφαρμογές τους μέσω UDP επειδή θέλουν να αποφύγουν τον έλεγχο συμφόρησης του TCP. Επίσης, ορισμένες εφαρμογές δεν χρειάζονται την αξιόπιστη μεταφορά δεδομένων που παρέχεται από το TCP.

6. Είναι δυνατόν μια εφαρμογή να απολαμβάνει αξιόπιστη μεταφορά δεδομένων ακόμη και όταν η εφαρμογή εκτελείται μέσω UDP; Αν ναι, πώς;

Ναί. Ο προγραμματιστής της εφαρμογής μπορεί να τοποθετήσει αξιόπιστη μεταφορά δεδομένων στο πρωτόκολλο επιπέδου εφαρμογής. Ωστόσο, αυτό θα απαιτούσε σημαντικό όγκο εργασίας και εντοπισμού σφαλμάτων.

9. Στα πρωτοκολλα μας rdt, γιατί χρειαζόταν να εισαγάγουμε αριθμούς ακολουθίας;

Οι αριθμοί ακολουθίας απαιτούνται για να ανακαλύψει ένας δέκτης εάν ένα πακέτο που φτάνει περιέχει νέα δεδομένα ή είναι μια αναμετάδοση.

10. Στα πρωτοκολλα μας rdt, γιατί χρειάστηκε να εισαγάγουμε χρονόμετρα; Για να χειριστεί τις απώλειες στο κανάλι. Εάν το ACK για ένα μεταδιδόμενο πακέτο δεν ληφθεί εντός της διάρκειας του χρονοδιακόπτη για το πακέτο, το πακέτο (ή το ACK ή το NACK του) θεωρείται ότι έχει χαθεί. Ως εκ τούτου, το πακέτο αναμεταδίδεται.

11. Ας υποθέσουμε ότι η καθυστέρηση μετ' επιστροφής μεταξύ αποστολέα και παραλήπτη είναι σταθερή και γνωστή στον αποστολέα. Θα εξακολουθούσε να είναι απαραίτητος ένας χρονοδιακόπτης στο πρωτόκολλο rdt 3.0, υποθέτοντας ότι τα πακέτα μπορούν να χαθούν;

Ένας χρονοδιακόπτης θα εξακολουθούσε να είναι απαραίτητος στο πρωτόκολλο rdt 3.0. Εάν είναι γνωστός ο χρόνος μετ' επιστροφής, τότε το μόνο πλεονέκτημα θα είναι ότι, ο αποστολέας γνωρίζει με βεβαιότητα ότι είτε το πακέτο είτε το ACK (ή NACK) για το πακέτο έχει χαθεί, σε σύγκριση με το πραγματικό σενάριο, όπου το ACK (ή NACK) ενδέχεται να είναι ακόμα καθ' οδόν προς τον αποστολέα, μετά τη λήξη του χρονοδιακόπτη. Ωστόσο, για την ανίχνευση της απώλειας, για κάθε πακέτο, θα εξακολουθεί να είναι απαραίτητος ένας χρονοδιακόπτης σταθερής διάρκειας στον αποστολέα.

(τα ακολουθα υπάρχουν και στην συγκεντρωτικη ενοτητα Σ/Λ υπ' αριθμον: 70-79)

- Ο κεντρικός υπολογιστής A στέλνει στον κεντρικό υπολογιστή B ένα μεγάλο αρχείο μέσω μιας σύνδεσης TCP. Ας υποθέσουμε ότι ο κεντρικός υπολογιστής B δεν έχει δεδομένα για αποστολή στον κεντρικό υπολογιστή A. Ο κεντρικός υπολογιστής B δεν θα στείλει επιβεβαιώσεις στον κεντρικό υπολογιστή A επειδή ο κεντρικός υπολογιστής B δεν μπορεί να επιστρέψει τις επιβεβαιώσεις στα δεδομένα. **[ΛΑΘΟΣ]**
- Το μέγεθος του TCP rwnd δεν αλλάζει ποτέ καθ' όλη τη διάρκεια του σύνδεση. **[ΛΑΘΟΣ]**
- Ας υποθέσουμε ότι ο κεντρικός υπολογιστής A στέλνει στον κεντρικό υπολογιστή B ένα μεγάλο αρχείο μέσω μιας σύνδεσης TCP. Ο αριθμός των μη επιβεβαιωμένων byte που στέλνει ο A δεν μπορεί να υπερβαίνει το μέγεθος του buffer λήψης. **[ΣΩΣΤΟ]**
- Ας υποθέσουμε ότι ο κεντρικός υπολογιστής A στέλνει ένα μεγάλο αρχείο στον κεντρικό υπολογιστή B μέσω μιας σύνδεσης TCP. Εάν ο αύξων αριθμός για ένα τμήμα αυτής της σύνδεσης είναι m, τότε ο αύξων αριθμός για το επόμενο τμήμα θα είναι απαραίτητα m + 1. **[ΛΑΘΟΣ]**
- Το τμήμα TCP έχει ένα πεδίο στην κεφαλίδα του για rwnd. **[ΣΩΣΤΟ]**
- Ας υποθέσουμε ότι το τελευταίο SampleRTT σε μια σύνδεση TCP είναι ίσο με 1 δευτερόλεπτο. Η τρέχουσα τιμή του TimeoutInterval για τη σύνδεση θα είναι αναγκαστικά ≥ 1 sec. **[ΛΑΘΟΣ]**
- Με το πρωτόκολλο SR, είναι δυνατό για τον αποστολέα να λάβει ένα ACK για ένα πακέτο που βρίσκεται εκτός του τρέχοντος παραθύρου του. **[ΣΩΣΤΟ]** Ας υποθέσουμε ότι ο αποστολέας έχει μέγεθος παραθύρου 3 και στέλνει πακέτα 1, 2, 3 σε 0t. Στο 1t)01(tt ο παραλήπτης ACKs 1, 2, 3. Στο 2t)12(tt ο αποστολέας λήγει και στέλνει ξανά 1, 2, 3. Στο 3t ο παραλήπτης λαμβάνει τα διπλότυπα και επιβεβαιώνει ξανά 1, 2, 3. Στο 4t ο αποστολέας λαμβάνει τα ACK που έστειλε ο παραλήπτης στο 1t και προωθεί το παράθυρό του σε 4, 5, 6.

Στις 5t ο αποστολέας λαμβάνει τα ACKs 1, 2, 3 ο δέκτης που αποστέλλεται σε 2t. Αυτά τα ACK βρίσκονται έξω από το παράθυρό του .

- Με το GBN, είναι δυνατό για τον αποστολέα να λάβει ένα ACK για ένα πακέτο εκτός του τρεχόντος παραθύρου. **[ΣΩΣΤΟ]**
- Το πρωτόκολλο εναλλασσόμενων bit είναι το ίδιο με το πρωτόκολλο SR με μέγεθος παραθύρου αποστολέα και παραλήπτη 1. **[ΣΩΣΤΟ]**
- Το πρωτόκολλο εναλλασσόμενων bit είναι το ίδιο με το πρωτόκολλο GBN με μέγεθος παραθύρου αποστολέα και παραλήπτη 1. **[ΣΩΣΤΟ]**

με μέγεθος παραθύρου 1, τα SR, GBN και το πρωτόκολλο εναλλασσόμενου bit είναι λειτουργικά ισοδύναμα. Το μέγεθος παραθύρου 1 αποκλείει τη δυνατότητα πακέτων εκτός σειράς (εντός του παραθύρου). Ένα αθροιστικό ACK είναι απλώς ένα συνηθισμένο ACK σε αυτήν την περίπτωση, καθώς μπορεί να αναφέρεται μόνο στο μεμονωμένο πακέτο μέσα στο παράθυρο

