Εικόνα 12.6

Βασικές κατηγορίες διακομιστών

Διακομιστές εκτυπώσεων	Διακομιστές εφαρμογών	Διακομιστές βάσεων δεδομένων	Διακομιστές αυθεντικοποίησης
			
Διαχειρίζονται όλες τις εργασίες εκτύπωσης για υπολογιστές πελάτες	Εξυπηρετούν ως αποθήκη λογισμικού εφαρμογών	Παρέχουν σε υπολογιστές πελάτες πρόσβαση σε βάσεις δεδομένων	Καταγράφουν τους χρήστες που συνδέονται στο δίκτυο
Διακομιστές αρχείων	**Διακομιστές ηλεκτρονικού ταχυδρομείου**	**Διακομιστές επικοινωνιών**	**Διακομιστές web/cloud**
			
Αποθηκεύουν και διαχειρίζονται αρχεία για χρήστες δικτύων	Επεξεργάζονται και παραδίδουν εισερχόμενα και εξερχόμενα μηνύματα ηλεκτρονικού ταχυδρομείου	Αναλαμβάνουν τον χειρισμό όλων των επικοινωνιών ανάμεσα στο δίκτυο και σε άλλα δίκτυα	Φιλοξενούν διαδικτυακούς τόπους, ώστε να τους διαθέτουν μέσω διαδικτύου

(Naypong/Fotolia· Julien Eichinger/Fotolia· Maksym Yemelyanov/Fotolia· Maksim Kabakou/Fotolia· Felix Jork/Fotolia· TAex/Fotolia· AG Visuell/Fotolia· Mariusz Prusaczyk/Fotolia)

κριμένης λειτουργίας, όπως ο χειρισμός του ηλεκτρονικού ταχυδρομείου. Όταν σε ένα δίκτυο προστίθενται περισσότεροι χρήστες, προστίθενται επίσης αποκλειστικοί διακομιστές, ώστε να μειωθεί ο φόρτος εργασίας στον κύριο διακομιστή. Όταν χρησιμοποιούνται αποκλειστικοί διακομιστές, ο αρχικός κύριος διακομιστής μπορεί να γίνει αποκλειστικός διακομιστής.

Ποιες λειτουργίες αναλαμβάνουν οι αποκλειστικοί διακομιστές; Οποιαδήποτε εργασία που επαναλαμβάνεται ή απαιτεί πολύ χρόνο από τον επεξεργαστή (CPU) ενός υπολογιστή θα μπορούσε να ανατεθεί σε έναν αποκλειστικό διακομιστή. Κοινοί τύποι αποκλειστικών διακομιστών είναι οι διακομιστές αυθεντικοποίησης, οι διακομιστές αρχείων, οι διακομιστές εκτυπώσεων, οι διακομιστές εφαρμογών, οι διακομιστές βάσεων δεδομένων, οι διακομιστές ηλεκτρονικού ταχυδρομείου, οι διακομιστές επικοινωνιών, οι διακομιστές web και οι διακομιστές cloud. Οι διακομιστές συνδέονται σε δίκτυο πελάτη/διακομιστή, ώστε όλοι οι υπολογιστές πελάτες που θα χρειαστεί να χρησιμοποιήσουν τις υπηρεσίες τους να μπορούν να τους προσπελάσουν, όπως βλέπετε στην Εικόνα 12.6.

Διακομιστές αυθεντικοποίησης και αρχείων

Τι είναι οι διακομιστές αυθεντικοποίησης και αρχείων; Ένας **διακομιστής αυθεντικοποίησης** (authentication server) είναι ο διακομιστής που παρακολουθεί και καταγράφει ποιος συνδέεται στο δίκτυο και ποιες υπηρεσίες είναι διαθέσιμες στο δίκτυο για κάθε χρήστη. Οι διακομιστές αυθεντικοποίησης συνήθως ενεργούν ως επόπτες του δικτύου. Διευθύνουν και συντονίζουν τις υπηρεσίες που παρέχουν οι άλλοι αποκλειστικοί διακομιστές που υπάρχουν στο δίκτυο.

Ένας **διακομιστής αρχείων** (file server) είναι ο διακομιστής που αποθηκεύει και διαχειρίζεται αρχεία για χρήστες του δικτύου. Στο δίκτυο στην εργασία ή στη σχολή σας, ίσως σας παραχωρείται χώρος σε κάποιον διακομιστή αρχείων για να αποθηκεύετε τα αρχεία που δημιουργείτε.

Διακομιστές εκτυπώσεων

Πώς λειτουργεί ένας διακομιστής εκτυπώσεων; Οι **διακομιστές εκτυπώσεων** (print server) διαχειρίζονται όλες τις εργασίες εκτύπωσης που αιτούνται οι χρήστες για όλους τους εκτυπωτές στο δίκτυο, κάτι που βοηθά τους υπολογιστές πελάτες να εργάζονται

πιο παραγωγικά καθώς απελευθερώνονται από τέτοια καθήκοντα. Όταν ζητάτε από τον υπολογιστή σας να εκτυπώσει ένα έγγραφο, αναθέτει την εργασία στον διακομιστή εκτυπώσεων και η CPU του υπολογιστή σας είναι ελεύθερη να εκτελέσει άλλες εργασίες.

Πώς γνωρίζει ο εκτυπωτής ποιο έγγραφο πρέπει να εκτυπώσει; Η **ουρά εκτύπωσης** (ή *spooler*) είναι λογισμικό που κρατά μια περιοχή για εργασίες εκτύπωσης. Όταν ο διακομιστής εκτυπώσεων λαμβάνει μια αίτηση για εκτύπωση από έναν υπολογιστή πελάτη, τοποθετεί την εργασία σε μια ουρά εκτύπωσης στον διακομιστή εκτυπώσεων. Φυσιολογικά, κάθε εκτυπωτής στο δίκτυο έχει τη δική του ουρά εκτύπωσης με ένα μοναδικό όνομα. Οι εργασίες παίρνουν έναν αριθμό όταν εισέρχονται στην ουρά και πηγαίνουν στον εκτυπωτή με τη σειρά τους. Ως εκ τούτου, οι διακομιστές εκτυπώσεων οργανώνουν τις εργασίες εκτύπωσης διατηρώντας τη σειρά αρίθμησης, ώστε οι εκτυπώσεις να ολοκληρώνονται πιο αποδοτικά σε έναν κοινόχρηστο εκτυπωτή.

Ακόμα μια χρήσιμη πτυχή των διακομιστών εκτυπώσεων είναι ότι οι διαχειριστές δικτύων μπορούν να τους ρυθμίζουν έτσι ώστε να θέτουν προτεραιότητες σε εργασίες εκτύπωσης. Διαφορετικοί χρήστες και τύποι εργασιών εκτύπωσης μπορούν να λάβουν διαφορετική προτεραιότητα, ώστε οι εργασίες υψηλότερης προτεραιότητας να εκτυπώνονται πρώτες. Για παράδειγμα, σε μια εταιρεία στην οποία τα έγγραφα πρέπει να εκτυπώνονται αμέσως όταν ζητηθούν από πελάτες, οι εργασίες εκτύπωσης αυτού του είδους θα πρέπει να έχουν προτεραιότητα σε σχέση, για παράδειγμα, με την αλληλογραφία των υπαλλήλων.

Διακομιστές εφαρμογών

Τι κάνει ένας διακομιστής εφαρμογών; Σε πολλά δίκτυα, όλοι οι χρήστες εκτελούν το ίδιο λογισμικό εφαρμογών στους υπολογιστές τους. Σε ένα δίκτυο χιλιάδων προσωπικών υπολογιστών, η εγκατάσταση λογισμικού εφαρμογών σε κάθε υπολογιστή χωριστά είναι χρονοβόρα. Ο **διακομιστής εφαρμογών** (application server) λειτουργεί ως αποθήκη για λογισμικό εφαρμογών.

Όταν ένας υπολογιστής πελάτης συνδέεται στο δίκτυο και αιτείται μια εφαρμογή, ο διακομιστής εφαρμογών παραδίδει το λογισμικό στον υπολογιστή πελάτη. Επειδή το λογισμικό δεν βρίσκεται στον ίδιο τον υπολογιστή πελάτη, διευκολύνεται η εργασία της εγκατάστασης και της αναβάθμισης. Η εφαρμογή θα χρειαστεί να εγκατασταθεί και να ενημερωθεί μόνο στον διακομιστή εφαρμογών και όχι σε κάθε υπολογιστή πελάτη.

Διακομιστές βάσεων δεδομένων

Τι κάνει ένας διακομιστής βάσεων δεδομένων; Ο **διακομιστής βάσεων δεδομένων** (database server) παρέχει στους υπολογιστές πελάτες πρόσβαση σε πληροφορίες που αποθηκεύονται σε βάσεις δεδομένων. Πολλές φορές, πολλοί άνθρωποι πρέπει να προσπελάσουν μια βάση δεδομένων ταυτόχρονα. Για παράδειγμα, πολλοί σύμβουλοι πανεπιστημίων (ειδικό λογισμικό παροχής υποστήριξης) μπορούν να εξυπηρετήσουν πολλούς φοιτητές ταυτόχρονα επειδή έχουν πρόσβαση στη βάση δεδομένων με τα στοιχεία των φοιτητών. Αυτό είναι δυνατόν επειδή η βάση δεδομένων βρίσκεται σε έναν διακομιστή βάσεων δεδομένων τον οποίο κάθε σύμβουλος μπορεί να προσπελάσει μέσω του δικτύου. Αν η βάση δεδομένων βρισκόταν σε έναν αυτόνομο υπολογιστή και όχι στο δίκτυο, τότε μόνο ένας σύμβουλος θα μπορούσε να τη χρησιμοποιήσει κάθε φορά.

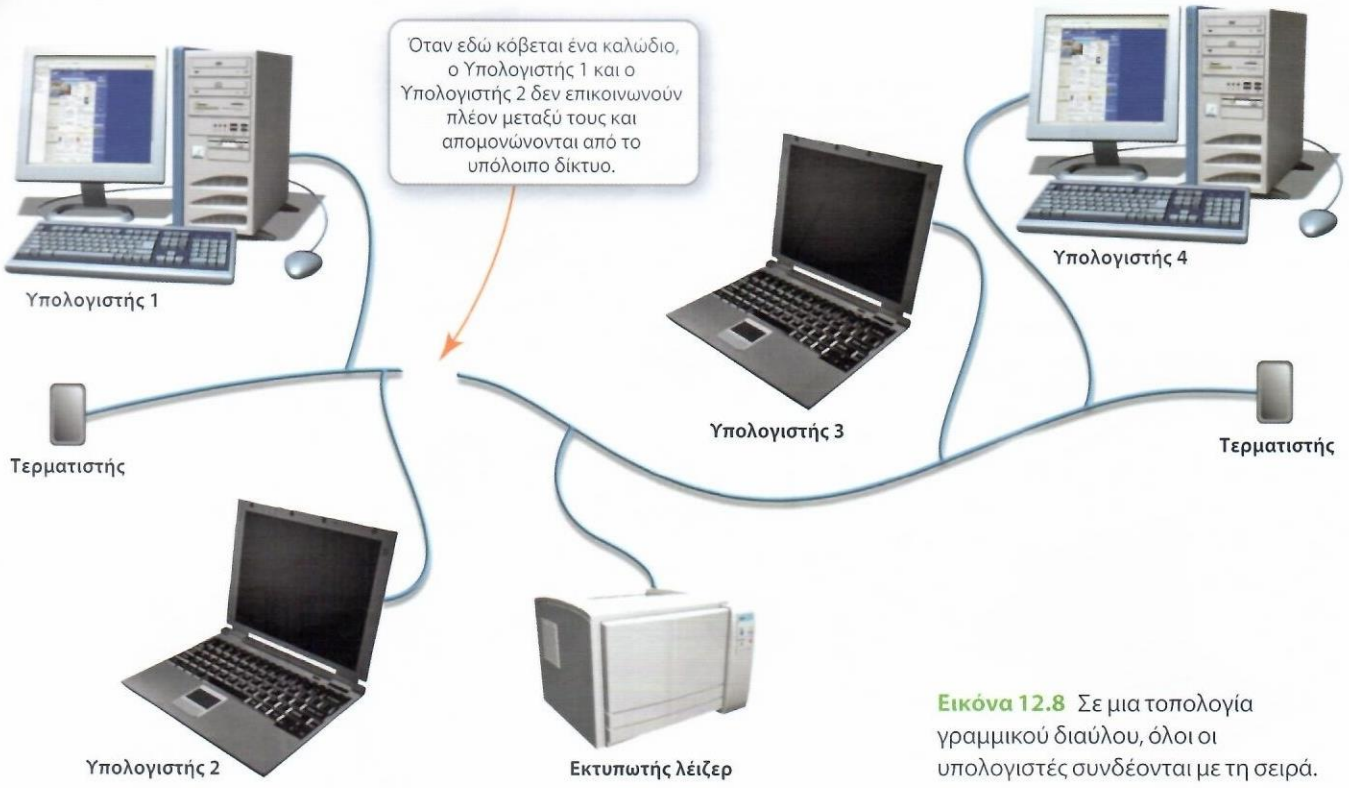
Διακομιστές ηλεκτρονικού ταχυδρομείου

Πώς γίνεται η διαχείριση του ηλεκτρονικού ταχυδρομείου σε ένα μεγάλο δίκτυο πελάτη/διακομιστή; Η μοναδική λειτουργία ενός **διακομιστή ηλεκτρονικού ταχυδρομείου** (e-mail server) είναι η επεξεργασία και η παράδοση εισερχόμενων και εξερχόμενων μηνυμάτων. Ο όγκος των μηνυμάτων σε ένα μεγάλο δίκτυο αυξάνεται πολύ γρήγορα και θα μπορούσε να υπερφορτώσει έναν διακομιστή ο οποίος θα επιχειρούσε να εκτελέσει και άλλες λειτουργίες. Σε ένα δίκτυο με έναν διακομιστή ηλεκτρονικού ταχυδρομείου, όταν στέλνετε ή παραλαμβάνετε ένα μήνυμα, αυτό περνά από τον διακομιστή ηλεκτρονικού ταχυδρομείου και αυτός είναι που χειρίζεται τη δρομολόγηση και την παράδοση του μηνύματός σας.

