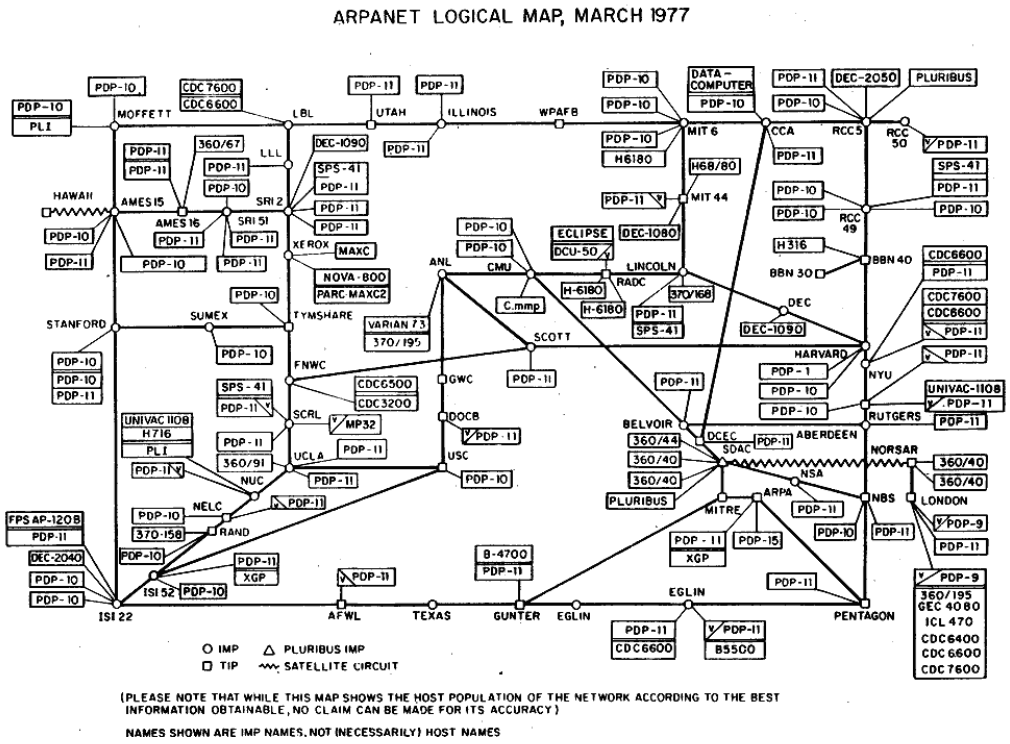
Εργαστηριακή Άσκηση 2
Δικτύωση συστημάτων