Κεφ 4 απαντήσεις στις επαναληπτικές ερωτήσεις βιβλίου

1. Το όνομα ενός πακέτου επιπέδου μεταφοράς είναι τμήμα και ότι το όνομα ενός πακέτου επιπέδου σύνδεσης είναι πλαίσιο. Ποιο είναι το όνομα ενός πακέτου επιπέδου δικτύου; Θυμηθείτε ότι τόσο οι δρομολογητές όσο και οι διακόπτες επιπέδου σύνδεσης ονομάζονται μεταγωγείς πακέτων. Ποια είναι η θεμελιώδης διαφορά μεταξύ ενός δρομολογητή και ενός ΜΕΤΑΓΩΓΕΑ επιπέδου ζευξης;

4. . Ποιος είναι ο ρόλος του πίνακα προώθησης εντός ενός δρομολογητή;

Ο ρόλος του πίνακα προώθησης μέσα σε έναν δρομολογητή είναι να κρατά καταχωρήσεις για να προσδιορίσει τη διεπαφή εξερχόμενης σύνδεσης στην οποία θα προωθηθεί ένα πακέτο που φτάνει μέσω του υφάσματος μεταγωγής

5.Είπαμε ότι το μοντέλο υπηρεσίας ενός επιπέδου δικτύου «καθορίζει τα χαρακτηριστικά του

μεταφορά από άκρο σε άκρο πακέτων μεταξύ κεντρικών υπολογιστών αποστολής και λήψης.» Ποιο είναι το μοντέλο υπηρεσίας του επιπέδου δικτύου του Διαδικτύου; Ποιες εγγυήσεις παρέχονται από το μοντέλο υπηρεσιών του Διαδικτύου σχετικά με την παράδοση δεδομένων από κεντρικό υπολογιστή σε κεντρικό υπολογιστή;

ο μοντέλο υπηρεσίας του επιπέδου δικτύου του Διαδικτύου είναι best-effort service. Με αυτό το μοντέλο υπηρεσίας, δεν υπάρχει καμία εγγύηση ότι τα πακέτα θα παραληφθούν με τη σειρά με την οποία στάλθηκαν, καμία εγγύηση για την τελική παράδοσή τους, καμία εγγύηση για την καθυστέρηση από άκρο σε άκρο και καμία εγγύηση ελάχιστου εύρους ζώνης.

9. Ας υποθέσουμε ότι ένα πακέτο που φτάνει ταιριάζει με δύο ή περισσότερες καταχωρήσεις στον πίνακα προώθησης ενός δρομολογητή. Με την παραδοσιακή προώθηση βάσει προορισμού, ποιος κανόνας εφαρμόζει ένας δρομολογητής για να προσδιορίσει ποιοι από αυτούς τους κανόνες θα πρέπει να εφαρμοστούν για τον προσδιορισμό της θύρας εξόδου στην οποία πρέπει να μεταφερθεί το πακέτο που φτάνει

A router uses longest prefix matching to determine which link interface a packet will be forwarded to if the packet's destination address matches two or more entries in the forwarding table. That is, the packet will be forwarded to the link interface that has the longest prefix match with the packet's destination.

11.Περιγράψτε πώς μπορεί να συμβεί απώλεια πακέτων στις θύρες εισόδου. Περιγράψτε πώς μπορεί να εξλειφθεί η απώλεια πακέτων στις θύρες εισόδου (χωρίς τη χρήση άπειρων buffers).

If the rate at which packets arrive to the fabric exceeds switching fabric rate, then packets will need to queue at the input ports. If this rate mismatch persists, the queues will get larger and larger and eventually overflow the input port buffers, causing packet loss. Packet loss can be eliminated if the switching fabric speed is at least n times as fast as the input line speed, where n is the number of input ports.

12. Περιγράψτε πώς μπορεί να συμβεί απώλεια πακέτων στις θύρες εξόδου. Μπορεί αυτή η απώλεια να αποτραπεί αυξάνοντας την ταχύτητα του υφάσματος του διακόπτη;

Assuming input and output line speeds are the same, packet loss can still occur if the rate at which packets arrive to a single output port exceeds the line speed. If this rate mismatch persists, the queues will get larger and larger and eventually overflow the output port buffers, causing packet loss. Note that increasing switch fabric speed cannot prevent this problem from occurring.

18. Ποιο πεδίο στην κεφαλίδα IP μπορεί να χρησιμοποιηθεί για να διασφαλιστεί ότι ένα πακέτο προωθείται

Time-to-live

21. Οι δρομολογητές έχουν διευθύνσεις IP; Αν ναι, πόσα;

Yes. They have one address for each interface

Κεφ 5 απαντήσεις στις επαναληπτικές ερωτήσεις βιβλίου

19 . Κατονομάστε 4 διαφορετικούς τύπους ICMP:

- Echo reply (to ping), type 0, code 0
- Destination network unreachable, type 3 code 0
- Destination host unreachable, type 3, code 1.
- Source quench (congestion control), type 4 code 0

20. Ποιοι δύο τύποι μηνυμάτων ICMP λαμβάνονται κατά την εκτέλεση του κεντρικού υπολογιστή αποστολής το πρόγραμμα Traceroute ;

- ICMP warning message (type 11 code 0) and a
- destination port unreachable ICMP message (type 3 code 3).

Κεφ 6 απαντήσεις στις επαναληπτικές ερωτήσεις βιβλίου

9. Πόσο μεγάλος είναι ο χώρος διευθύνσεων MAC; Ο χώρος διευθύνσεων IPv4;

- 2^{48} MAC addresses
- 2^{32} IPv4 addresses

10. Ας υποθέσουμε ότι οι κόμβοι A, B και C συνδέονται ο καθένας στο ίδιο LAN

εκπομπής (μέσω των προσαρμογέων τους). Εάν ο Α στείλει χιλιάδες datagrams IP στο Β με κάθε πλαίσιο απομόνωσης ενθυλάκωσης που απευθύνεται στη διεύθυνση MAC του Β, ο προσαρμογέας του C θα επεξεργαστεί αυτά τα πλαίσια; Εάν ναι, ο προσαρμογέας του C θα περάσει τα datagrams IP σε αυτά τα πλαίσια στο επίπεδο δικτύου C; Πώς θα άλλαζαν οι απαντήσεις σας εάν ο Α στείλει καρέ με τη διεύθυνση εκπομπής MAC;

C's adapter will process the frames, but the adapter will not pass the datagrams up the protocol stack. If the LAN broadcast address is used, then C's adapter will both process the frames and pass the datagrams up the protocol stack

11. Γιατί αποστέλλεται ένα ερώτημα ARP μέσα σε ένα πλαίσιο εκπομπής; Γιατί είναι ένα ARP η απάντηση στάλθηκε μέσα σε ένα πλαίσιο με μια συγκεκριμένη διεύθυνση MAC προορισμού;

An ARP query is sent in a broadcast frame because the querying host does not which adapter address corresponds to the IP address in question. For the response, the sending node knows the adapter address to which the response should be sent, so there is no need to send a broadcast frame (which would have to be processed by all the other nodes on the LAN).

ΘΕΜΑ 1°

(1.5 μονάδα) Τι είναι ένας προσωρινός αποθηκευτικός χώρος ιστού (Web cache) (ή πληρεξούσιος εξυπηρετήτης (proxy server)); Πως λειτουργεί; Η Web cache είναι πελάτης ή εξυπηρετήτης; Για ποιούς λόγους έχει εξαπλωθεί το Web Caching; Τι είναι η GET υπό συνθήκη και πως λειτουργεί;

ΤΑ ΘΕΜΑΤΑ ΕΠΙΣΤΡΕΦΟΝΤΑΙ ΜΑΖΙ ΜΕ ΤΟ ΓΡΑΠΤΟ!!!