Διακομιστές επικοινωνιών

Τι τύπους επικοινωνιών χειρίζεται ένας διακομιστής επικοινωνιών; Ένας **διακομιστής επικοινωνιών** (communication server) χειρίζεται όλες τις επικοινωνίες ανάμεσα στο δίκτυο και άλλα δίκτυα, συμπεριλαμβανομένης της διαχείρισης της συνδεσιμότητας στο διαδίκτυο. Όλες οι αιτήσεις για πληροφορίες από το διαδίκτυο και όλα τα μηνύματα που αποστέλλονται μέσω διαδικτύου διέρχονται από τον διακομιστή επικοινωνιών. Επειδή υπάρχει μεγάλη κυκλοφορία στο διαδίκτυο για κάθε οργανισμό, ο διακομιστής επικοινωνιών έχει βαρύ φόρτο εργασίας.

Ο διακομιστής επικοινωνιών είναι πολλές φορές η μοναδική συσκευή σε ένα δίκτυο που συνδέεται στο διαδίκτυο. Οι διακομιστές ηλεκτρονικού ταχυδρομείου, οι διακομιστές web και άλλες συσκευές που πρέπει να επικοινωνήσουν με το διαδίκτυο συνήθως δρομολογούν όλη την κυκλοφορία τους μέσω του διακομιστή επικοινωνιών. Η παροχή ενός μόνο σημείου επα-



Εικόνα 12.8 Σε μια τοπολογία γραμμικού διαύλου, όλοι οι υπολογιστές συνδέονται με τη σειρά.

Πώς μεταφέρονται τα δεδομένα από ένα σημείο σε άλλο σε ένα δίκτυο διαύλου; Τα δεδομένα μεταδίδονται στο δίκτυο σε όλες τις συσκευές που συνδέονται σε αυτό. Τα δεδομένα αναλύονται σε μικρότερα τμήματα, τα λεγόμενα *πακέτα*. Κάθε πακέτο περιέχει τη διεύθυνση του υπολογιστή ή της περιφερειακής συσκευής στην οποία αποστέλλεται. Κάθε συσκευή που συνδέεται στο δίκτυο προσπαθεί να ανιχνεύσει τα δεδομένα που περιέχουν τη διεύθυνσή της. Όταν «ακούσει» δεδομένα που προέρχονται για αυτή, εξάγει τα δεδομένα από τα μέσα μετάδοσης και τα επεξεργάζεται.

Οι συσκευές (κόμβοι) που συνδέονται σε ένα δίκτυο διαύλου δεν κάνουν τίποτα για να μεταφέρουν δεδομένα στο δίκτυο, άρα το δίκτυο διαύλου είναι μια **παθητική τοπολογία**. Τα δεδομένα διανύουν όλο το μέσο και παραλαμβάνονται από όλες τις συσκευές του δικτύου. Στις άκρες του καλωδίου ενός δικτύου διαύλου ολοκληρώνεται η μετάδοση από τους τερματιστές (όπως βλέπετε στην Εικόνα 12.8). Ο **τερματιστής** (terminator) είναι μια συσκευή η οποία απορροφά ένα σήμα το οποίο δεν αντανακλάται πίσω στα μέρη του δικτύου που το έχουν ήδη λάβει.

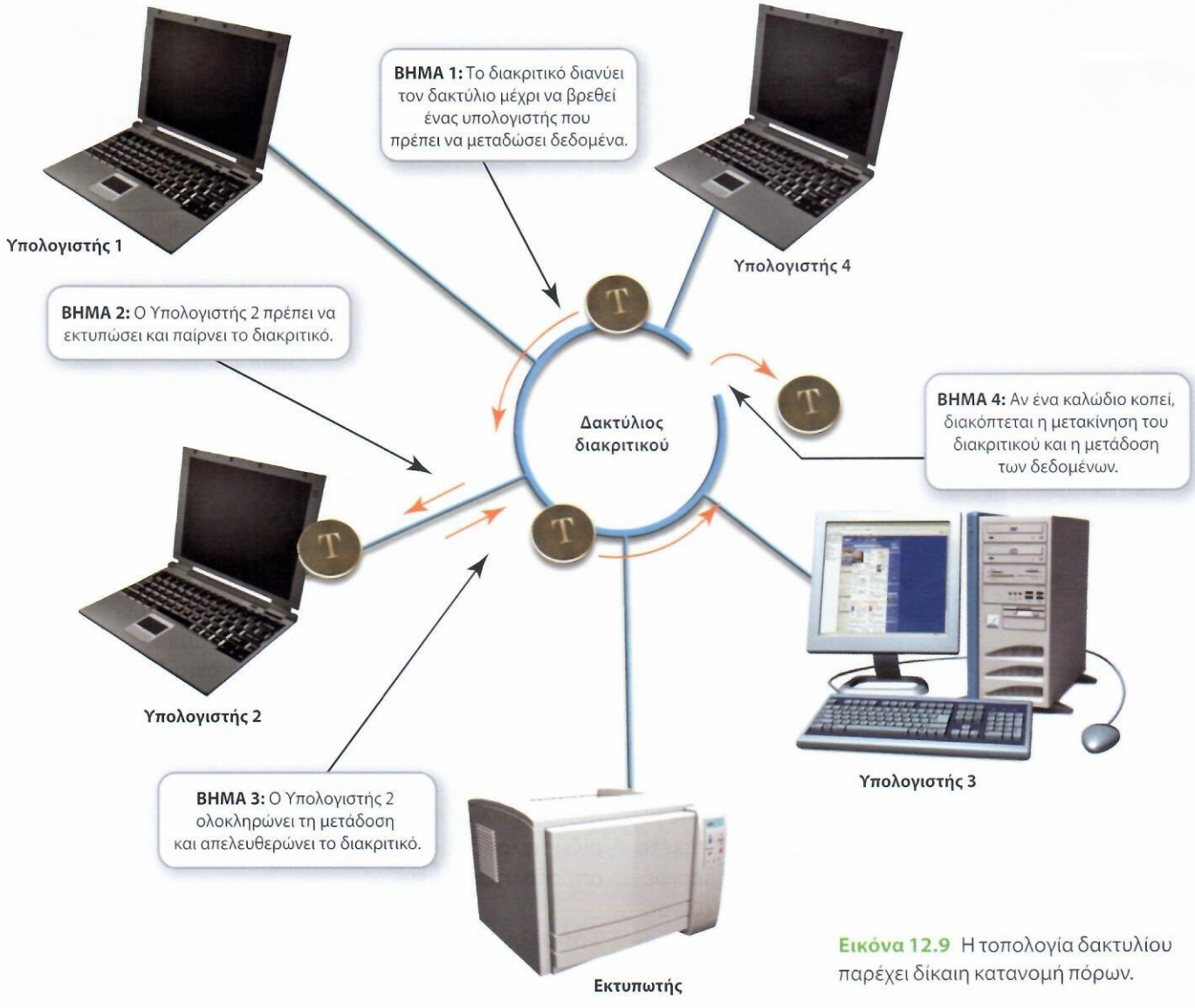
Ποια είναι τα πλεονεκτήματα και ποια τα μειονεκτήματα των δικτύων διαύλου; Η απλότητα και το χαμηλό κόστος της τοπολογίας ενός δικτύου διαύλου είναι τα βασικά πλεονεκτήματά της. Όπως βλέπετε στην Εικόνα 12.8, το κυριότερο μειονέκτημα είναι ότι, αν το καλώδιο κοπεί, το δίκτυο διαύλου ουσιαστικά καταργείται, επειδή ορισμένοι υπολογιστές απομονώνονται από το δίκτυο. Επίσης, επειδή μόνο ένας υπολογιστής μπορεί να επικοινωνεί κάθε φορά, η προσθήκη πολλών κόμβων σε ένα δίκτυο διαύλου περιορίζει την απόδοση και προκαλεί καθυστερήσεις στην αποστολή δεδομένων.

Τοπολογία δακτυλίου

Πώς είναι η τοπολογία δακτυλίου; Από το όνομα καταλαβαίνουμε ότι οι υπολογιστές και οι περιφερειακές συσκευές σε μια **τοπολογία δακτυλίου** (ring topology) (ή **βρόχου**) διατάσσονται κατά τρόπο τέτοιο που μοιάζει με κύκλο, όπως βλέπετε στην Εικόνα 12.9. Τα δεδομένα ρέουν γύρω από τον κύκλο από μία συσκευή σε άλλη, προς μία μόνο κατεύθυνση. Επειδή τα δεδομένα περνούν μέσα από ένα ειδικό πακέτο δεδομένων που ονομάζεται **διακριτικό** (**token**), αυτός ο τύπος τοπολογίας κάποτε ονομαζόταν *τοπολογία διακριτικού δακτυλίου*.

Πώς μεταφέρει δεδομένα ένα διακριτικό γύρω από έναν δακτύλιο; Το διακριτικό περνά από υπολογιστή σε υπολογιστή γύρω από τον δακτύλιο μέχρι να φτάσει στον υπολογιστή που πρέπει να μεταδώσει δεδομένα. Ο υπολογιστής «κρατά» το διακριτικό μέχρι να ολοκληρώσει τη μετάδοση δεδομένων. Μόνο ένας υπολογιστής στον δακτύλιο μπορεί να «κρατά» το διακριτικό κάθε φορά και συνήθως σε έναν δακτύλιο υπάρχει μόνο ένα διακριτικό.

Αν ένας κόμβος έχει δεδομένα για αποστολή, όπως



Εικόνα 12.9 Η τοπολογία δακτυλίου παρέχει δίκαιη κατανομή πόρων.

ένα έγγραφο που πρέπει να μεταφερθεί στον εκτυπωτή, περιμένει να λάβει το διακριτικό. Ο κόμβος αποσύρει τότε το διακριτικό από την κυκλοφορία και στέλνει τα δεδομένα στον προορισμό τους. Όταν ο παραλήπτης κόμβος παραλάβει μια ολοκληρωμένη μετάδοση των δεδομένων (εν προκειμένω, όταν το έγγραφο φτάσει στον εκτυπωτή), μεταδίδει μια επιβεβαίωση στον αποστολέα κόμβο. Ο αποστολέας κόμβος παράγει τότε ένα νέο διακριτικό και το περιφέρει στον δακτύλιο. Πρόκειται για τη **μέθοδο διακριτικού** (token method) και είναι η μέθοδος πρόσβασης που χρησιμοποιούν τα δίκτυα δακτυλίου για να αποφεύγουν συγκρούσεις δεδομένων.

Η τοπολογία δακτυλίου είναι μια **ενεργή τοπολογία** (active topology), δηλαδή οι κόμβοι συμμετέχουν στη μεταφορά δεδομένων μέσω του δικτύου. Κάθε κόμβος στο δίκτυο είναι υπεύθυνος για την αναμετάδοση του διακριτικού ή των δεδομένων στον επόμενο κόμβο στον δακτύλιο. Μεγάλα δίκτυα δακτυλίου μπορούν να χρησιμοποιούν πολλαπλά διακριτικά, ώστε τα δεδομένα να κινούνται ταχύτερα.

Ποια είναι τα πλεονεκτήματα και ποια τα μειονεκτήματα της τοπολογίας δακτυλίου; Η τοπολογία δακτυλίου παρέχει μια πιο δίκαιη κατανομή των πόρων δικτύου από μια τοπολογία διαύλου. Χρησιμοποιώντας ένα διακριτικό, το δίκτυο δακτυλίου παρέχει σε όλους τους κόμβους του δικτύου ίσες ευκαιρίες να στέλνουν δεδομένα. Ένας «φλύαρος» κόμβος δεν μπορεί να μονοπωλήσει το εύρος ζώνης του δικτύου όσο εύκολα μπορεί να το κάνει σε μια τοπολογία διαύλου επειδή οφείλει να διαβιβάσει το διακριτικό αφού στείλει μια δεσμίδα δεδομένων. Επιπλέον, η απόδοση της τοπολογίας δακτυλίου παραμένει αποδεκτή ακόμα κι όταν οι χρήστες είναι πολλοί.

Όπως βλέπετε στην Εικόνα 12.9, ένα μειονέκτημα του δικτύου δακτυλίου είναι ότι, αν ένας υπολογιστής αστοχήσει, όλο το δίκτυο θα μπορούσε να έρθει σε τέλμα επειδή αυτός ο συγκεκριμένος υπολογιστής

Μέρος 2

Εγκατάσταση δικτύων επιχειρήσεων

Μαθησιακό αποτέλεσμα 12.2 **Θα είστε σε θέση να περιγράψετε τι είναι τα μέσα μετάδοσης, το λογισμικό λειτουργικού συστήματος δικτύου και οι συσκευές πλοήγησης δικτύου και να εξηγήσετε τις κυριότερες απειλές για την ασφάλεια του δικτύου και πώς αντιμετωπίζονται.**

Η εγκατάσταση δικτύων επιχειρήσεων είναι παρόμοια με τη διαμόρφωση των οικιακών δικτύων. Πρέπει να εξετάσετε το είδος των μέσων μετάδοσης, να εξασφαλίσετε ότι όλοι οι κόμβοι διαθέτουν προσαρμογείς δικτύων και να εγκαταστήσετε τις κατάλληλες συσκευές επικοινωνίας δικτύου.

Μέσα μετάδοσης

Μπορεί να έχετε μόνο ασύρματα μέσα μετάδοσης στο οικιακό δίκτυό σας, αλλά οι επιχειρήσεις δεν έχουν τις ίδιες ανάγκες με τους οικιακούς χρήστες. Θα ξεκινήσουμε εξετάζοντας τα μέσα μετάδοσης που χρησιμοποιούνται σε δίκτυα επιχειρήσεων.

Ενσύρματα και ασύρματα μέσα μετάδοσης

Στόχος 12.6 *Οι τύποι ενσύρματων και ασύρματων μέσων μετάδοσης που χρησιμοποιούνται σε δίκτυα.*

Τι ακριβώς είναι τα μέσα μετάδοσης; Τα **μέσα μετάδοσης** (transmission media), είτε πρόκειται για ενσύρματη είτε για ασύρματη τεχνολογία επικοινωνιών, αποτελούν το φυσικό σύστημα που ακολουθούν τα δεδομένα προκειμένου να μεταφερθούν από μία συσκευή σε άλλη στο δίκτυο. Χωρίς μέσα μετάδοσης, οι συσκευές δικτύου δεν θα μπορούσαν να επικοινωνήσουν. Τα περισσότερα εταιρικά δίκτυα περιέχουν έναν συνδυασμό ενσύρματων και ασύρματων μέσων.

Γιατί στα δίκτυα επιχειρήσεων χρησιμοποιούνται ενσύρματες συνδέσεις; Οι ενσύρματες συνδέσεις είναι δημοφιλείς στα δίκτυα επιχειρήσεων επειδή παρέχουν γενικά υψηλότερη απόδοση και καλύτερη ασφάλεια από τις ασύρματες συνδέσεις. Οι σταθεροί υπολογιστές εξακολουθούν να παρέχουν περισσότερη υπολογιστική ισχύ με μικρότερο κόστος από τους φορητούς, κάτι που καθιστά τους σταθερούς υπολογιστές δημοφιλείς επιλογές σε δίκτυα επιχειρήσεων. Επειδή οι σταθεροί υπολογιστές

Εικόνα 12.13

Παράγοντες που εξετάζονται για την επιλογή καλωδίων δικτύου

Μέγιστο μήκος διαδρομής
- Πόσο μακριά μπορεί να φτάσει ένα καλώδιο πριν αρχίσει να υποβαθμίζεται το σήμα δεδομένων.
- Η απόσταση μεταξύ των κόμβων καθορίζει το μήκος διαδρομής που απαιτείται.

Εύρος ζώνης
- Η ποσότητα δεδομένων που μεταδίδεται στο μέσο.
- Μετριέται σε bit ανά δευτερόλεπτο (bps).

Ευκαμψία (ακτίνα κάμψης)
- Πόσο μπορεί να λυγίσει ένα καλώδιο πριν χαλάσει.
- Πολλές γωνίες; Χρειάζεστε καλώδιο με μεγάλη ακτίνα κάμψης.

Κόστος καλωδίου
- Το κόστος διαφέρει για κάθε τύπο καλωδίου.
- Ο προϋπολογισμός μπορεί να περιορίζει την επιλογή του τύπου καλωδίου.

Κόστος εγκατάστασης
- Το καλώδιο συνεστραμμένου ζεύγους και το ομοαξονικό καλώδιο δεν έχουν υψηλό κόστος εγκατάστασης.
- Το καλώδιο οπτικών ινών απαιτεί ειδική εκπαίδευση και εξοπλισμό, άρα το κόστος του είναι υψηλό.

Παρεμβολή
- Το συνεστραμμένο ζεύγος είναι πιο ευαίσθητο σε παρεμβολές.
- Το καλώδιο οπτικών ινών δεν επηρεάζεται από παρεμβολές.

(Maridav/Fotolia· Victoria/Fotolia· Nicholas Piccillo/Fotolia· Ion Popa/Fotolia Auremar/Fotolia· Ermess/Fotolia)

δεν μετακινούνται συχνά, συνήθως συνδέονται σε ένα δίκτυο μέσω ενσύρματης σύνδεσης.

Ποιοι είναι οι σημαντικοί παράγοντες στην επιλογή του τύπου καλωδίου; Για τα δίκτυα επιχειρήσεων, οι τρεις τύποι καλωδίων που χρησιμοποιούνται είναι το *συνεστραμμένο ζεύγος*, το *ομοαξονικό καλώδιο* και το *καλώδιο οπτικών ινών*. Αν και κάθε τύπος καλωδίου είναι διαφορετικός, οι ίδιοι έξι παράγοντες εξετάζονται πάντοτε κατά την επιλογή του τύπου καλωδίου (βλ. Εικόνα 12.13): μέγιστο μήκος διαδρομής, εύρος ζώνης, ευκαμψία (ακτίνα κάμψης), κόστος καλωδίου, κόστος εγκατάστασης και παρεμβολή.

Τι προκαλεί παρεμβολή στα σήματα δεδομένων; Τα σήματα που ταξιδεύουν σε ένα καλώδιο υπόκεινται σε δύο τύπους παρεμβολής:

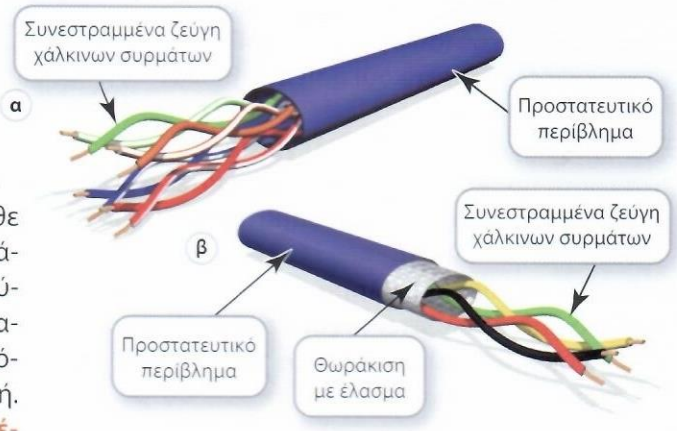
1. Η *ηλεκτρομαγνητική παρεμβολή (EMI)*, η οποία προκαλείται όταν το καλώδιο εκτίθεται σε ισχυρά ηλεκτρομαγνητικά πεδία, μπορεί να παραμορφώσει ή να υποβαθμίσει τα σήματα που μεταφέρονται στο καλώδιο. Οι λάμπες φθορισμού και οι μηχανές με κινητήρες ή μετασχηματιστές είναι οι πιο κοινές πηγές εκπομπών EMI.
2. Τα σήματα στα καλώδια μπορεί επίσης να αλλοιώνονται από *παρεμβολή ραδιοσυχνότητας (RFI)*, η οποία συνήθως προκαλείται από πηγές εκπομπής (τηλεόραση και ραδιόφωνο) που βρίσκονται κοντά στο δίκτυο.

Το ομοαξονικό καλώδιο και το καλώδιο συνεστραμμένου ζεύγους στέλνουν ηλεκτρικούς παλμούς σε αγώγιμο υλικό για τη μετάδοση σημάτων δεδομένων, με αποτέλεσμα να είναι πιο ευάλωτα σε παρεμβολές. Το καλώδιο οπτικών ινών μεταδίδει τα σήματα δεδομένων ως παλμούς φωτός. Επειδή τα EMI και RFI δεν επηρεάζουν τα κύματα του φωτός, το καλώδιο οπτικών ινών είναι σχεδόν απρόσβλητο από παρεμβολές.

Στις ενότητες που ακολουθούν, θα εξετάσουμε τα χαρακτηριστικά κάθε τύπου καλωδίου και θα μελετήσουμε τη χρήση ασύρματων μέσων ως εναλλακτικού μέσου μετάδοσης.

Καλώδιο συνεστραμμένου ζεύγους

Γιατί είναι συνεστραμμένα τα σύρματα στο καλώδιο συνεστραμμένου ζεύγους; Το **καλώδιο συνεστραμμένου ζεύγους** (twisted-pair cable) αποτελείται από ζεύγη χάλκινων συρμάτων που στρέφονται το ένα γύρω από το άλλο και καλύπτονται από ένα προστατευτικό περίβλημα. Οι συστροφές είναι σημαντικές επειδή αναγκάζουν τα μαγνητικά πεδία που σχηματίζονται γύρω από τα σύρματα να περιπλέκονται και να είναι ως εκ τούτου λιγότερο ευάλωτα σε εξωτερικές παρεμβολές. Οι συστροφές μειώνουν επίσης τις διασταυρούμενες παρεμβολές (την τάση που έχουν τα σήματα σε ένα σύρμα να παρεμβάλλονται στα σήματα ενός σύρματος που βρίσκεται δίπλα του).



Εικόνα 12.14 Ανατομία ενός (α) μη θωρακισμένου καλωδίου συνεστραμμένου ζεύγους (UTP) και ενός (β) θωρακισμένου καλωδίου συνεστραμμένου ζεύγους (STP)

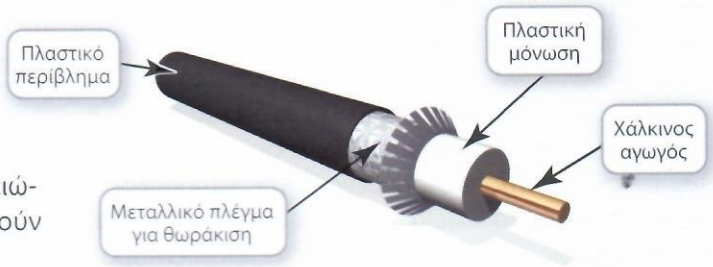
Αν το καλώδιο συνεστραμμένου ζεύγους περιέχει ένα επίπεδο θωράκισης με πλέγματα θωράκισης από αλουμίνιο για τον περιορισμό των παρεμβολών, τότε το καλώδιο ονομάζεται **θωρακισμένο καλώδιο συνεστραμμένου ζεύγους** (shielded twisted-pair – **STP**). Τα περισσότερα οικιακά δίκτυα χρησιμοποιούν μη θωρακισμένα καλώδια (UTP) τα οποία δεν διαθέτουν αυτή την προστασία με πλέγματα. Το καλώδιο UTP είναι περισσότερο ευάλωτο σε παρεμβολές από το STP. Η Εικόνα 12.14 παρουσιάζει αμφότερους τους τύπους καλωδίου συνεστραμμένου ζεύγους. Χάρη στη χαμηλή τιμή του, το UTP χρησιμοποιείται σε δίκτυα επιχειρήσεων, εκτός αν πρέπει να ξεπεραστούν σημαντικές πηγές παρεμβολής, όπως συμβαίνει σε ένα εργοστασιακό περιβάλλον όπου τα μηχανήματα δημιουργούν μαγνητικά πεδία.

Ομοαξονικό καλώδιο

Εξακολουθεί να χρησιμοποιείται το ομοαξονικό καλώδιο σε επαγγελματικά δίκτυα; Αν και δεν είναι το ίδιο δημοφιλές με το παρελθόν, το ομοαξονικό καλώδιο εξακολουθεί να χρησιμοποιείται σε κάποιες εγκαταστάσεις όπου τα μηχανήματα δημιουργούν έντονες ηλεκτρικές παρεμβολές. Το **ομοαξονικό καλώδιο** (coaxial cable) (όπως βλέπετε στην Εικόνα 12.15) αποτελείται από τέσσερα στοιχεία:

1. Έναν αγωγό (συνήθως χάλκινο) ο οποίος βρίσκεται στον πυρήνα του καλωδίου και χρησιμοποιείται για τη μετάδοση του σήματος.

2. Ένα συμπαγές στρώμα μη αγώγιμου μονωτικού υλικού (συνήθως ενός σκληρού και χοντρού πλαστικού) που περιβάλλει τον αγωγό.
3. Ένα στρώμα μεταλλικού πλέγματος θωράκισης που καλύπτει τη μόνωση, ώστε να μειώνονται οι παρεμβολές στα σήματα που περνούν μέσα από τον αγωγό.
4. Ένα εξωτερικό περίβλημα από ελαφρύ πλαστικό, το οποίο καλύπτει τα εσωτερικά στοιχεία του καλωδίου προκειμένου να τα προστατεύει από ζημιές.



Εικόνα 12.15 Το ομοαξονικό καλώδιο αποτελείται από τέσσερα βασικά στοιχεία: έναν αγωγό, μια μονωμένη επικάλυψη, ένα μεταλλικό πλέγμα για θωράκιση και ένα πλαστικό περίβλημα.

Καλώδιο οπτικών ινών

Πώς είναι το καλώδιο οπτικών ινών; Όπως βλέπετε στην Εικόνα 12.16, το **καλώδιο οπτικών ινών** (fiber-optic cable) αποτελείται από τα εξής:

- Μια γυάλινη (ή πλαστική) ίνα (ή μια δεσμίδα ινών που σχηματίζουν έναν αγωγό) μέσω της οποίας μεταδίδονται τα δεδομένα.
- Ένα προστατευτικό στρώμα γυάλινης ή πλαστικής επικάλυψης που τυλίγεται γύρω από τον αγωγό για να τον προστατεύει.
- Για επιπλέον προστασία, έχει εξωτερικό περίβλημα, το οποίο συνήθως αποτελείται από ένα ανθεκτικό υλικό, όπως το Kevlar (το υλικό που χρησιμοποιείται για την κατασκευή αλεξίσφαιρων γιλέκων).

Εικόνα 12.16 Το καλώδιο οπτικών ινών αποτελείται από μια γυάλινη ή πλαστική ίνα (ή δεσμίδα ινών), μια γυάλινη ή πλαστική επίστρωση και ένα προστατευτικό περίβλημα.

Οι μεταδόσεις δεδομένων μπορούν να διέρχονται από το καλώδιο οπτικών ινών προς μία μόνο κατεύθυνση. Επομένως, υπάρχουν τουλάχιστον δύο ίνες (ή αγωγοί) στα περισσότερα καλώδια οπτικών ινών, ώστε να επιτρέπεται η μετάδοση προς αμφότερες τις κατευθύνσεις.