ΘΕΜΑ 1°

(1.5 μονάδα) Τι είναι ένας προσωρινός αποθηκευτικός χώρος ιστού (Web cache) (ή πληρεξούσιος εξυπηρετήτης (proxy server)); Πως λειτουργεί; Η Web cache είναι πελάτης ή εξυπηρετήτης; Για ποιούς λόγους έχει εξαπλωθεί το Web Caching; Τι είναι η GET υπό συνθήκη και πως λειτουργεί;

ΘΕΜΑ 2°

α) (0.5 μονάδα) Τι είναι διαλύσιμο ACK στο TCP πρωτόκολλο;

β) (1 μονάδα) Ποιά είναι ενέργεια ενός παραλήπτη TCP στο συμβάν «Αφίξη ενός τμήματος που μερικώς ή πλήρως συμπληρώνει το χάσμα στα ληφθέντα δεδομένα»;

γ) (1.5 μονάδα) Χαρακτηρίστε κάθε μία από τις παρακάτω προτάσεις σαν Σωστή ή Λάθος και αιτιολογήστε επιμελώς την απάντησή σας:

1. Το UDP θεωρείται connectionless πρωτόκολλο διότι δεν εγγράφει την παράδοση των πακέτων.
2. Τα παράθυρα συμμόρφησης & λήψης (cwnd/rwnd) υπολογίζονται από τον παραλήπτη του TCP.
3. Η επικεφαλίδα TCP διαθέτει πεδίο για την ενιμάωση σχετικά με το παράθυρο λήψης (rwnd).
4. Το TCP Reno αποφεύγει τους χαμηλούς ρυθμούς μετάδοσης της αργής εκκίνησης χάρη στο μηχανισμό «ταχείας επαναμετάδοσης».

ΘΕΜΑ 3°

α) (1.5 μονάδα) Αν ο υπολογιστής προορισμού έχει προσδιορίσει ότι τρία δεδομενογράμματα/πακέτα ανήκουν στο ίδιο μεγαλύτερο δεδομένογράμμα, ποια πεδία του IP δεδομενογράμματος εξετάζει για να καθορίσει την σειρά τους, δηλαδή ποιο προηγείται των άλλων δύο, ποιο έπεται των άλλων δύο και ποιο είναι στο μέσον; Κατόπιν, ποια πεδία εξετάζει και τι πρέπει να ισχύει ώστε τα τρία παραπάνω δεδομενογράμματα να είναι συνεχόμενα;

β) (1 μονάδα) Λοού όλα τα δεδομενογράμματα (πακέτα) που φτάνουν σε έναν δρομολογητή NAT (Network Address Translation) από το WAN/Internet έχουν την ίδια διεύθυνση προορισμού IP, πως ξέρει ο δρομολογητής τον εσωτερικό υπολογιστή στον οποίο πρέπει να προσεβήσεται ένα συγκεκριμένο δεδομένογράμμα; Περιγράψτε εν συντομία την διαδικασία.

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 εξυπηρετές ταχυδρομείου στους εξυπηρετές 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 εξυπηρετής 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 θεωρείται συνδεσμικό, καθώς δυο διεργασίες πρέπει να κάνουμε μια “χειραψία” μεταξύ τους πριν αρχίσουν να στέλνουν δεδομένα ή 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 A που επικοινωνεί με μια διεργασία στον υπολογιστή B, τότε η A μπορεί να στέλνει δεδομένα εφαρμογής στη B ταυτόχρονα όσο η B μπορεί να στέλνει δεδομένα εφαρμογής στην A.

Τί, πότε και γιατί καλεί την διαδικασία ταχείας αναμετάδοσης το πρωτόκολλο TCP;

Όταν συμβεί απώλεια πακέτων ο αποστολέας το καταλαβαίνει από 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 εξυπηρετή) 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 A στο τμήμα του είναι ο αριθμός ακολουθίας του επόμενου byte που περιμένει ο υπολογιστής A από τον υπολογιστή B.

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 από 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 διπλασιάζει 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 (γемίζει) 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 ποιο πρωτόκολλο επιπέδου μεταφοράς πρέπει να παραδοθεί το δεδομένογραμμα 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 δεδομένογραμμα 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 δεδομένογραμμα 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 απάντηση 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 δένδρογραμμάτων 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 δεδομένογραμμα 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 ring 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 να 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 εξυπηρετητή – 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 διαδικτυακά παιχνίδια η απαίτηση μας είναι να έχουμε ασφάλεια ή χρονισμό; Κλπ.
 - Τα 4 requirements + τι είναι το κάθε ένα και παραδείγματα 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
Εγγραφα 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 5^ο 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 ** Αντιστοίχιση. Σελ 96.

Εφαρμογή	Πρωτόκολλο εφαρμογής	Υποκείμενο Πρωτόκολλο μεταφοράς
Ηλεκτρονικό ταχυδρομείο	SMTP [RFC 2821]	TCP
e-mail		
Απομακρυσμένη προσπέλαση	Telnet [RFC 854]	TCP
τερματικού		
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 *

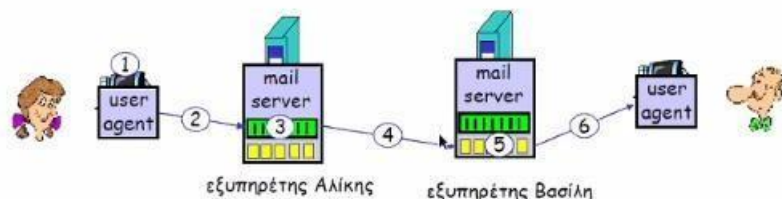
- Τα πάντα.
- Δεν χρησιμοποιείται το UDP
- Τι είναι καταστατικό και τι ακαταστατικό. Ποια πρωτόκολλα είναι ακαταστατικά και ποια ακαταστατικά. ** Σελ. 101-102 (4^{ου} επιπέδου είναι η σύνδεση παραμένουσα – μη παραμενουσα)

10. HTTP Connections **

- Τι είναι παραμένουσα και τι μη παραμενουσα. Σελ. 101-102 (4^{ου} 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 διαβάσει 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.

Σενάριο: Η Αλίκη στέλνει μήνυμα στον Βασίλη

- 1) Η Αλίκη χρησιμοποιεί πράκτορα χρήστη (user agent-UA) για τη σύνθεση του μηνύματος "προς" vassilis@di.uoa.gr
- 2) Ο πράκτορας της Αλίκης στέλνει το μήνυμα στον εξυπηρετή ταχυδρομείου της, το μήνυμα τοποθετείται στην ουρά μηνυμάτων
- 3) Η πλευρά του πελάτη του SMTP ανοίγει TCP σύνδεση με τον εξυπηρετή ταχυδρομείου του Βασίλη
- 4) Ο πελάτης SMTP στέλνει το μήνυμα της Αλίκης πάνω από τη σύνδεση TCP
- 5) Ο εξυπηρετής ταχυδρομείου του Βασίλη τοποθετεί το μήνυμα στην ταχυδρομική θυρίδα του Βασίλη
- 6) Ο Βασίλη χρησιμοποιεί το δικό του πράκτορα για να το διαβάσει



- Ερώτηση Στα 2,4,6 χρησιμοποιούμε 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 κεντριοποιημένο;
- 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.