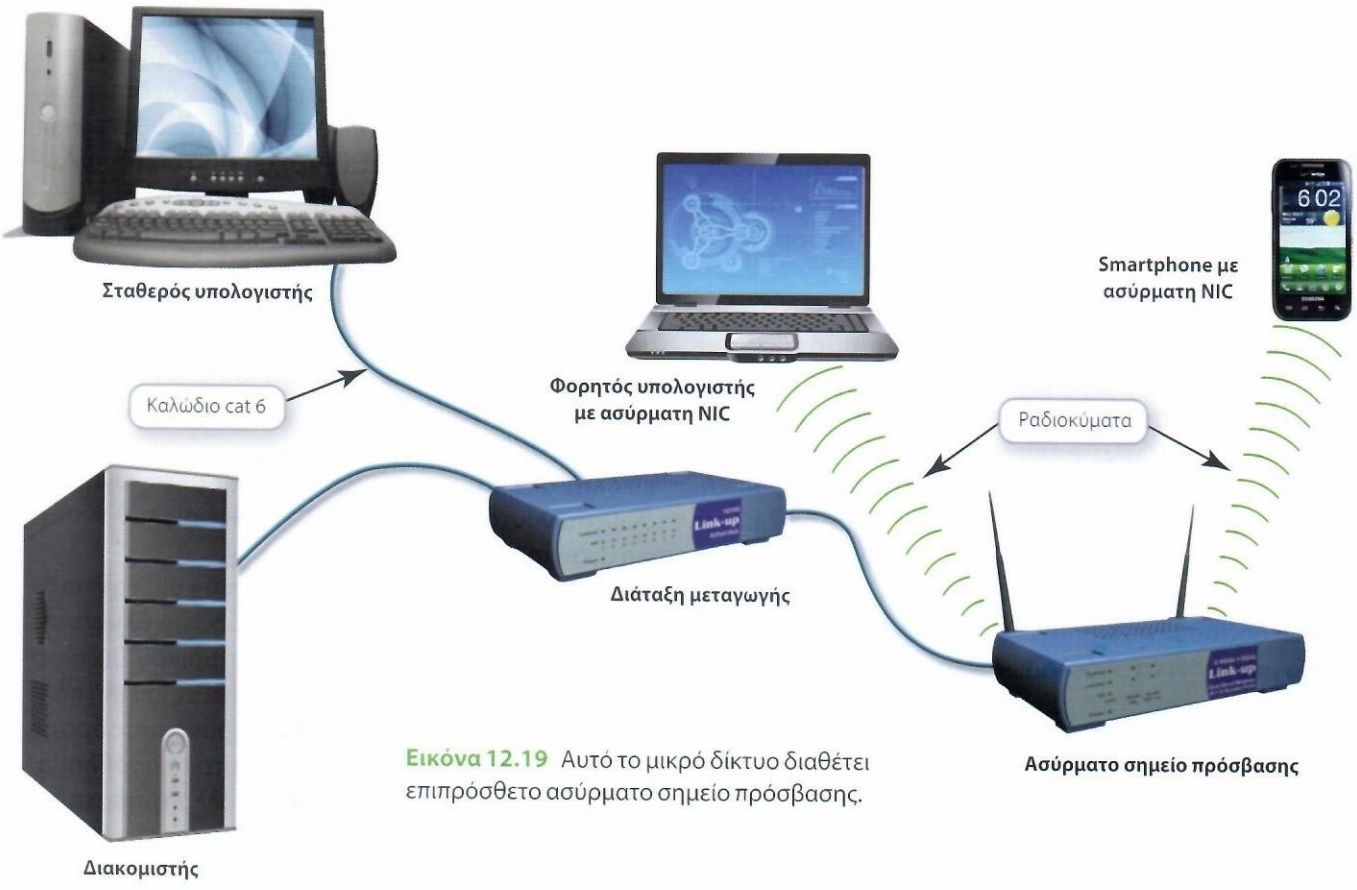
Επιλογές ασύρματων μέσων

Ποιες επιλογές ασύρματων μέσων υπάρχουν; Τα περισσότερα δίκτυα επιχειρήσεων χρησιμοποιούν τα ίδια πρότυπα Ethernet με τα οικιακά δίκτυα. Επομένως, οι ασύρματες επιλογές για δίκτυα επιχειρήσεων είναι σχεδόν ίδιες με εκείνες που υπάρχουν για τα οικιακά δίκτυα. Γίνεται εγκατάσταση *ασύρματων σημείων πρόσβασης* τα οποία παρέχουν την απαραίτητη κάλυψη για τις περιπτώσεις που οι υπάλληλοι χρησιμοποιούν φορητές συσκευές, όπως συμβαίνει στις αίθουσες συσκέψεων.

Σύγκριση των μέσων μετάδοσης

Ποιο μέσο είναι το καλύτερο για δίκτυα επιχειρήσεων; Οι μηχανικοί δικτύων ειδικεύονται στη σχεδίαση και ανάπτυξη δικτύων και είναι υπεύθυνοι για την επιλογή των κατάλληλων τοπολογιών δικτύων και τύπων μέσων μετάδοσης. Η απόφασή τους σχετικά με το μέσο μετάδοσης που θα χρησιμοποιηθεί για ένα δίκτυο βασίζεται στην επιλεγμένη τοπολογία, στο μήκος των καλωδίων που χρειάζονται, στον όγκο των παρεμβολών που υπάρχουν και στην ανάγκη για ασύρματη συνδεσιμότητα.

Όπως αναφέραμε νωρίτερα, τα περισσότερα μεγάλα δίκτυα χρησιμοποιούν έναν συνδυασμό τύπων μέσων μετάδοσης. Για παράδειγμα, το καλώδιο οπτικών ινών μπορεί να μην είναι κατάλληλο για το κομμάτι του δικτύου που διέρχεται από τον χώρο ενός εργοστασίου, όπου οι παρεμβολές από μαγνητικά πεδία είναι σημαντικές. Το καλώδιο UTP όμως μπορεί να λειτουργήσει πολύ καλά σε χώρους γραφείων. Τα ασύρματα μέσα πιθανόν να είναι απαραίτητα όταν υπάρχουν πολλές πιθανότητες να συνδέονται φορητές ψηφιακές συσκευές ή όπου είναι ανέφικτη ή ακριβή η λύση του καλωδίου.



Εικόνα 12.19 Αυτό το μικρό δίκτυο διαθέτει επιπρόσθετο ασύρματο σημείο πρόσβασης.

ρόμοια με έναν σειριακό αριθμό σε μια συσκευή. Αυτή η διεύθυνση ονομάζεται **διεύθυνση ελέγχου πρόσβασης μέσου** (media access control – **MAC**) και αποτελείται από 6 χαρακτήρες δύο θέσεων, όπως 01:40:87:44:79:A5. (Μη συγχέετε αυτό το MAC με τους υπολογιστές Apple που έχουν το ίδιο όνομα.) Τα τρία πρώτα σύνολα χαρακτήρων (σε αυτή την περίπτωση, το 01:40:87) προσδιορίζουν τον κατασκευαστή του προσαρμογέα δικτύου και το δεύτερο σύνολο χαρακτήρων (σε αυτή την περίπτωση, το 44:79:A5) είναι μια μοναδική διεύθυνση. Επειδή όλες οι διευθύνσεις MAC πρέπει να είναι μοναδικές, υπάρχει μια επιτροπή του IEEE (Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών) που είναι υπεύθυνη για την ανάθεση αριθμών σε κατασκευαστές προσαρμογέων δικτύου.

Οι διευθύνσεις MAC είναι ίδιες με τις διευθύνσεις IP; Οι διευθύνσεις MAC και οι διευθύνσεις IP (πρωτόκολλο διαδικτύου) δεν είναι το ίδιο πράγμα. Μια διεύθυνση MAC χρησιμοποιείται για την αναγνώριση συσκευών *εσωτερικά* σε ένα δίκτυο. Μια διεύθυνση IP είναι η διεύθυνση που χρησιμοποιούν *εξωτερικές* οντότητες για να επικοινωνούν με το δίκτυό σας. Σκεφτείτε το ως εξής: η ταχυδρομική υπηρεσία παραδίδει ένα πακέτο (πακέτο δεδομένων) στο κτίριο της εστίας σας με βάση τη διεύθυνσή της (διεύθυνση IP). Ο υπεύθυνος υπάλληλος της εστίας παραδίδει το πακέτο στο δωμάτιό σας επειδή έχει το δικό σας όνομα πάνω του (διεύθυνση MAC) και όχι αυτό του γείτονά σας. Αμφότερες οι πληροφορίες είναι απαραίτητες προκειμένου να εξασφαλιστεί ότι το πακέτο (ή τα δεδομένα) φτάνουν στον προορισμό τους.

Πώς συσκευάζονται τα πακέτα δεδομένων για μετάδοση; Τα πακέτα δεδομένων δεν αποστέλλονται απαραίτητα το καθένα μόνο του. Μερικές φορές, ομάδες πακέτων δεδομένων αποστέλλονται μαζί σε ένα πακέτο, το **πλαίσιο** (frame). Το πλαίσιο είναι μια θήκη που μπορεί να περιέχει πολλά πακέτα δεδομένων και θα μπορούσαμε να πούμε ότι προσομοιάζει την τοποθέτηση σε έναν μεγάλο φάκελο πολλών επιστολών που έχουν τον ίδιο προορισμό. Ενώ τα πακέτα δεδομένων συγκεντρώνονται σε πλαίσια, το λειτουργικό σύστημα δικτύου (NOS) εκχωρεί την κατάλληλη διεύθυνση MAC στο πλαίσιο αυτό. Το NOS παρακολουθεί όλες τις συσκευές και τις διευθύνσεις τους στο δίκτυο. Περίπου όπως ένας φάκελος που παραδίδεται με εμπιστοσύνη στην ταχυδρομική υπηρεσία, το πλαίσιο παραδίδεται στη διεύθυνση MAC που εκχώρησε το NOS στο πλαίσιο.

Πώς παραδίδονται τα πλαίσια στη σωστή συσκευή στο δίκτυο; Σε ένα μικρό δίκτυο διαύλου, τα πλαίσια απλώς κινούνται στο μέσο μετάδοσης μέχρι ο σωστός υπολογιστής πελάτης να παρατηρήσει ότι το

πλαίσιο απευθύνεται σε αυτόν και να αναγνώσει το σήμα από το μέσο. Κάτι τέτοιο όμως δεν μπορεί να γίνει σε ένα μεγαλύτερο δίκτυο. Γι' αυτό και έχουν αναπτυχθεί πολλοί τύποι συσκευών για την αποδοτική παράδοση των δεδομένων στους προορισμούς τους. Αυτές οι συσκευές σχεδιάζονται έτσι ώστε να δρομολογούν σήματα και να ανταλλάσσουν δεδομένα με άλλα δίκτυα.

Οι διευθύνσεις MAC είναι χρήσιμες για οτιδήποτε άλλο πέρα από τον προσδιορισμό μιας συγκεκριμένης συσκευής δικτύου; Σε δίκτυα με ασύρματες δυνατότητες, οι διευθύνσεις MAC μπορούν να χρησιμοποιηθούν για την ενίσχυση της ασφάλειας δικτύων. Επειδή κάθε διεύθυνση MAC είναι μοναδική, μπορείτε να εισάγετε μια λίστα με εξουσιοδοτημένες διευθύνσεις MAC στον δρομολογητή. Αν κάποιος που χρησιμοποιεί έναν μη εξουσιοδοτημένο προσαρμογέα δικτύου επιχειρήσει να συνδεθεί στο δίκτυο, δεν θα μπορέσει να ολοκληρώσει τη σύνδεση.

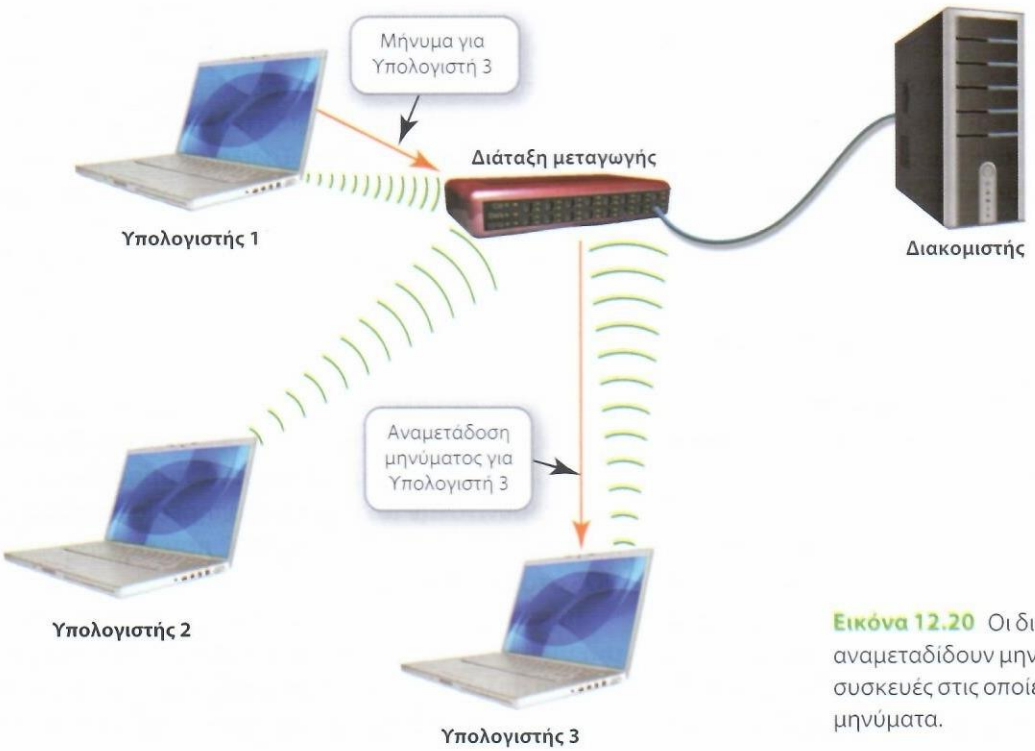
Διατάξεις μεταγωγής, γέφυρες και δρομολογητές

Στόχος 12.9 *Οι διάφορες συσκευές πλοήγησης δικτύου και πώς δρομολογούν τα δεδομένα στα δίκτυα.*

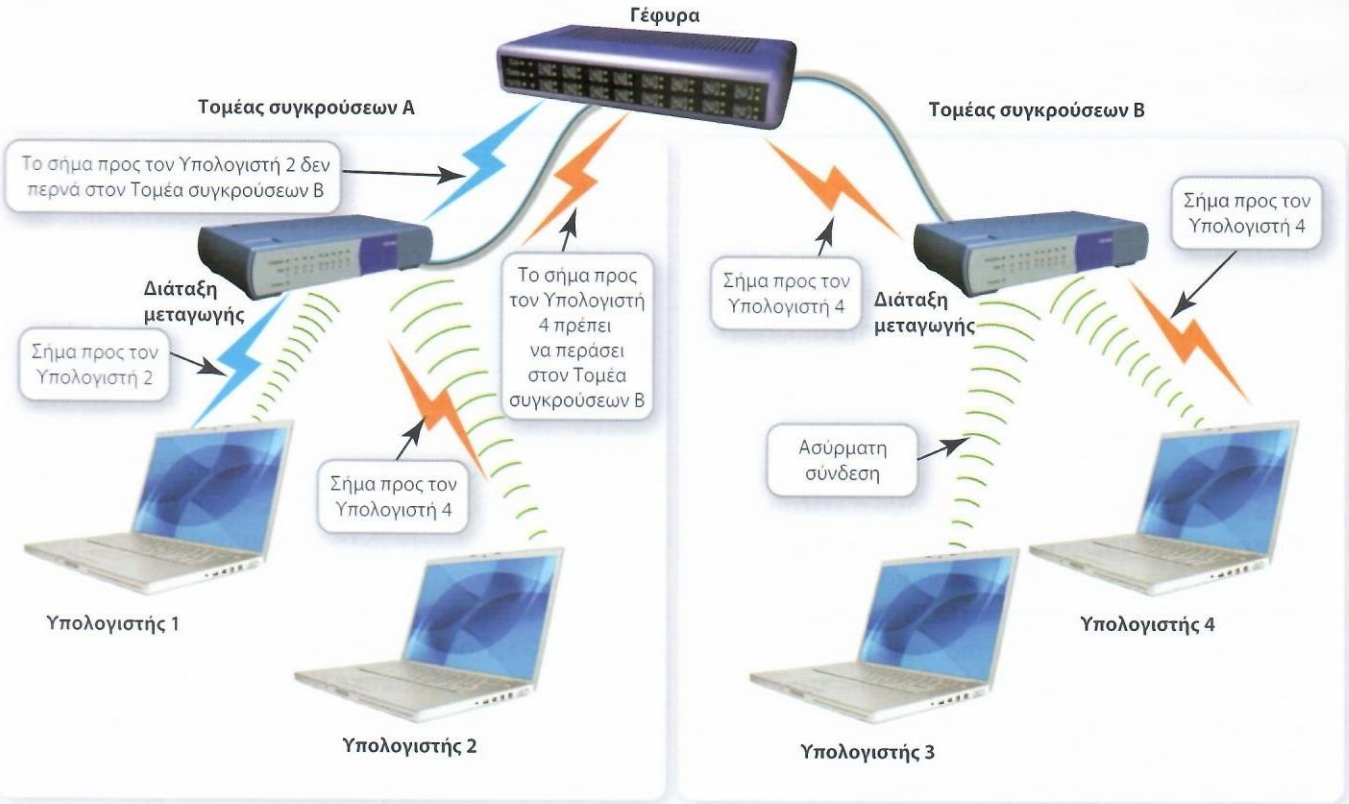
Ποιες συσκευές χρησιμοποιούνται για τη δρομολόγηση σημάτων μέσω ενός δικτύου; Οι διατάξεις μεταγωγής χρησιμοποιούνται για την αποστολή δεδομένων σε συγκεκριμένη διαδρομή μέσω του δικτύου. Μια **διάταξη μεταγωγής** (switch) λαμβάνει αποφάσεις, με βάση τη διεύθυνση MAC των δεδομένων, σχετικά με το πού πρέπει να σταλούν τα δεδομένα και τα αναμεταδίδει στον κατάλληλο κόμβο δικτύου. Αυτή η διαδικασία βελτιώνει την απόδοση του δικτύου, καθώς εξασφαλίζει ότι κάθε κόμβος θα παραλαμβάνει μόνο τα δεδομένα που απευθύνονται σε αυτόν. Η Εικόνα 12.20 δείχνει πώς χρησιμοποιείται μια διάταξη μεταγωγής για την αναμετάδοση ενός μηνύματος.

Όλα τα δίκτυα Ethernet πρέπει να έχουν διατάξεις μεταγωγής; Οι διατάξεις μεταγωγής είναι απαραίτητες σε δίκτυα Ethernet είτε εγκαθίστανται σε οικίες είτε σε επιχειρήσεις. (Οι διατάξεις μεταγωγής ενσωματώνονται στους δρομολογητές που πωλούνται για οικιακή χρήση.)

Οι διατάξεις μεταγωγής επαρκούν για την αποδοτική μεταφορά δεδομένων σε δίκτυα όλων των μεγεθών; Όταν το μέγεθος ενός εταιρικού δικτύου μεγαλώνει, η απόδοση μπορεί να μειωθεί, επειδή πολλές συσκευές ανταγωνίζονται για χρόνο μετάδοσης στο δίκτυο. Προκειμένου να λυθεί αυτό το πρόβλημα, ένα δίκτυο μπορεί να αναλυθεί σε πολλά τμήματα, τα οποία ονομάζονται *τομείς συγκρούσεων*. Η **γέφυρα** (bridge) είναι μια συσκευή που χρησιμοποιείται για την αποστολή δεδομένων ανάμεσα σε διαφορετικούς τομείς συγκρούσεων, ανάλογα με το πού βρίσκεται η συσκευή που παραλαμβάνει τα δεδομένα, όπως βλέπετε στην Εικόνα 12.21. Τα σήματα που παραλαμβάνονται από τη γέφυρα από τον Τομέα συγκρούσεων A



Εικόνα 12.20 Οι διατάξεις μεταγωγής αναμεταδίδουν μηνύματα – αλλά μόνο στις συσκευές στις οποίες απευθύνονται τα μηνύματα.



Εικόνα 12.21 Οι γέφυρες είναι συσκευές που χρησιμοποιούνται για την αποστολή δεδομένων μεταξύ διαφορετικών τομέων συγκρούσεων δικτύου.

πελάτη και διακομιστή που συνδέεται στο δίκτυο πρέπει να εγκατασταθεί ειδικό λογισμικό, το λεγόμενο **λειτουργικό σύστημα δικτύου** (network operating system – **NOS**), το οποίο θα παρέχει τις υπηρεσίες που είναι απαραίτητες για την επικοινωνία των συσκευών. Το NOS παρέχει ένα σύνολο από κοινούς κανόνες (το *πρωτόκολλο*) οι οποίοι ελέγχουν την επικοινωνία μεταξύ των συσκευών στο δίκτυο. Τα σύγχρονα λειτουργικά συστήματα, όπως τα Windows και το macOS, περιλαμβάνουν λογισμικό πελάτη NOS στη βασική εγκατάστασή τους. Τα μεγάλα δίκτυα όμως, όπως αυτά που χρησιμοποιούν οι επιχειρήσεις, απαιτούν πιο προηγμένο λογισμικό διακομιστή NOS.

Γιατί είναι απαραίτητο το λογισμικό διακομιστή NOS σε μεγάλα δίκτυα; Το λογισμικό λειτουργικού συστήματος σχεδιάζεται έτσι ώστε να διευκολύνει την επικοινωνία ανάμεσα στο λογισμικό και το υλικό του υπολογιστή σας. Το λογισμικό NOS σχεδιάζεται ειδικά ώστε να παρέχει υπηρεσίες διακομιστή, επικοινωνίες μεταξύ δικτύων, διαχείριση περιφερειακών συσκευών και αποθήκευσης δεδομένων δικτύων. Μερικά δημοφιλή προγράμματα λογισμικού διακομιστή είναι το Windows Server, το Red Hat Enterprise Linux και το SUSE Linux Enterprise Server. Το λογισμικό NOS εγκαθίσταται σε διακομιστές.

Προκειμένου να παρέχουν επικοινωνία δικτύων, οι υπολογιστές πελάτες πρέπει να χρησιμοποιούν ένα μικρό μέρος του NOS εκτός από το δικό τους ΛΣ. Τα Windows και το macOS διαθέτουν δυνατότητες επικοινωνίας δικτύων και, επομένως, συνήθως δεν υπάρχει άλλο λογισμικό NOS διαθέσιμο σε τέτοιους υπολογιστές πελάτες.

Για τα δίκτυα P2P απαιτείται ειδικό λογισμικό NOS; Το λογισμικό που χρειάζονται τα δίκτυα P2P ενσωματώνεται στα λειτουργικά συστήματα Windows, Linux και macOS. Επομένως, αν έχετε ένα απλό δίκτυο P2P, δεν υπάρχει λόγος να προμηθευτείτε ένα εξειδικευμένο λογισμικό NOS.

Πώς ελέγχει την επικοινωνία δικτύων το NOS; Κάθε NOS έχει τη δική του αποκλειστική γλώσσα επικοινωνίας, δομή διαχείρισης αρχείων και δομή διαχείρισης συσκευών. Το NOS ορίζει και ελέγχει επίσης τα πρωτόκολλα για όλες τις συσκευές που επιθυμούν να επικοινωνήσουν στο δίκτυο. Το αποκλειστικό πρωτόκολλο του NOS ενός κατασκευαστή δεν συνεργάζεται με το NOS άλλου κατασκευαστή.

Επειδή όμως το διαδίκτυο χρησιμοποιεί ένα ανοιχτό πρωτόκολλο (το TCP/IP) για επικοινωνίες, όλα σχεδόν τα εταιρικά δίκτυα χρησιμοποιούν το TCP/IP ως τυπικό πρωτόκολλο δικτύωσης ανεξάρτητα από τον κατασκευαστή του NOS τους. Όλα τα σύγχρονα NOS υποστηρίζουν το TCP/IP.

Μπορεί ένα δίκτυο να χρησιμοποιεί δύο διαφορετικά NOS; Πολλά μεγάλα εταιρικά δίκτυα χρησιμοποιούν πολλά διαφορετικά NOS ταυτόχρονα και αυτό συμβαίνει επειδή διαφορετικά NOS παρέχουν διαφορετικές δυνατότητες, με κάποιες εξ αυτών να είναι πιο χρήσιμες σε συγκεκριμένες καταστάσεις από άλλες. Για παράδειγμα, αν και οι υπάλληλοι ενός οργανισμού μπορεί να χρησιμοποιούν Windows για τους σταθερούς υπολογιστές και το e-mail τους, οι διακομιστές αρχείων και οι διακομιστές web μπορεί να λειτουργούν με NOS που βασίζεται στο Linux.

Προστασία δικτύων πελάτη/διακομιστή

Στόχος 12.11 *Οι μεγαλύτερες απειλές για την ασφάλεια των δικτύων και πώς μπορούν οι διαχειριστές δικτύων να αντιμετωπίσουν αυτές τις απειλές.*

Βουτιά στα βαθιά

Το μοντέλο OSI: Ορισμός προτύπων πρωτοκόλλων

Το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE) έχει αναλάβει τον ορισμό πρωτοκόλλων δικτύωσης για όλο τον κόσμο, συμπεριλαμβανομένου ενός προτύπου επικοινωνιών που ονομάζεται **διασύνδεση ανοιχτών συστημάτων** (open systems interconnection – **OSI**). Το μοντέλο OSI, το οποίο έχει υιοθετηθεί απ' όλο τον κόσμο της πληροφορικής, παρέχει οδηγίες πρωτοκόλλου για όλα τα σύγχρονα δίκτυα. Όλα τα σύγχρονα πρωτόκολλα λειτουργικών συστημάτων δικτύου (NOS) σχεδιάζονται έτσι ώστε να αλληλεπιδρούν με τα πρότυπα που ορίζονται στο μοντέλο OSI.

Το μοντέλο OSI χωρίζει τις εργασίες επικοινωνιών σε επτά διεργασίες που ονομάζονται επίπεδα. Κάθε επίπεδο σε ένα δίκτυο OSI έχει συγκεκριμένη λειτουργία και γνωρίζει πώς να επικοινωνεί με τα επίπεδα πάνω και κάτω του. Η Εικόνα 12.22 παρουσιάζει τα επίπεδα του μοντέλου OSI και τις λειτουργίες τους.

Αυτή η προσέγγιση διαστρωμάτωσης ενισχύει την αποδο-

Εικόνα 12.22

Τα επίπεδα του μοντέλου OSI και οι λειτουργίες τους

Επίπεδο εφαρμογής

- Χειρίζεται όλες τις διασυνδέσεις μεταξύ του λογισμικού εφαρμογών και του δικτύου
- Μεταφράζει τις πληροφορίες χρηστών σε μια μορφή που μπορεί να κατανοήσει το επίπεδο παρουσίασης

Επίπεδο παρουσίασης

- Αναμορφοποιεί τα δεδομένα ώστε να μπορεί να τα κατανοήσει το επίπεδο συνόδου
- Συμπιέζει και κρυπτογραφεί δεδομένα

Επίπεδο συνόδου

- Δημιουργεί μια εικονική (όχι φυσική) σύνδεση μεταξύ των συσκευών αποστολής και παραλαβής
- Διαχειρίζεται τις συνόδους επικοινωνιών

Επίπεδο μεταφοράς

- Δημιουργεί πακέτα και χειρίζεται την επιβεβαίωση λήψης πακέτων

Επίπεδο δικτύου

- Προσδιορίζει πού πρέπει να σταλούν τα πακέτα στο δίκτυο

Επίπεδο σύνδεσης δεδομένων

- Συγκεντρώνει τα δεδομένα σε πλαίσια, ορίζει τον προορισμό τους και τα στέλνει στο φυσικό επίπεδο

Φυσικό επίπεδο

- Μεταδίδει (παραδίδει) δεδομένα στο δίκτυο ώστε να μπορούν να φτάσουν στον προορισμό τους

τικότητα των επικοινωνιών επειδή εξειδικευμένα κομμάτια του NOS εκτελούν συγκεκριμένες εργασίες. Η διαστρωματική προσέγγιση ακολουθεί τα πρότυπα της γραμμής παραγωγής στα βιομηχανικά περιβάλλοντα.

Η παραγωγή χιλιάδων αυτοκινήτων κάθε μέρα θα ήταν δύσκολη αν ένα άτομο έπρεπε να κατασκευάσει ένα ολόκληρο αυτοκίνητο μόνο του. Χωρίζοντας, ωστόσο, το έργο της συναρμολόγησης ενός αυτοκινήτου σε εξειδικευμένες εργασίες και αναθέτοντας τις εργασίες σε άτομα που τις κάνουν καλά, επιτυγχάνεται σημαντική αποδοτικότητα. Τα επίπεδα OSI ενισχύουν την αποδοτικότητα των επικοινωνιών μέσω κατάλληλων χειρισμών εξειδικευμένων εργασιών και επικοινωνίας μόνο με τα επίπεδα που βρίσκονται ακριβώς από πάνω και από κάτω τους.