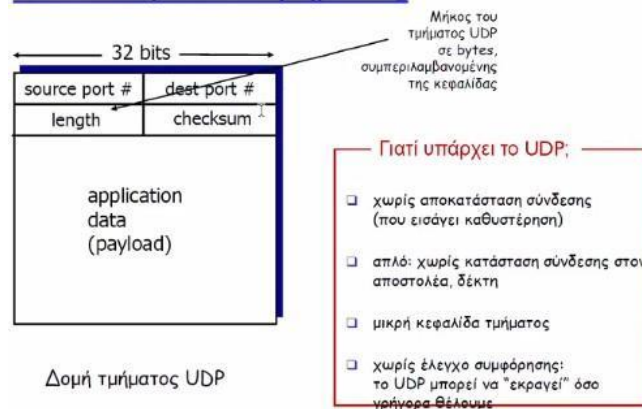
Chapter 3 : Transport Layer

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 4^ο 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; ***
 - ι. Ναι μπορεί να παρέχει αξιόπιστη μεταφορά αλλά αυτό είναι στο χέρι του προγραμματιστή στο 5^ο 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; **
 - ι. Όχι. Αν χαθεί, χάθηκε.
 - Πως μπορούμε σε ένα streaming να έχουμε ανοχή στις απώλειες;
 - Best effort

5. UDP: κεφαλίδα τμήματος

UDP: κεφαλίδα τμήματος



- Σε bytes, όχι σε bits.
6. Principles of Reliable Data Transfer σελ 206
- Τι είναι αξιοπιστία, τι προϋποθέσεις 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 2^{ου} επιπέδου και είδε ότι δεν έχει λάθη. Αφού δεν έχει λάθη στο 2^ο επίπεδο, μπορεί να έχει λάθη στο 4^ο 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 μετριοούνται 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 είναι 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;
 - Σελ 244
 - Αναλίστο = χωρίς χαμένα bits
 - Χωρίς κενά = τα στέλνει ταξινομημένα
 - Χωρίς διπλότυπα ACK = Όχι αναμετάδοση
 - Χρησιμοποιεί ένα χρονομετρητή

19. Σενάρια αναμεταδόσεων TCP ****

- Σενάριο συσσωρευτικού ACK
 - Αφού δεν πήρα το ACK 100 και πήρα το ACK 120, θα κάνω αναμετάδοση;
 - 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.
 - Συνδυασμός seq num + data bytes.

Παραγωγή TCP ACK [RFC 1122, RFC 2581]

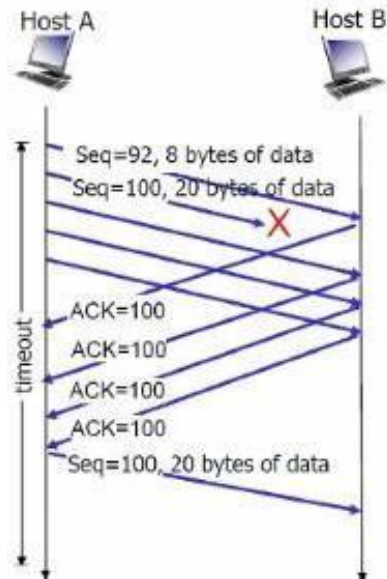
Συμβάν στο δέκτη	Ενέργεια δέκτη TCP
Άφιξη τμήματος σε σειρά με αναμενόμενο # ακολουθίας. Όλα τα δεδομένα μέχρι τον αναμενόμενο # ακολουθίας έχουν επιβεβαιωθεί	Καθυστερημένο ACK. Αναμονή 500ms για το επόμενο τμήμα. Αν όχι επόμενο τμήμα στείλε ACK
Άφιξη τμήματος σε σειρά με αναμενόμενο # ακολουθίας. Ένα 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 <i>duplicate ACK</i> 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 ***
 - 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) Δουλεύει Selective Repeat γιατί ξέρει ακριβώς ποιο θέλει να ξανά στείλει. Σελ 252.

22. TCP Flow Control σελ 252-254 **

- Υπηρεσία ταιριάσματος ταχύτητας ταιρίασμα. 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 είναι 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 πάει απευθείας σε close.

25. Principles of congestion control

- Διαφορά ελέγχου ροής με ελέγχου συμφώρησης.

26. TCP Congestion Control ***** PERMA SOS

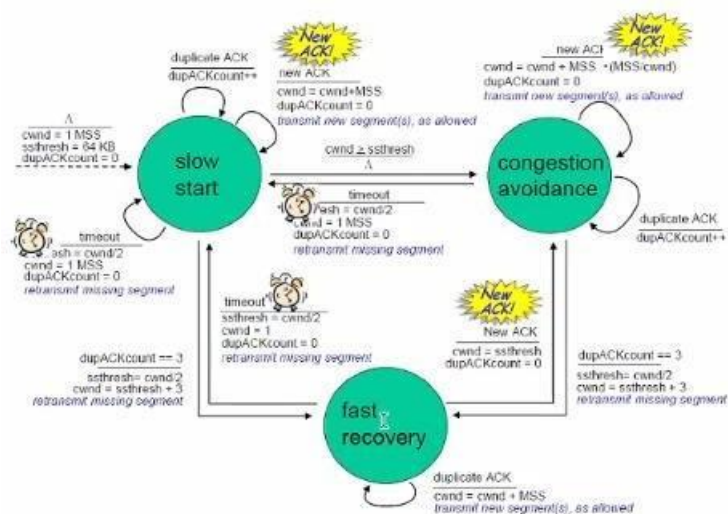
- Additive increase, multiplicative decrease.
- Σελ 269 3 ερωτήσεις.
- Τι είναι το cwnd; Πως καθορίζεται; ****

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

- Μαθηματικός τύπος 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 $\frac{1}{2}$, 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 πάω;
 - a) Στο slow start.
 - ii. Είμαστε σε κατάσταση fast recovery και παίρνω ACK. Σε ποια κατάσταση θα πάω;
 - a) Στο congestion avoidance.



iii.

- Ποια είναι η σύγκριση ανάμεσα στην ταχεία ανάκαμψη και στην ταχεία αναμετάδοση; Ομοιότητες και διαφορές. (το ταχεία δεν παροτρύνει 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.

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 από 1 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

29.

Chapter 4 : The Network Layer: Data Plane

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

Κατάτμηση και Ανασύνθεση του IP

Παράδειγμα

- 4000 byte datagram
- MTU = 1500 bytes

1480 bytes
στο πεδίο δεδομένων
(data field)

Μετατόπιση (offset) =
 $1480/8$

length	ID	fragflag	offset
=4000	=x	=0	=0

Ένα μεγάλο datagram γίνεται
πολλά μικρότερα datagrams

length	ID	fragflag	offset
=1500	=x	=1	=0

length	ID	fragflag	offset
=1500	=x	=1	=185

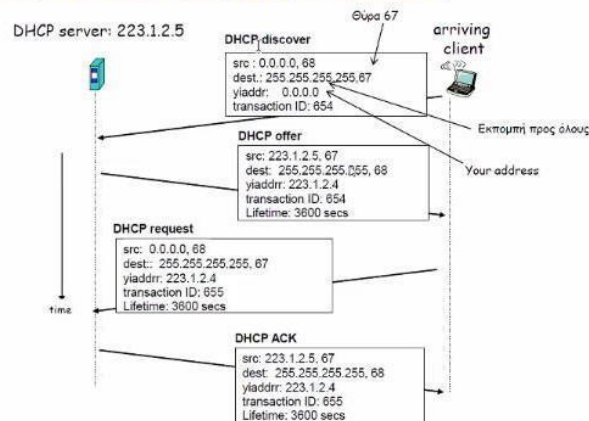
length	ID	fragflag	offset
=1040	=x	=0	=370

- Το 1040 από που βγήκε και γιατί 1500;
 - Τα καθαρά data είναι length value - 40 bytes (20IP + 20TCP/αλλιώς + 8UDP)
- Τι είναι τα fragflag, offset

5. DHCP **** σελ 342

- Πως λειτουργεί; Πως είναι η διαδικασία για να πάρω IP Address;
- Επισκόπηση DHCP

Σενάριο πελάτη-εξυπηρετή DHCP



- Από το 5^ο επίπεδο έρχεται το DHCP Discover

6. NAT σελ 345-347

- Τι είναι και πως λειτουργεί;

Chapter 5: The Network Layer: Control Pane

- 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 3^{ου} επιπέδου με τις διευθυνσιοδοτήσεις 2^{ου} επιπέδου.
 - Τι μαθαίνουμε μέσω του ARP;
 - Σύγκριση ARP – DNS ****
 - ι. 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 3^ο και σε 2^ο επίπεδο. Δεν είναι ξεκάθαρα του 2^{ου} επειδή παίρνει πληροφορίες και από τα δύο επίπεδα.
 - Πως μαθαίνουμε την MAC διεύθυνση του άλλου;
 - ι. Εξήγηση στο τετράδιο. Broadcast – Unicast.
18. Routing to another LAN όλες οι υποθέσεις
- Routing to Another LAN σελ. 473 ***
 - ι. Πως θα παει στο επόμενο subnet;
 - Αν ο B είναι ένας server, με ποιο πρωτόκολλο θα μάθουμε την IP του;
 - ι. Με DNS θα μάθω την IP του και μετά μέσω του ARP θα μάθουμε την MAC του και να μεταφερθεί το πακέτο.
 - 3^η υπόθεση. (πως;) Με ποιο πρωτόκολλο μαθαίνει το gateway; ΔΕΝ χρησιμοποιείται static routing.
 - ι. Με το DHCP θα μάθουμε ποιος είναι ο router πρώτου hop.
 - 4^η υπόθεση. (πως;)
 - ι. Με ARP θα μάθουμε την MAC.
19. Ethernet σελ 475
- Είναι ελεύθερο συγκρούσεων. Πως;
20. Δομή πλαισίου
- Σύγκριση 3^{ου} επιπέδου με 2^{ου} 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 δίνει 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 οκεί, 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 ζεύξης 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 εξυπηρετής (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 να 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.