Θα μελετήσουμε τώρα πώς λειτουργεί κάθε επίπεδο του OSI ακολουθώντας μέσα στα επίπεδα ένα μήνυμα ηλεκτρονικού ταχυδρομείου που δημιουργείτε και στέλνετε σε έναν φίλο σας:

- *Επίπεδο εφαρμογής:* Χειρίζεται το σύνολο της αλληλεπίδρασης ανάμεσα στο λογισμικό εφαρμογής και το δίκτυο. Μεταφράζει τα δεδομένα από την εφαρμογή σε μια μορφή που μπορεί να καταλάβει το επίπεδο παρουσίασης. Για παράδειγμα, όταν στέλνετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου, το επίπεδο εφαρμογής παίρνει το μήνυμα που δημιουργήσατε στο Microsoft Outlook, το μεταφράζει σε μια μορφή που κατανοεί το δίκτυό σας και το μεταβιβάζει στο επίπεδο παρουσίασης.
- *Επίπεδο παρουσίασης:* Αναμορφοποιεί τα δεδομένα έτσι ώστε να μπορεί να τα καταλάβει το επίπεδο συνόδου. Χειρίζεται επίσης την κρυπτογράφηση (αλλάζοντας τα δεδομένα σε μια μορφή που είναι πιο δύσκολο να διαβαστεί) και τη συμπίεση των δεδομένων, αν χρειάζεται. Στο παράδειγμά μας με το μήνυμα, το επίπεδο παρουσίασης παρατηρεί ότι επιλέξατε κρυπτογράφηση για το μήνυμα ηλεκτρονικού ταχυδρομείου και κρυπτογραφεί τα δεδομένα πριν σταλούν στο επίπεδο συνόδου.
- *Επίπεδο συνόδου:* Δημιουργεί μια εικονική (όχι φυσική) σύνδεση μεταξύ των συσκευών αποστολής και παραλαβής και έπειτα διαχειρίζεται την επικοινωνία μεταξύ των δύο συσκευών. Στο παράδειγμά μας, το επίπεδο συνόδου θα καθόριζε τις παραμέτρους για τη σύνοδο επικοινωνίας μεταξύ του υπολογιστή σας και του παρόχου υπηρεσιών διαδικτύου (ISP) που διατηρεί τον λογαριασμό του φίλου σας. Το επίπεδο συνόδου παρακολουθεί τότε τη μετάδοση του μηνύματος, μέχρι να μείνει ικανοποιημένο ότι όλα τα δεδομένα στο μήνυμα έχουν παραληφθεί από τον ISP του φίλου σας.
- *Επίπεδο μεταφοράς:* Χωρίζει τα δεδομένα σε πακέτα και τα τοποθετεί σε κατάλληλη σειρά. Χειρίζεται επίσης την επιβεβαίωση των πακέτων (δηλαδή διαπιστώνει αν τα πακέτα παρελήφθησαν στον προορισμό τους) και αποφασίζει αν πρέπει να σταλούν ξανά κάποια πακέτα. Στο παράδειγμά μας, το επίπεδο μεταφοράς χωρίζει το μήνυμα ηλεκτρονικού ταχυδρομείου σε πακέτα και τα στέλνει στο επίπεδο δικτύου, εξασφαλίζοντας ότι όλα τα πακέτα φτάνουν στον προορισμό τους.
- *Επίπεδο δικτύου:* Προσδιορίζει πού πρέπει να σταλούν τα πακέτα στο δίκτυο, καθώς και τον καλύτερο τρόπο δρομολόγησής τους. Στο παράδειγμά μας, το επίπεδο δικτύου εξετάζει τη διεύθυνση στα πακέτα (τη διεύθυνση του ISP του φίλου σας) και προσδιορίζει πώς θα δρομολογηθούν τα πακέτα ώστε να φτάσουν στον ISP και τελικά στον υπολογιστή παραλήπτη.
- *Επίπεδο σύνδεσης δεδομένων:* Είναι υπεύθυνο για τη συγκέντρωση των πακέτων δεδομένων σε πλαίσια, τον ορισμό της διεύθυνσης προορισμού των πλαισίων και την παράδοσή τους στο φυσικό επίπεδο, ώστε να μπορούν να σταλούν στον προορισμό τους. Είναι αντίστοιχο με έναν ταχυδρομικό υπάλληλο που διαβάζει τη διεύθυνση σε έναν φάκελο και βεβαιώνεται ότι φτάνει στον σωστό παραλήπτη. Στο παράδειγμά μας, το επίπεδο σύνδεσης δεδομένων συγκεντρώνει τα πακέτα δεδομένων του μηνύματος σε πλαίσια, τα οποία συνοδεύονται από τις κατάλληλες πληροφορίες δρομολόγησης που λαμβάνει από το επίπεδο δικτύου.
- *Φυσικό επίπεδο:* Αναλαμβάνει την παράδοση των δεδομένων. Μετατρέπει τα δεδομένα σε σήμα και τα μεταδίδει στο δίκτυο έτσι ώστε να μπορούν να φτάσουν στον προορισμό τους. Στο παράδειγμά μας, το φυσικό επίπεδο στέλνει τα δεδομένα μέσω διαδικτύου στον τελικό προορισμό τους (στον ISP του φίλου σας).

Ακολουθώντας τυποποιημένα πρωτόκολλα που ορίζονται από το μοντέλο OSI, το λογισμικό NOS μπορεί να επικοινωνεί με τους υπολογιστές και τις περιφερειακές συσκευές που συνδέονται στο δίκτυο, καθώς και με άλλα δίκτυα.

σίγουρα δεν αποκτάτε δικαίωμα πρόσβασης στο σύστημα εισαγωγής βαθμών.

Πώς ο περιορισμός των δικαιωμάτων πρόσβασης προστατεύει ένα δίκτυο; Επειδή η διαχείριση των λογαριασμών πρόσβασης στο δίκτυο γίνεται κεντρικά στον διακομιστή αυθεντικοποίησης, είναι εύκολο για τον διαχειριστή δικτύου να δημιουργεί λογαριασμούς για νέους χρήστες και να τους χορηγεί δικαιώματα πρόσβασης μόνο στα συστήματα και στο λογισμικό που χρειάζονται. Η κεντρική φύση της παροχής του δικαιώματος πρόσβασης και η δυνατότητα περιορισμού της πρόσβασης σε συγκεκριμένες περιοχές του δικτύου καθιστούν το δίκτυο πελάτη/διακομιστή πιο ασφαλές από το δίκτυο P2P.

Πέρα από τη μη εξουσιοδοτημένη πρόσβαση, πώς αλλιώς μπορεί να υπάρξει κλοπή και καταστροφή δεδομένων; Ένα μεγάλο πρόβλημα που υπάρχει με τις φορητές συσκευές, όπως είναι οι μονάδες flash, είναι η κλοπή δεδομένων ή πνευματικής ιδιοκτησίας. Επειδή είναι εύκολο να κρύψει κανείς τέ-

Μετάδοση δεδομένων

Στόχος 13.3 *Τα πρωτόκολλα του διαδικτύου για τη μετάδοση δεδομένων.*

Τι είναι πρωτόκολλο; Ακριβώς όπως οποιοδήποτε άλλο δίκτυο, το διαδίκτυο τηρεί ένα καθορισμένο σύνολο κανόνων για να στέλνει πληροφορίες μεταξύ υπολογιστών. Ένα **πρωτόκολλο υπολογιστών** είναι το σύνολο των κανόνων που αφορούν την ανταλλαγή ηλεκτρονικών πληροφοριών. Αν το διαδίκτυο είναι ο αυτοκινητόδρομος ταχείας κυκλοφορίας των πληροφοριών, τα πρωτόκολλα είναι ο κώδικας οδικής κυκλοφορίας.

Γιατί αναπτύχθηκαν τα πρωτόκολλα του διαδικτύου; Η ιδέα στην οποία βασίζεται ένα πρωτόκολλο είναι ότι οποιοσδήποτε μπορεί να το χρησιμοποιήσει στο σύστημα υπολογιστή του προκειμένου να επικοινωνήσει με οποιονδήποτε άλλον υπολογιστή που χρησιμοποιεί το ίδιο πρωτόκολλο. Οι πιο κοινές εργασίες στο διαδίκτυο –επικοινωνία, συνεργασία, δημιουργία περιεχομένου, αναζήτηση πληροφοριών και αγορές– εκτελούνται όλες με τον ίδιο τρόπο σε οποιοδήποτε σύστημα, ακολουθώντας αποδεκτά πρωτόκολλα διαδικτύου.

Όταν τηρούνται κοινά πρωτόκολλα επικοινωνίας, τα δίκτυα μπορούν να επικοινωνούν ακόμα κι αν έχουν διαφορετικές τοπολογίες, μέσα μετάδοσης ή λειτουργικά συστήματα. Για να επιτευχθούν οι αρχικοί στόχοι του διαδικτύου, έπρεπε να καθοριστούν πρωτόκολλα στα οποία θα συμφωνούσαν οι χρήστες. Κάθε πρωτόκολλο έπρεπε να είναι ένα **ανοιχτό σύστημα**, δηλαδή η σχεδίασή του θα έπρεπε να διατίθεται δημόσια, ώστε να την προσπελάσει και να τη μελετήσει οποιοσδήποτε ενδιαφερόμενος. Αυτή η προσέγγιση είχε εντελώς αντίθετη κατεύθυνση από το μοντέλο του **ιδιοταγούς συστήματος** (ιδιωτικό σύστημα) το οποίο ήταν ο κανόνας εκείνη την εποχή.

Υπήρξαν προβλήματα κατά την ανάπτυξη ενός πρωτοκόλλου διαδικτύου ανοιχτού συστήματος; Η συμφωνία σε κοινά πρότυπα ήταν σχετικά εύκολη. Το δύσκολο ήταν η ανάπτυξη μιας νέας μεθόδου επικοινωνίας, επειδή η τεχνολογία που υπήρχε τη δεκαετία του 1960 –η μεταγωγή σε κύκλωμα– δεν μπορούσε να χρησιμοποιηθεί αποδοτικά στην επικοινωνία μεταξύ υπολογιστών.

Μεταγωγή σε κύκλωμα

Γιατί δεν χρησιμοποιούμε τη μεταγωγή σε κύκλωμα για να συνδέσουμε δύο υπολογιστές; Η τεχνολογία αυτή χρησιμοποιείται από τις πρώτες μέρες του τηλεφώνου για την επίτευξη επικοινωνίας. Στη **μεταγωγή σε κύκλωμα** (circuit switching), σχηματίζεται μια αποκλειστική σύνδεση μεταξύ δύο σημείων (όπως δύο άνθρωποι στο τηλέφωνο) και η σύνδεση παραμένει ενεργή για όσο διαρκεί η μετάδοση. Αυτή η μέθοδος επικοινωνίας είναι σημαντική όταν οι επικοινωνίες πρέπει να παραληφθούν με τη σειρά αποστολής τους, όπως συμβαίνει στις τηλεφωνικές συνομιλίες.

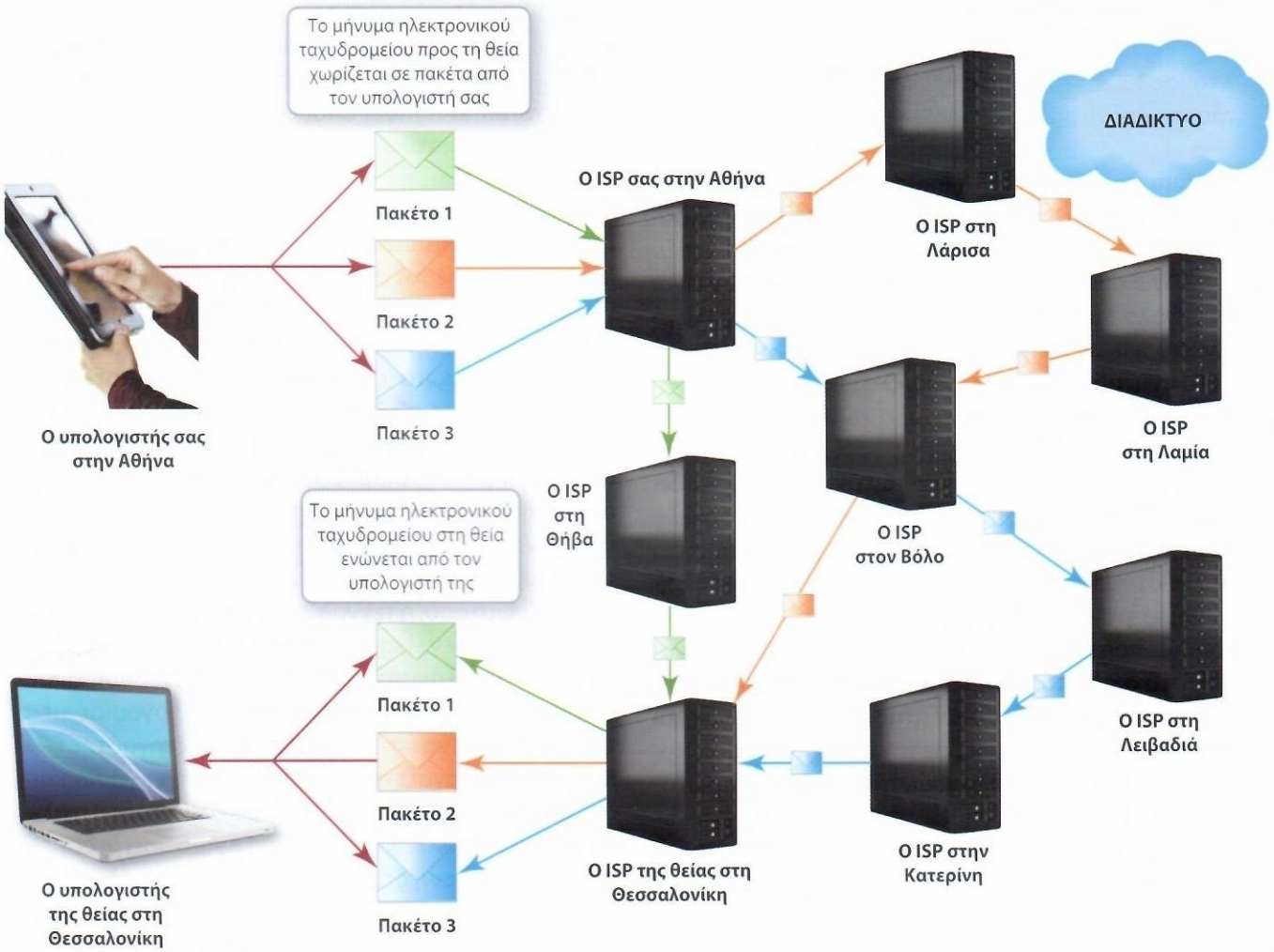
Όταν, ωστόσο, η τεχνολογία αυτή εφαρμόζεται σε υπολογιστές, δεν είναι αποδοτική. Καθώς ο επεξεργαστής ενός υπολογιστή εκτελεί τις ενέργειες που είναι απαραίτητες για την ολοκλήρωση μιας εργασίας, μεταδίδει δεδομένα κατά δεσμίδες. Ο επεξεργαστής ξεκινά τότε να εργάζεται για την επόμενη εργασία και σταματά να επικοινωνεί με τις συσκευές εξόδου ή άλλα δίκτυα μέχρι να είναι έτοιμος να μεταδώσει δεδομένα με την επόμενη δεσμίδα. Η μεταγωγή σε κύκλωμα είναι αναποτελεσματική για υπολογιστές επειδή είτε το κύκλωμα θα έπρεπε να παραμείνει ανοιχτό και επομένως μη διαθέσιμο για οποιοδήποτε άλλο σύστημα, με μακρές περιόδους αδράνειας, είτε θα έπρεπε να δημιουργείται εκ νέου για κάθε δεσμίδα δεδομένων.