Εφαρμογή	Απώλεια δεδομένων	Ρυθμαπόδοση	Ευαισθησία ως προς το χρόνο
Μεταφορά αρχείου	όχι απώλειες	ελαστική	όχι
e-mail	όχι απώλειες	ελαστική	όχι
Έγγραφο 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

10.

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.

Εφαρμογή	Πρωτόκολλο εφαρμογής	Υποκείμενο Πρωτόκολλο μεταφοράς
Ηλεκτρονικό ταχυδρομείο e-mail	SMTP [RFC 2821]	TCP
Απομακρυσμένη προσπέλαση τερματικού Web	Telnet [RFC 854]	TCP
	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, ιδιοπαγές (π.χ. Skype)	TCP ή UDP

12.

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

13. HTTP

- Το HTTP είναι πρωτόκολλο 5^{ου} 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.
- Το HTTP χρησιμοποιεί TCP ως πρωτόκολλο μεταφοράς. Ο πελάτης εκκινεί πρώτα μία σύνδεση TCP με τον σερβερ και ανταλλάσσουν τα δεδομένα μέσω των sockets.
- 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.
- Το HTTP χρησιμοποιεί την αρχιτεκτονική εφαρμογής Client-Server.
- Το HTTP δεν ασχολείται με τα χαμένα δεδομένα. Είναι ευθύνη του TCP.
- Τι είναι καταστατικό και τι ακαταστατικό. Ποια πρωτόκολλα είναι ακαταστατικά και ποια ακαταστατικά.

14. Τι είναι παραμένονα και τι μη-παραμένονα;

- 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.
- 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 εγκαθίδρυση 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 ιδιαιτερότητας 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 μέσω 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 αντικείμενο, τότε 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 σέρβερ 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. Όταν 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

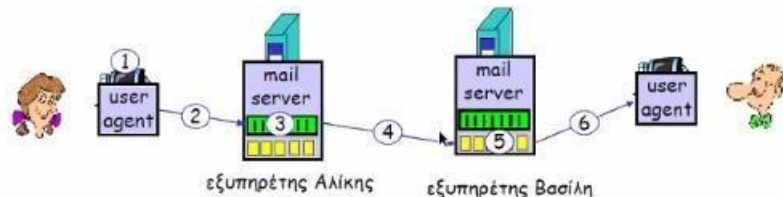
- a. Ποια είναι τα τρία κύρια συστατικά μέρη και τι είναι το κάθε ένα;
 - i. Πράκτορες χρήστη (user agents)
 - 1. Οι πράκτορες χρήστη είναι οι εφαρμογές που χρησιμοποιούμε για να διαβάζουμε, να απαντάμε, να προωθούμε, να αποθηκεύουμε και να συνδέουμε μηνυματα.
 - ii. Εξυπηρετές ταχυδρομείου (mail servers)
 - 1. Οι mail servers έχουν ταχυδρομική θυρίδα για τον κάθε εγγεγραμμένο χρήστη.
 - 2. Όταν στείλουμε ένα mail, το παίρνει ο εξυπηρετητής ταχυδρομείου, το βάζει σε μία ουρά και έχει status to-be-send. Σε αυτή την ουρά αρχίζει και στέλνει τα mails στους άλλους mail servers.(Σε περίπτωση που δεν μπορεί να το στείλει επανατοποθετείται στην ουρα.)
 - 3. Ο κάθε εξυπηρετητής ταχυδρομείου όταν στέλνει είναι πελάτης SMTP και όταν δέχεται είναι εξυπηρετητής SMTP.
 - 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 εντολή 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.

Σενάριο: Η Αλίκη στέλνει μήνυμα στον Βασίλη

- 1) Η Αλίκη χρησιμοποιεί πράκτορα χρήστη (user agent-UA) για τη σύνθεση του μηνύματος "προς" vassilis@di.uoa.gr
- 2) Ο πράκτορας της Αλίκης στέλνει το μήνυμα στον εξυπηρετή ταχυδρομείου της, το μήνυμα τοποθετείται στην ουρά μηνυμάτων
- 3) Η πλευρά του πελάτη του SMTP ανοίγει TCP σύνδεση με τον εξυπηρετή ταχυδρομείου του Βασίλη
- 4) Ο πελάτης SMTP στέλνει το μήνυμα της Αλίκης πάνω από τη σύνδεση TCP
- 5) Ο εξυπηρετής ταχυδρομείου του Βασίλη τοποθετεί το μήνυμα στην ταχυδρομική θυρίδα του Βασίλη
- 6) Ο Βασίλη χρησιμοποιεί το δικό του πράκτορα για να το διαβάσει



c.

- i. Στα 2,4,6 χρησιμοποιούμε 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

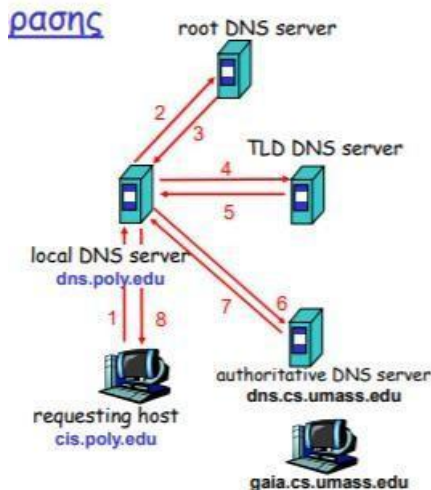
mail server και μπορούμε να βλέπουμε τα mails μας σε οποιοδήποτε υπολογιστή.

- 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 αντιστοίχιση 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 κεντροποιημένη 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 κεντροποιημένη βάση;
 - i. Υπάρχει το ρίσκο αν καταρρεύσει ο σέρβερ 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, de, uk). Οι TLD παρέχουν τις διευθύνσεις IP για αυθεντικούς εξυπηρέτες 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 κατόπιν 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.
- Όλα τα ερωτήματα μπορούν να είναι και επαναληπτικό ή αναδρομικό.
 - Αναδρομικό είναι όταν ζητάς από κάποιον να βρει την αντιστοίχιση εκ μέρους του.
 - Επαναληπτικό είναι όταν όλες οι αποκρίσεις επιστρέφονται απευθείας σε αυτόν που κάνει την δουλειά της αναδρομής.
- h. Τι είναι το DNS caching;
- 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;
- 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 PUSH τραβάω δεδομένα για να μην χρειάζεται να τραβάω κάθε λίγο.
- j. DNS Records

RR format: (name, value, type, ttl)

□ Type=A

- name είναι το όνομα του υπολογιστή
- value είναι η διεύθυνση IP

□ Type=CNAME

- name είναι ψευδώνυμο για κάποιο κανονικό (πραγματικό) όνομα
- www.ibm.com είναι στην πραγματικότητα servereast.backup2.ibm.com
- value είναι το κανονικό όνομα

□ Type=NS

- name είναι τομέας (domain) (π.χ., foo.com)
- value είναι το όνομα υπολογιστή (hostname) του αυθεντικού εξυπηρετή ονομάτων για αυτόν τον τομέα

□ Type=MX

- value είναι το όνομα του εξυπηρετή mail που σχετίζεται με το name

i.

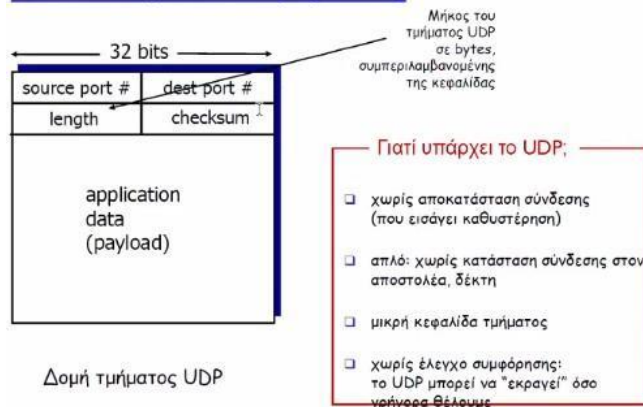
Chapter 3: Transport Layer

1. Τι παρέχει ένα πρωτόκολλο μεταφοράς;
 - a. Υπάρχει μία λογική σύνδεση ανάμεσα στις διεργασίες του 5^{ου} 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 3^ο επίπεδο ποια είναι η IP, ανεβαίνει στο 4^ο επίπεδο και βλέπει τον συνδυασμό του IP-Port number όπου έχει ως αποτέλεσμα το socket και ξέρει σε ποιον απευθύνεται.
4. Στο 4^ο 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 συνεχής 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 5^ο 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.

UDP: κεφαλίδα τμήματος



- 6.
7. Τι είναι αξιοπιστία και τι προϋποθέσεις έχει;
- a. Το 4^ο 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 4^{ου} 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 2^{ου} επιπέδου και είδε ότι δεν έχει λάθη. Αφού δεν έχει λάθη στο 2^ο επίπεδο, μπορεί να έχει λάθη στο 4^ο 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 κάποιο 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 σταλούν 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 ΝΑΚ. Αυτό που θα μου έστελνε ο

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

14. Rdt3.0

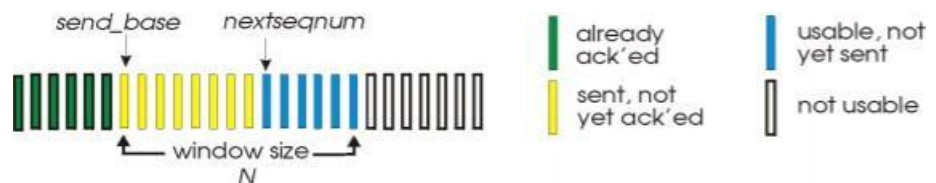
- a. Ο αποστολέας περιμένει για ένα χρονικό διάστημα για το ACK. Αν δεν ληφθεί ACK σε αυτό το διάστημα τότε αναμεταδίδει. Αν απλά καθυστέρησε τότε οι αναμεταδόσεις θα είναι διπλές (duplicate) αλλά θα αντιμετωπιστεί από το sequence number. Αφού θα χρειαστεί χρονομετρητής για την επαναμετάδοση τότε ο αποστολέας 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.

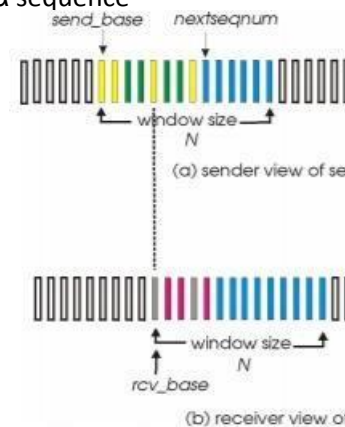


- iii.
- iv. Κάθε φορά που παίρνω τα ACKs για το base και για τα επόμενα, το window προχωράει προς τα δεξιά. Μέσα στο window υπάρχουν και τα πακέτα τα οποία είναι έτοιμα προς αποστολή αλλά δεν τα έχω στείλει. Μετά από το παράθυρο είναι τα πακέτα που δεν είναι έτοιμα προς αποστολή.
- v. Όταν παίρνω ένα 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;

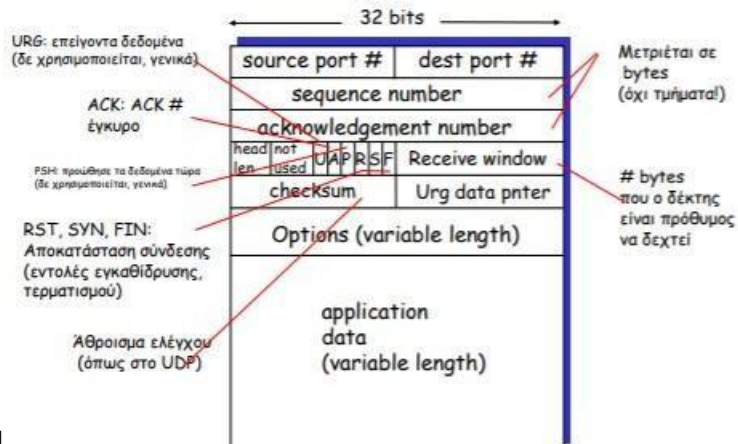
- i. Το Go-back-N έχει ένα χρονομετρητή ενώ το Selective Repeat έχει ένα χρονομετρητή για το κάθε πακέτο, αφού μόνο ένα πακέτο θα μεταδοθεί κατά την λήξη του χρόνου.

17. TCP

- a. Είναι συνδεδεσμένο επειδή πρέπει να γίνει πρώτα η τριμερής χειραψία
- b. Η σύνδεση είναι αμφίδρομη. Δηλαδή ο A και ο B 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

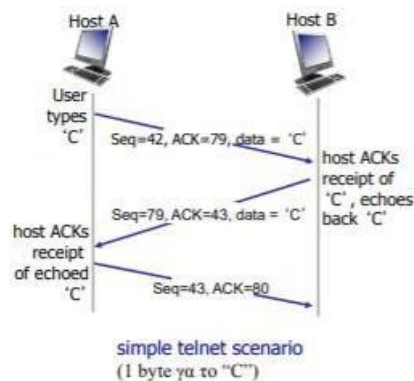
μέσω του MSS.

- f. Έχουμε buffers για αποστολή και λήψη.



18.1..

- 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 μετριοούνται 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 μετρίεται 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 έγκαιρα.

21. Αξιόπιστη μεταφορά δεδομένων του TCP

- a. Το TCP δημιουργεί μία υπηρεσία αξιόπιστης μεταφοράς δεδομένων πάνω από την αναξιόπιστη υπηρεσία βέλτιστης προσπάθειας του IP. Χρησιμοποιεί τμήματα σε διοχέτευση 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.

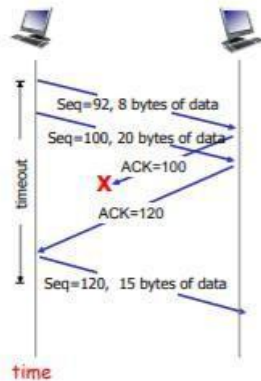
22. Γεγονότα του αποστολέα TCP

- 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 προκάλεσε 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 πήρα το ACK 120, θα κάνω αναμετάδοση;



a. Σενάριο συσσωρευτικού ACK

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 <i>duplicate ACK</i> 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

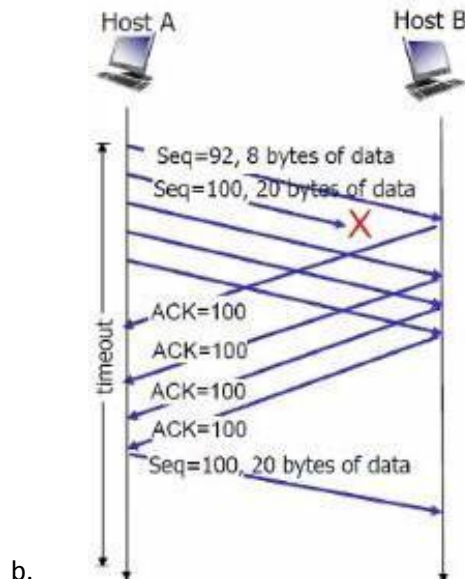
25.2...