Μεταγωγή σε πακέτα

Αν δεν χρησιμοποιούν μεταγωγή σε κύκλωμα, τι άλλο μπορούν να χρησιμοποιήσουν οι υπολογιστές για να επικοινωνήσουν; Η **μεταγωγή σε πακέτα** (packet switching) (δηλαδή η ανταλλαγή πακέτων) είναι η μεθοδολογία επικοινωνιών που επιτρέπει την επικοινωνία μεταξύ υπολογιστών. Η μεταγωγή σε πακέτα δεν απαιτεί τη δημιουργία αποκλειστικού κυκλώ-

Bits&Bytes Ένας δωρεάν διακομιστής cloud για εσάς

Σας ενδιαφέρει να δοκιμάσετε τις ικανότητές σας στην ανάπτυξη εφαρμογών web αλλά διστάζετε όταν σκέφτεστε ότι πρέπει να εγκαταστήσετε και να λειτουργήσετε τον δικό σας διακομιστή; Όχι πια! Το Cloud9 (**c9.io**) θα σας βοηθήσει να εγκαταστήσετε και να λειτουργήσετε όσους χώρους εργασίας Ubuntu χρειάζεστε. Κάθε χώρος εργασίας είναι μια εύχρηστη επιφάνεια εργασίας Linux η οποία κατοικεί στο cloud και την προσπελαύνετε μέσω του προγράμματος περιήγησης. Χρησιμοποιήστε έναν χώρο εργασίας για εξάσκηση των δεξιοτήτων σας σε μια γραμμή εντολών Linux ή για να χρησιμοποιήσετε τις γλώσσες που υποστηρίζει το Cloud9, όπως τις Ruby, C++ και PHP, για να αρχίσετε να προγραμματίζετε τον δικό σας διακομιστή στο cloud.



Εικόνα 13.4 Κάθε πακέτο που αποστέλλεται μέσω διαδικτύου μπορεί να ακολουθήσει τη δική του διαδρομή ως τον τελικό προορισμό του. Η σειριακή αρίθμηση των πακέτων εξασφαλίζει τη σωστή συναρμολόγησή τους στον προορισμό τους.
(Ifong/Shutterstock· Adventtr/Getty Images· Nikada/E+/Getty Images)

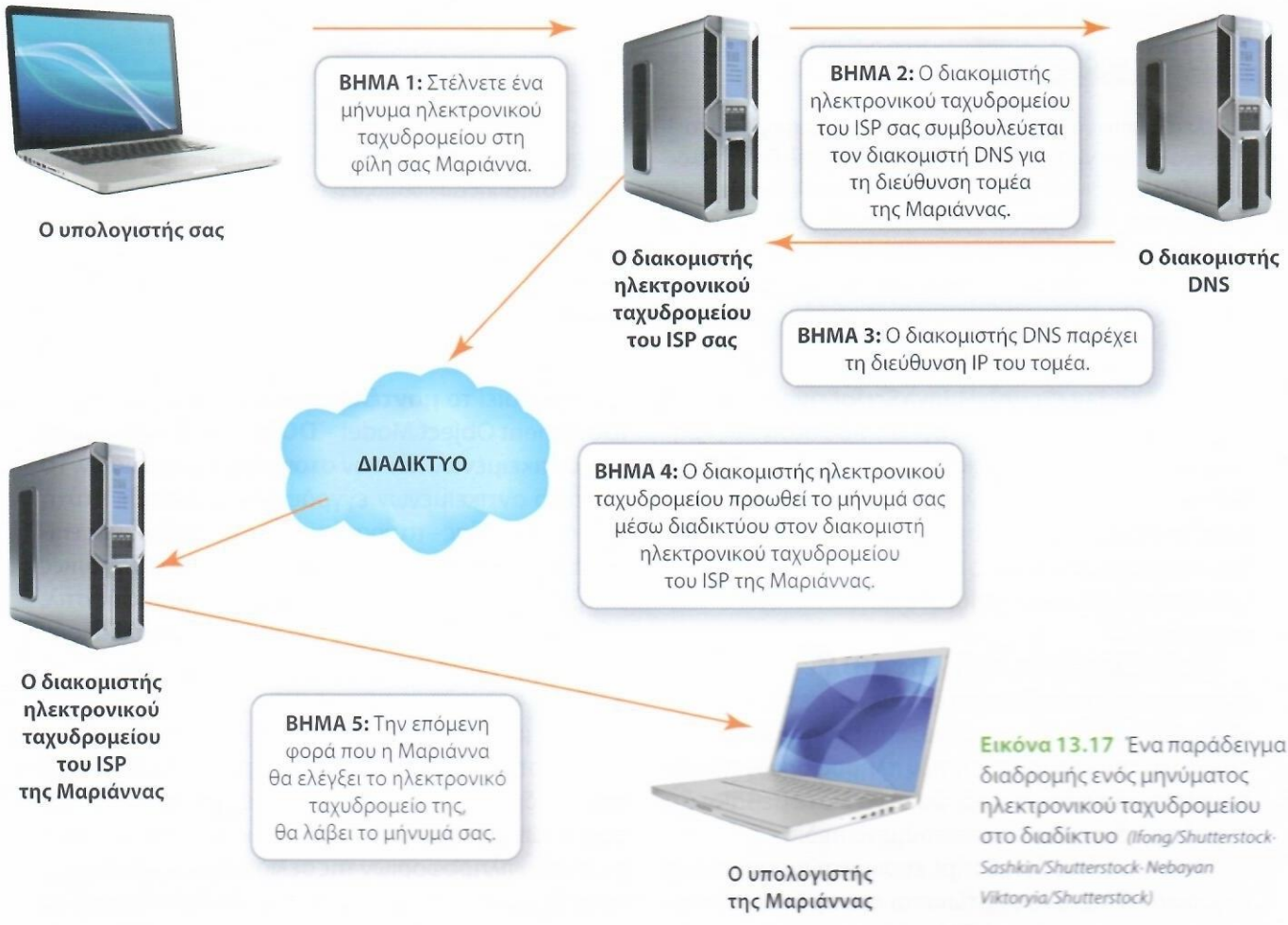
ματος επικοινωνίας. Σύμφωνα με αυτή την τεχνική, τα δεδομένα αναλύονται σε μικρότερα κομμάτια που ονομάζονται **πακέτα** (ή **πακέτα δεδομένων**). Τα πακέτα αποστέλλονται μέσω διάφορων διαδρομών ταυτόχρονα. Όταν φτάσουν στον προορισμό τους, συναρμολογούνται από τον παραλήπτη υπολογιστή. Αυτή η τεχνολογία προέκυψε από έναν από τους πρώτους στόχους του διαδικτύου: Αν ένας κόμβος στο διαδίκτυο καταστραφεί ή τεθεί εκτός λειτουργίας, τα δεδομένα μπορούν να κινηθούν από εναλλακτική διαδρομή για να φτάσουν στον προορισμό τους.

Τι πληροφορίες περιέχει ένα πακέτο; Τα περιεχόμενα των πακέτων διαφέρουν ανάλογα με το πρωτόκολλο που εφαρμόζεται. Κατ' ελάχιστο, όλα τα πακέτα πρέπει να περιέχουν τα εξής:

1. Μια διεύθυνση στην οποία αποστέλλεται το πακέτο
2. Τη διεύθυνση από την οποία απεστάλη το πακέτο
3. Οδηγίες συναρμολόγησης, αν τα αρχικά δεδομένα χωρίζονται σε πακέτα
4. Τα δεδομένα που μεταδίδονται

Η αποστολή ενός πακέτου μοιάζει με την αποστολή μιας επιστολής. Έστω ότι στέλνετε μια μεγάλη ποσότητα πληροφοριών σε γραπτή μορφή από το τηλέφωνό σας από την Αθήνα σε μια θεία σας στη Θεσσαλονίκη. Οι πληροφορίες είναι πολύ μεγάλες για να χωρέσουν σε έναν μικρό φάκελο, γι' αυτό στέλνετε τρεις διαφορετικούς φακέλους στη θεία σας. Κάθε φάκελος περιλαμβάνει τη διεύθυνση της θείας, τη διεύθυνση επιστροφής και τις πληροφορίες που περιέχει. Οι σελίδες των επιστολών σε κάθε φάκελο απαριθμούνται, ώστε η θεία σας να γνωρίζει με ποια σειρά πρέπει να τις διαβάσει.

Πιθανόν οι φάκελοι να μην ακολουθήσουν όλοι την ίδια διαδρομή. Ακόμα όμως κι αν οι επιστολές



Εικόνα 13.17 Ένα παράδειγμα διαδρομής ενός μηνύματος ηλεκτρονικού ταχυδρομείου στο διαδίκτυο *(Ilfong/Shutterstock· Sashkin/Shutterstock· Nebayan Viktoryia/Shutterstock)*

αναπτύχθηκε από ένα απλό πρόγραμμα που έγραψε ο Tomlinson προκειμένου να επιτρέψει στους χρήστες υπολογιστών να αφήνουν μηνύματα κειμένου σε άλλους σε έναν υπολογιστή. Η λογική επέκταση αυτού ήταν η αποστολή μηνυμάτων κειμένου μεταξύ υπολογιστών στο διαδίκτυο. Το ηλεκτρονικό ταχυδρομείο έγινε η πιο δημοφιλής εφαρμογή του ARPANET και μέχρι το 1973 η χρήση του ανερχόταν στο 75% του συνόλου της κυκλοφορίας των δεδομένων.

Πώς ταξιδεύει ένα μήνυμα ηλεκτρονικού ταχυδρομείου στο διαδίκτυο; Ακριβώς όπως άλλα είδη δεδομένων που ρέουν στο διαδίκτυο, το ηλεκτρονικό ταχυδρομείο έχει το δικό του πρωτόκολλο. Το **απλό πρωτόκολλο μεταφοράς ταχυδρομείου** (Simple Mail Transfer Protocol – **SMTP**) είναι υπεύθυνο για την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου μέσω του διαδικτύου στον προορισμό τους. Το SMTP ανήκει στο σύνολο πρωτοκόλλων διαδικτύου. Όπως και στις περισσότερες εφαρμογές του διαδικτύου, το ηλεκτρονικό ταχυδρομείο είναι μια εφαρμογή πελάτη/διακομιστή. Κατευθυνόμενα προς τον προορισμό τους, τα μηνύματά σας περνούν μέσα από **διακομιστές ηλεκτρονικού ταχυδρομείου** – εξειδικευμένους υπολογιστές των οποίων η αποκλειστική λειτουργία είναι να αποθηκεύουν, να επεξεργάζονται και να στέλνουν μηνύματα ηλεκτρονικού ταχυδρομείου.

Πού βρίσκονται οι διακομιστές ηλεκτρονικού ταχυδρομείου; Αν ο ISP σας σας παρέχει λογαριασμό ηλεκτρονικού ταχυδρομείου, τότε λειτουργεί έναν διακομιστή ηλεκτρονικού ταχυδρομείου που χρησιμοποιεί το SMTP. Για παράδειγμα, όπως βλέπετε στην Εικόνα 13.17, έστω ότι στέλνετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου στη φίλη σας Μαριάννα. Η Μαριάννα χρησιμοποιεί ως ISP την εταιρεία Verizon. Επομένως, το μήνυμα ηλεκτρονικού ταχυδρομείου από εσάς προς αυτήν προορίζεται για τη διεύθυνση Marianna@verizon.net.

Ας ακολουθήσουμε τώρα αυτό το μήνυμα ηλεκτρονικού ταχυδρομείου:

Βήμα 1. Όταν στέλνετε το μήνυμα ηλεκτρονικού ταχυδρομείου, ο διακομιστής ηλεκτρονικού ταχυδρομείου του ISP σας το παραλαμβάνει.

Βήμα 2. Ο διακομιστής ηλεκτρονικού ταχυδρομείου διαβάζει το όνομα τομέα (verizon.net) και

Κρυπτογράφηση

Στόχος 13.9 *Βελτίωση της ασφάλειας με κρυπτογράφηση δεδομένων.*

Μπορούν να διαβάσουν άλλοι το ηλεκτρονικό ταχυδρομείο μου; Το ηλεκτρονικό ταχυδρομείο είναι πολύ ευάλωτο σε επιθέσεις, επειδή αποστέλλεται με απλό κείμενο. Επιπλέον, αντίγραφα των μηνυμάτων σας μπορεί να υπάρχουν, μόνιμα ή προσωρινά, σε πολλούς διακομιστές, καθώς περνούν από αυτούς μέσω του διαδικτύου προκειμένου να φτάσουν στον προορισμό τους. Για να προστατεύετε εμπιστευτικά μηνύματα ηλεκτρονικού ταχυδρομείου, επιβάλλεται η χρήση κρυπτογράφησης.

Πώς κρυπτογραφώ το ηλεκτρονικό ταχυδρομείο μου; Πολλές υπηρεσίες ηλεκτρονικού ταχυδρομείου προσφέρουν ενσωματωμένη κρυπτογράφηση. Το Hushmail (**hushmail.com**) και το Comodo SecureEmail (**comodo.com**) προσφέρουν δωρεάν εκδόσεις των ασφαλών υπηρεσιών ηλεκτρονικού ταχυδρομείου τους. Μπορείτε να εγγραφείτε στους διαδικτυακούς τόπους τους και να δοκιμάσετε την αποστολή κρυπτογραφημένων μηνυμάτων ηλεκτρονικού ταχυδρομείου τους. Δεν θα χρειαστεί μάλιστα να εγκαταλείψετε τους λογαριασμούς που διατηρείτε ήδη – απλώς χρησιμοποιείτε τον ασφαλή λογαριασμό σας όταν απαιτούνται ασφαλείς επικοινωνίες.

Πώς λειτουργεί η κρυπτογράφηση; Η **κρυπτογράφηση** (encryption) είναι η διαδικασία κωδικοποίησης του ηλεκτρονικού ταχυδρομείου σας έτσι ώστε μόνο το άτομο που κατέχει μία επιπρόσθετη πληροφορία, το κλειδί, να μπορεί να αποκωδικοποιήσει το μήνυμα. Υπάρχουν δύο βασικοί τύποι κρυπτογράφησης:

1. Κρυπτογράφηση ιδιωτικού κλειδιού
2. Κρυπτογράφηση δημόσιου κλειδιού

Τι είναι η κρυπτογράφηση ιδιωτικού κλειδιού; Στην **κρυπτογράφηση ιδιωτικού κλειδιού** (private-key encryption), μόνο τα δύο μέρη που εμπλέκονται στη διαδικασία αποστολής του μηνύματος κατέχουν τον τρόπο, δηλαδή το κλειδί, κρυπτογράφησης/αποκρυπτογράφησης (το ίδιο και για τις δύο αυτές διαδικασίες). Αυτό το κλειδί θα μπορούσε να είναι το αποτέλεσμα μιας απλής μετατόπισης, όπου τα γράμματα της αλφαβήτου μετατοπίζονται σε νέα θέση (βλ. Εικόνα 13.19).

Για παράδειγμα, σε ένα κλειδί που επιτάσσει δεξιά μετατόπιση δύο θέσεων, το γράμμα α γίνεται γ, το β γίνεται δ κ.ο.κ. Εναλλακτικά, το κλειδί θα μπορούσε να ακολουθεί ένα πιο σύνθετο μοτίβο αντικατάστασης (α = θ, β = ρ, γ = ζ κ.λπ.). Το βασικό πρόβλημα που προκύπτει από την κρυπτογράφηση ιδιωτικού κλειδιού είναι η ασφάλεια του κλειδιού. Αν κάποιος κλέψει ένα αντίγραφο του κωδικού ή είναι καλός στην αποκωδικοποίηση, ο κωδικός καταστρέφεται.

Τι είναι η κρυπτογράφηση δημόσιου κλειδιού;

Bits&Bytes — Τυχαίοι αριθμοί: Η κρυπτογράφηση δεν θα ήταν εφικτή χωρίς αυτούς!

Η κρυπτογράφηση ηλεκτρονικού ταχυδρομείου, η κρυπτογράφηση SSL και σχεδόν οτιδήποτε κάνουμε για να διατηρούμε το ιδιωτικό απόρρητό μας στο διαδίκτυο απαιτεί τυχαίους αριθμούς. Η κρυπτογράφηση επιτυγχάνεται με τη χρήση ακολουθιών τυχαίων αριθμών, οι οποίες είναι ακολουθίες αριθμών στις οποίες δεν μπορεί να αναγνωριστεί κανένα μοτίβο. Ακόμα και για μια συναλλαγή ηλεκτρονικού εμπορίου (όπως η αγορά ενός βιβλίου από το **BarnesandNoble.com**) η οποία χρησιμοποιεί κρυπτογράφηση SSL για την κωδικοποίηση του αριθμού της πιστωτικής κάρτας σας, μπορεί να χρειαστούν έως 368 bit τυχαίων δεδομένων. Μόνο 128 bit απαιτούνται για το κλειδί κρυπτογράφησης, αλλά είναι υποχρεωτικό να υπάρχουν και άλλα τυχαία δεδομένα για τη δημιουργία κωδικών αυθεντικοποίησης και για την αποτροπή επιθέσεων επανάληψης. Επιθέσεις επανάληψης ονομάζονται εκείνες οι επιθέσεις κατά τις οποίες οι χάκερ προσπαθούν να αντιγράψουν πακέτα που ταξιδεύουν στο διαδίκτυο και να εξάγουν δεδομένα (όπως κωδικούς κρυπτογράφησης) από αυτά. Οι χάκερ τότε επαναλαμβάνουν (χρησιμοποιούν εκ νέου) τα δεδομένα, ώστε να αποκτήσουν πρόσβαση σε δίκτυα ή συναλλαγές.

Από πού όμως προέρχονται όλοι αυτοί οι τυχαίοι αριθμοί; Η παραγωγή πραγματικά τυχαίων ακολουθιών είναι πιο δύσκολη απ' όσο ακούγεται. Οι περισσότερες γεννήτριες τυχαίων αριθμών είναι στην πραγματικότητα ψευδοτυχαίες, επειδή βασίζονται σε κάποιο είδος αλγόριθμου για την παραγωγή των αριθμών. Το 1998, όμως, ο Mads Haahr της σχολής επιστήμης υπολογιστών και στατιστικής στο Trinity College του Δουβλίνου δημιούργησε τον διαδικτυακό τόπο **random.org**, ο οποίος ασχολείται αποκλειστικά με την παροχή πραγματικά τυχαίων αριθμών για εφαρμογές web, όπως για αλγόριθμους κρυπτογράφησης. Οι αριθμοί παράγονται με βάση τον ατμοσφαιρικό θόρυβο, ο οποίος είναι πραγματικά τυχαίος. Ο θόρυβος συλλέγεται από ραδιόφωνα που δεν συντονίζονται σε συγκεκριμένο σταθμό και άρα εκπέμπουν στατικό ηλεκτρισμό. Οποιοσδήποτε μπορεί να προσπελάσει τον διαδικτυακό τόπο και να λάβει τυχαίους αριθμούς τους οποίους θα χρησιμοποιήσει για κρυπτογράφηση ή άλλες σημαντικές υπηρεσίες, όπως κληρώσεις τυχερών παιχνιδιών. Για περισσότερες πληροφορίες, επισκεφτείτε το **random.org**.

A = C	N = P
B = D	O = Q
C = E	P = R
D = F	Q = S
E = G	R = T
F = H	S = U
G = I	T = V
H = J	U = W
I = K	V = X
J = L	W = Y
K = M	X = Z
L = N	Y = A
M = O	Z = B

Η λέξη
COMPUTER
με την κρυπτογράφηση μετατόπισης δύο θέσεων στα αριστερά γίνεται:

EQORWVGT

Αν δεν έχει κάποιος το κλειδί του κώδικα που βλέπετε (δηλαδή δύο θέσεις μετατόπισης στα δεξιά, που τώρα πρέπει να εφαρμοστεί προς τα αριστερά για την αποκρυπτογράφηση), είναι πολύ δύσκολο να ερμηνεύσει το μήνυμα.

Εικόνα 13.19 Η εγγραφή της λέξης *COMPUTER* με κωδικό κρυπτογράφησης δεξιάς μετατόπισης δύο θέσεων δίνει τη λέξη *EQORWVGT*.

Στην **κρυπτογράφηση δημόσιου κλειδιού** (public-key encryption), δημιουργούνται δύο κλειδιά, το **ζεύγος κλειδιών** (key pair). Χρησιμοποιείται ένα κλειδί για την κρυπτογράφηση και το άλλο για την αποκρυπτογράφηση. Το κλειδί για την κρυπτογράφηση διανέμεται γενικά ως **δημόσιο κλειδί**. Μπορείτε να τοποθετήσετε αυτό το κλειδί στον διαδικτυακό τόπο σας, για παράδειγμα. Οποιοσδήποτε θέλει να σας στείλει ένα μήνυμα μπορεί να πάρει το δημόσιο κλειδί σας και να κρυπτογραφήσει το μήνυμα χρησιμοποιώντας αυτό το κλειδί.

Όταν εσείς παραλάβετε το μήνυμα, χρησιμοποιείτε το **ιδιωτικό κλειδί** σας για να το αποκρυπτογραφήσετε. Είστε ο μόνος που έχει στην κατοχή του αυτό το ιδιωτικό κλειδί και επομένως είναι εξαιρετικά ασφαλές. Τα κλειδιά παράγονται με τέτοιον τρόπο ώστε να λειτουργούν μόνο σε συνεργασία μεταξύ τους. Πρώτα παράγεται το ιδιωτικό κλειδί και έπειτα το δημόσιο κλειδί, με έναν σύνθετο μαθηματικό τρόπο, χρησιμοποιώντας συχνά πληροφορίες από το ιδιωτικό κλειδί. Οι πράξεις είναι τόσο περίπλοκες, που θεωρούνται απαραβίαστες. Αμφότερα τα κλειδιά είναι απαραίτητα για την αποκωδικοποίηση ενός μηνύματος. Αν χαθεί ένα κλειδί, το άλλο είναι εντελώς άχρηστο.

Ποιος τύπος κρυπτογράφησης χρησιμοποιείται στο διαδίκτυο; Η κρυπτογράφηση δημόσιου κλειδιού είναι η πιο συνηθισμένη μέθοδος κρυπτογράφησης στο διαδίκτυο. Υπάρχουν πακέτα δημόσιου κλειδιού, όπως το **Pretty Good Privacy** (**PGP**), που μπορείτε να λάβετε από διαδικτυακούς τόπους, όπως το CNET Downloads (**download.cnet.com**), και μπορείτε συνήθως να τα χρησιμοποιείτε δωρεάν (αν και υπάρχουν πλέον εκδόσεις του PGP που διατίθενται επί πληρωμή). Αφού αποκτήσετε το λογισμικό PGP, μπορείτε να παράγετε ζεύγη κλειδιών για να παίρνετε ένα ιδιωτικό κλειδί εσείς και να παρέχετε ένα δημόσιο κλειδί στον υπόλοιπο κόσμο.

Πώς είναι τα κλειδιά; Τα κλειδιά είναι δυαδικοί αριθμοί. Διαφέρουν σε μέγεθος, ανάλογα με το πόσο ασφαλή πρέπει να είναι. Ένα κλειδί των 12 bit έχει 12 θέσεις και μπορεί να είναι κάπως έτσι:

100110101101

Τα μεγαλύτερα κλειδιά είναι πιο ασφαλή, επειδή μπορούν να πάρουν περισσότερες δυνατές τιμές. Ένα κλειδί με 12 bit παρέχει 4.096 διαφορετικές πιθανές τιμές, ενώ ένα κλειδί με 40 bit προσφέρει 1.099.511.627.776 πιθανές τιμές. Το κλειδί και το μήνυμα περνούν μέσα από έναν σύνθετο αλγόριθμο στο πρόγραμμα κρυπτογράφησης, το οποίο μετατρέπει το μήνυμα σε κάτι μη αναγνωρίσιμο. Κάθε κλειδί μετατρέπει το μήνυμα σε κάποιο διαφορετικό μη αναγνωρίσιμο μήνυμα.

Το ιδιωτικό κλειδί είναι πραγματικά ασφαλές; Λόγω της περιπλοκότητας των αλγόριθμων που χρησιμοποιούνται για την παραγωγή ζευγών κλειδιών, είναι αδύνατο να καταλήξουμε στην ανακάλυψη του ιδιωτικού κλειδιού γνωρίζοντας μόνο το δημόσιο κλειδί. Αυτό, ωστόσο, δεν σημαίνει ότι δεν είναι δυνατό να παραβιαστεί ένα κρυπτογραφημένο μήνυμα. Όπως μάθατε στο Κεφάλαιο 12, έχουμε επιθέσεις ωμής βίας όταν οι χάκερ δοκιμάζουν οποιονδήποτε πιθανό συνδυασμό κλειδιών για την αποκρυπτογράφηση ενός μηνύματος. Αυτός ο τύπος επίθεσης επιτρέπει στους χάκερ να βρίσκουν το κλειδί και να αποκρυπτογραφήσουν το μήνυμα.

Ποιο είδος κλειδιού θεωρείται ασφαλές; Στις αρχές της δεκαετίας του 1990, τα κλειδιά με 40 bit θεωρούνταν απολύτως ανθεκτικά σε επιθέσεις ωμής βίας και αποτελούσαν το πρότυπο για την κρυπτογράφηση. Το 1995, όμως, ένας γάλλος προγραμματιστής χρησιμοποίησε έναν νέο δικό του αλγόριθμο και έβαλε 120 σταθμούς εργασίας να επιχειρήσουν ταυτόχρονα να παραβιάσουν ένα κλειδί με 40 bit. Τελικά πέτυχε τον σκοπό του σε μόλις οχτώ ημέρες. Τότε περάσαμε στα κλειδιά με 128 bit. Με τη χρήση υπερυπολογιστών, όμως, οι ερευνητές έχουν γνωρίσει κάποιες επιτυχίες στις απόπειρές τους να παραβιάσουν κλειδιά με 128 bit. Επομένως, για ισχυρή κρυπτογράφηση πλέον απαιτούνται κλειδιά με 256 bit. Θεωρείται ότι ακόμα και με τους πιο ισχυρούς υπολογιστές που υπάρχουν σήμερα, για την παραβίαση ενός κλειδιού με 256 bit θα χρειαζόμασταν εκατοντάδες δισεκατομμύρια χρόνια.

Οι εταιρείες χρησιμοποιούν ειδική κρυπτογράφηση; Οι επιχειρήσεις πληρώνουν πολλές φορές υπηρεσίες κρυπτογράφησης που παρέχουν και άλλες δυνατότητες, όπως επιβεβαίωση παράδοσης μηνύμα-