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

26. Ταχεία αναμετάδοση

a. Εάν 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 5^ο 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 5^{ου} 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 δεδομένογραμμα IP που περιέχει το τμήμα TCP SYN φτάσει στον υπολογιστή εξυπηρέτη, ο εξυπηρέτης εξάγει το τμήμα TCP SYN από το δεδομένογραμμα, 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 σύνδεσης SYNACK, ο πελάτης δεσμεύει επίσης buffers και μεταβλητές στην σύνδεση. Ο υπολογιστής πελάτη 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 κλείσει δεν θα πάει 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, τότε 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 μέσω 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 αντιμετωπιστεί η συμφόρηση. 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. Εάν υπάρξει ένα συμβάν απώλειας λόγω 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. Εάν ανιχνευθούν τρία διπλότυπα ACK, οπότε το TCP εκτελεί μία ταχεία επαναμετάδοση. Αφού ανιχνευθούν τρία διπλότυπα ACK και όχι timeout, πάλι 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. Εάν η τιμή της cwnd ισούται με ssthresh, η αργή εκκίνηση τελειώνει και το TCP αλλάζει από αργή εκκίνηση σε αποφυγή συμφόρησης.
 - iv. Παράδειγμα

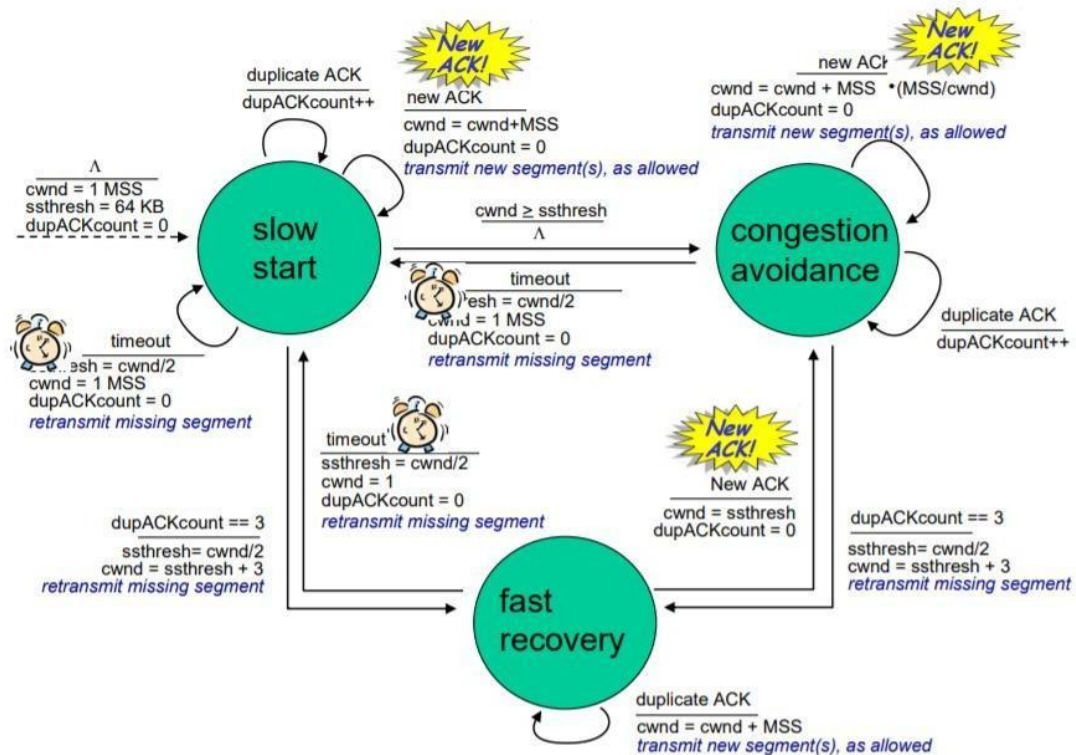
1. Την χρονική στιγμή 1 ξεκινάμε με 1MSS. Εφόσον παίρνουμε RTT, γίνεται 2, 4, 8 και μετά θα έπρεπε να γίνει 16 αλλά στην χρονική

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 κατά 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 $\frac{1}{2}$ 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 συμφόρησης 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 σύγκριση 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 επαναμεταδώσει 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.

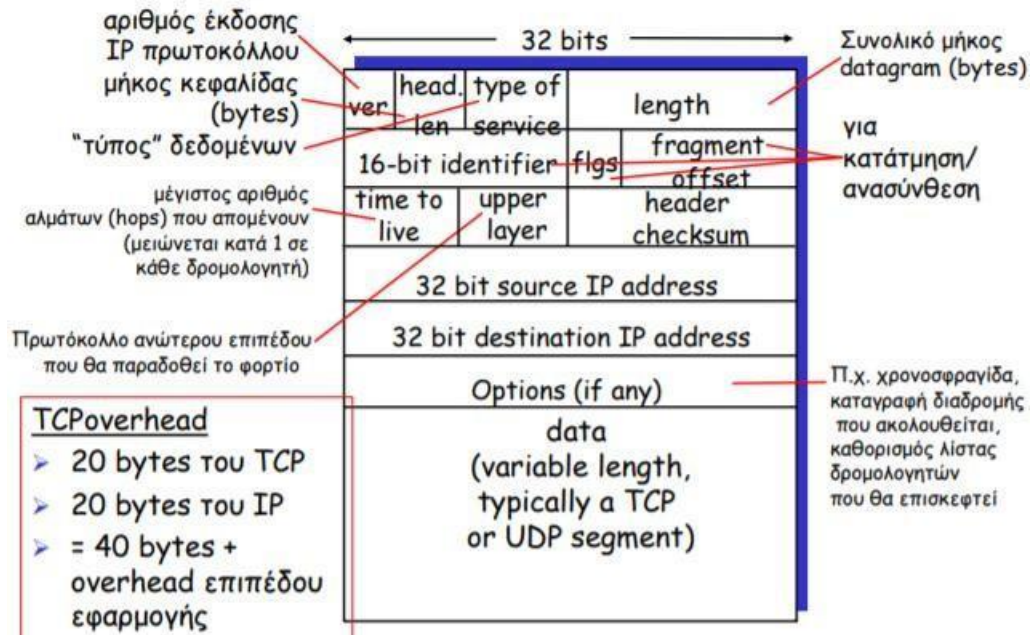
Κατάσταση	Συμβάν	Ενέργεια αποστολέα TCP	Σχόλια
Αργή Εκκίνηση Slow Start (SS)	Λήψη ACK για δεδομένα που δεν έχουν επιβεβαιωθεί προηγουμένως	$CongWin = CongWin + MSS$, If ($CongWin > Threshold$) θέσε κατάσταση σε «Αποφυγή Συμφόρησης»	Έχει ως αποτέλεσμα διπλασιασμό του CongWin σε κάθε RTT
Αποφυγή Συμφόρησης 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 από 1 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 διπλοτύπων ACK για το τμήμα η λήψη του οποίου επιβεβαιώθηκε	Τα CongWin και Threshold δεν αλλάζουν

37.

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.

Δομή IP datagram



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

Κατάτμηση και Ανασύνθεση του IP

Παράδειγμα

- 4000 byte datagram
- MTU = 1500 bytes

1480 bytes στο πεδίο δεδομένων (data field)

Μετατόπιση (offset) = $1480/8$

length	ID	fragflag	offset
=4000	=x	=0	=0

Ένα μεγάλο datagram γίνεται πολλά μικρότερα datagrams

length	ID	fragflag	offset
=1500	=x	=1	=0
=1500	=x	=1	=185
=1040	=x	=0	=370

- 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 αποδिकνύει 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 λόγω του περιορισμού που υπάρχει. Η ανασύνθεση των δεδεμενογραμμάτων γίνεται στον τελευταίο δρομολογητή.
5. DHCP
- a. Το πρωτόκολλο DHCP επιτρέπει σε έναν υπολογιστή να αποκτά 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 υπολογιστής που θέλει να πάρει πληροφορίες δικτύου. Κάθε υποδίκτυο έχει έναν εξυπηρέτη DHCP. Εάν 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 ενθυλακωμένο 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.
 - e.
6. 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 που 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 δεδομένογραμμα 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 δεδομένογραμμα 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 δεδομένογράφματος 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 αποστολέα για αναμετάδοση, 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 μεταδώσουν αλλά όχι ταυτόχρονα. (Ασύρματοι).
 - ii. Με full-duplex και οι δύο κόμβοι μπορούν να μεταδώσουν ταυτόχρονα.
5. Ανίχνευση σφαλμάτων
 - a. Στην ανίχνευση σφαλμάτων βάζουμε περισσότερα bits στο ήδη υπαρχών 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 αντιμετωπίζεται 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 αναβάλλει 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 $\{0,1,2,\dots,2^m-1\}$. Περιμένει για $K \cdot 512$ 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 κρέμεται 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.

- i. 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 3^ο και σε 2^ο επίπεδο. Δεν είναι ξεκάθαρα του 2^{ου} 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 τότε 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 B 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 B, καταχωρεί το ζεύγος του στον ARP πίνακα.

15. Σύγκριση ARP – DNS

- a. Αντιστοίχιση 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.

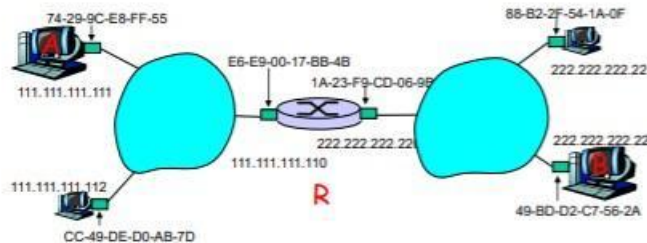
16. ARP – Έξω από το υποδίκτυο

- a. Ο A δημιουργεί datagram(3^{ου}) με τις source-dest IP.
- b. Ο A εγκυβοτίζει το datagram σε ένα πλαίσιο προσθέτοντας την MAC dest αυτή του router και MAC source του A.
- c. Το πλαίσιο φεύγει και φτάνει στον router. Αφαιρεί το 2^ο επίπεδο, κοιτάζει το 2^ο επίπεδο για την IP και διαβάζει ποια είναι η dest IP. Άρα παίρνει το πλαίσιο, αφαιρεί τις πληροφορίες του 2^{ου} 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 3^{ου} 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 2^{ου}, θα δει στο 3^ο ότι πρόκειται για την δικιά του IP και ανοίγει το πακέτο.

Διέλευση: στείλε το datagram από τον A στο B μέσω του R

- εστίασε στη διευθυνσιοδότηση - στο IP (datagram) και MAC επίπεδο (frame - πλαίσιο)
- υποθέτοντας πως ο A γνωρίζει τη διεύθυνση IP του B
- υποθέτοντας πως ο A γνωρίζει την IP διεύθυνση του δρομολογητή πρώτου άλματος, R (πώς;)
- υποθέτοντας πως ο A γνωρίζει τη MAC διεύθυνση του R (πώς;)



... .. π.χ. 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. 3^η υπόθεση. Με ποιο πρωτόκολλο μαθαίνει το gateway; (Δεν χρησιμοποιείται static routing.
 1. Με το DHCP θα μάθουμε ποιος είναι ο router πρώτου Hop.
- iii. 4^η 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 3^{ου} επιπέδου με 2^{ου} 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 τυχαίες προσπέλασης πρωτόκολλα αν δεν συμβεί σύγκρουση, έχει την εγγύηση ο αποστολέας ότι πήγε στον παραλήπτη. Αν έχει λάθη το 2^ο επίπεδο θα γίνει απόρριψη και δεν θα ανέβει στα πιο πάνω επίπεδα. Το 3^ο επίπεδο θα καταλάβει ότι δεν του έφτασε IP datagram, το 4^ο 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 μεταδώσω 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 χειραγώγηση των προσαρμογών.
 - ii. Αναξιόπιστο είναι γιατί ο προσαρμογέας λήψης δεν στέλνει ACK/NAK στον προσαρμογέα αποστολής. Άρα τα δεδομένα που απορρίφθηκαν ανακτώνται 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 3^{ου} επιπέδου.
 - ii. Τα switches είναι επιπέδου ζεύξης και εξετάζουν τις κεφαλίδες 2^{ου} επιπέδου.
 - b. Και τα δύο έχουν πίνακες προώθησης
 - i. Τα routers υπολογίζουν τους πίνακες χρησιμοποιώντας αλγορίθμους routing με βάση τις IP addresses.
 - ii. Τα switches μαθαίνουν μόνα τους και γεμίζουν τον πίνακα προώθησης χρησιμοποιώντας 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.

Quiz

Application Layer

5

SMTP is used to

- ☒ to transfer messages from one mail server to another
- ☐ to transfer messages from mail server to a user agent
- ☐ to define the format of message headers
- ☐ all of the above

Correct.

7

Local DNS name servers

- ☐ never cache resource records
- ☒ cache resource records, but discard them after a period of time that is on the order of a few days
- ☐ cache resource records and never discard them
- ☐ obtain resource records from Web caches

Correct.

3

It is possible for a mail client to send e-mail messages over HTTP rather than SMTP.

- ☒ True
- ☐ False

Correct.

7

With non-persistent connections between browser and origin server, it is possible for a single TCP segment to carry two distinct HTTP request messages.

☐ True

☒ False

Correct.

1

A server can use cookies to determine a user's postal address without the user's consent.

☐ True

☒ False

Correct.

Transport Layer

7

TCP applies fast retransmit to a segment when

☐ it estimates unusually large RTTs

☐ the segment's timer expires

☒ when it receives three ACKs for an earlier segment

☐ none of the above

Correct.

- 10 Over a TCP connection, suppose host A sends two segments to host B, host B sends an acknowledgement for each segment, the first acknowledgement is lost, but the second acknowledgement arrives before the timer for the first segment expires.

- ☐ Host A will retransmit the first segment
- ☐ Host A will retransmit the second segment
- ☐ Host A will retransmit both segments
- ☒ Host A will retransmit neither segments

Correct.

- 1 Consider an HTTP Web server using persistent connections. Suppose the server spawns a separate process for each client that connects to the server. Then each of these spawned processes will have different server port numbers.

- ☐ True
- ☒ False

Correct.

- 2 Host A is sending host B a large file over a TCP connection. Assume host B has no data to send A. Host B will not send acknowledgements to host A because host B cannot piggyback the acknowledgements on data.

- ☐ True
- ☒ False

Correct.

- 4 Suppose host A is sending a large file to host B over a TCP connection. If the sequence number for a segment of this connection is m , then the sequence number for the subsequent segment will necessarily be $m+1$.

- ☐ True
- ☒ False

Correct.

- 5 The TCP segment has a field in its header for `RcvWindow`.

- ☒ True
- ☐ False

Correct.

7 Suppose host A sends host B one segment with sequence number 38 and 4 bytes of data. Then in this same segment the acknowledgement number is necessarily 42.

☐ True

☒ False

Correct.

8 Suppose that host A wants to send data over TCP to host B, and host B wants to send data to host A over TCP. Two separate TCP connections - one for each direction - are needed.

☐ True

☒ False

Correct.

9 The MSS is the maximum size of a TCP segment including headers.

☐ True

☒ False

Correct.

10 In TCP, the acknowledgement number that a host puts in a segment is the sequence number of the next byte the host is expecting from the sender.

☒ True

☐ False

Correct.