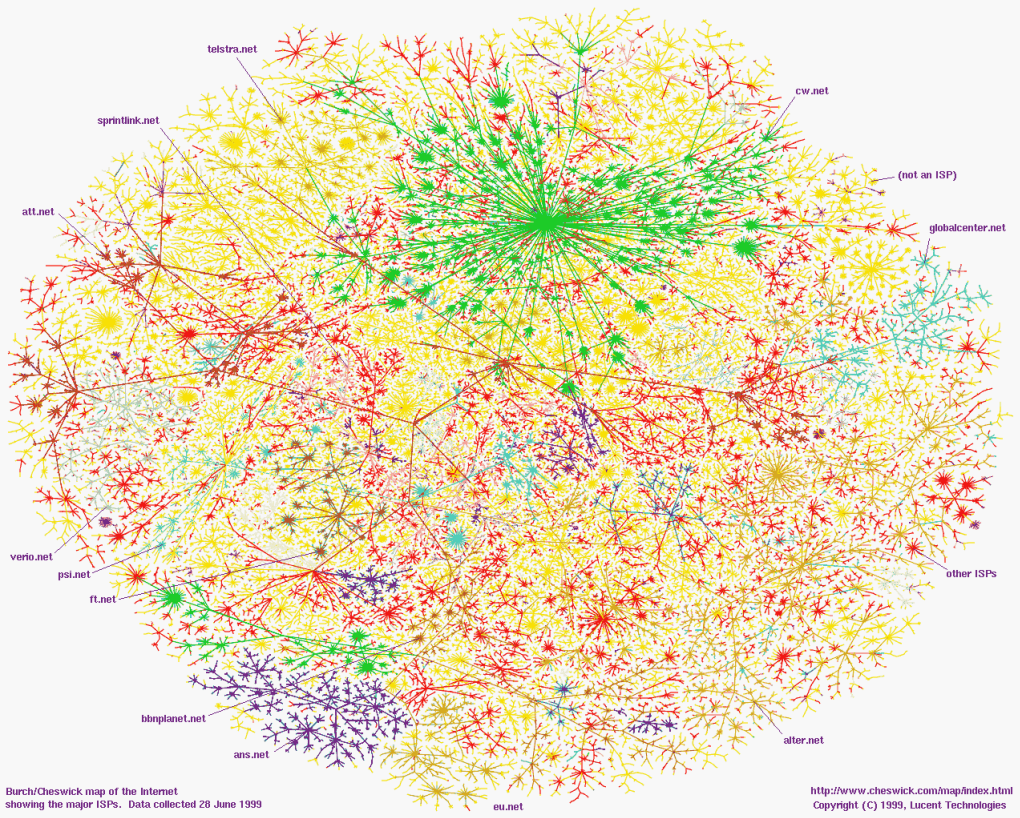
Τα δίκτυα και η δικτύωση υπολογιστικών συστημάτων τα τελευταία 15 χρόνια έχουν μεγαλώσει με εκθετικούς ρυθμούς, επιτρέποντας την ανταλλαγή πληροφοριών και το διαμοιρασμό πόρων. Ένα δίκτυο μπορεί να αποτελείται από κάποια τοπικά περιφερειακά υπολογιστή, όπως, ασύρματα πληκτρολόγια, ή να περιλαμβάνει συνδέσεις σε απομακρυσμένα συστήματα π.χ. για ανταλλαγή αλληλογραφίας μέσω ηλεκτρονικού ταχυδρομείου, περιήγηση στον παγκόσμιο ιστό (www), κατέβασμα αρχείων από εξυπηρετητές σελίδων HTML, και ανταλλαγή αρχείων ήχου και video. Ένας δικτυωμένος υπολογιστής έχει τη δυνατότητα να επεκτείνει τη χρησιμότητά του σε διάφορους τομείς και εν μέρει η επανάσταση των υπολογιστών οφείλεται και σε αυτή τη δυνατότητα. Στην εποχή μας όταν μιλάμε για δικτύωση εννοούμε κυρίως TCP/IP ή/και Ethernet.

Η σουίτα πρωτοκόλλων του Internet

Η αρχιτεκτονική στην οποία βασίζεται το Internet στη μορφή που το γνωρίζουμε σήμερα είναι το TCP/IP. Το TCP/IP είναι ένα σύνολο πρωτοκόλλων επικοινωνίας που έχει τις ρίζες του στο έργο ARPANET (Advanced Research Projects Agency Network) του Υπουργείου Εθνικής Άμυνας των Ηνωμένων Πολιτειών τη δεκαετία του 1970. Το ARPANET είναι ιδιαίτερα σημαντικό, επειδή εισήγαγε την έννοια της διαδικτύωσης (internetworking), όπου πολλαπλά ξεχωριστά δίκτυα ενώθηκαν σε ένα ενιαίο δίκτυο-δικτύων. Σχηματική απεικόνιση του ARPANET το 1977:



Το δίκτυο αυτό ήταν η βάση της δημιουργίας του internet, το οποίο με την πάροδο των χρόνων εξαπλώθηκε σε όλο τον κόσμο. Σχηματική απεικόνιση του Internet το 1999:



Πιο πρόσφατες απεικονίσεις υπάρχουν στα http://global-internet-map-2012.telegeography.com/ και http://www.submarinecablemap.com/. Περισσότερες πληροφορίες μπορείτε να βρείτε στους παρακάτω συνδέσμους:

http://www.columbia.edu/~rh120/other/tcpdigest_paper.txt
http://www.cs.utexas.edu/~chris/think/ARPANET/Technical_Tour/overview.shtml
http://www.livinginternet.com/i/ii_arpanet.html
http://www.newmedia.org/history-of-the-internet.html
http://www.computerhistory.org/internet_history/

Ο τρόπος λειτουργίας ενός δικτύου TCP/IP παραμένει ο ίδιος, ανεξάρτητα από το μέγεθος του. Αυτό μας διευκολύνει ιδιαίτερα στη μελέτη του, φτιάχνοντας και δοκιμάζοντας διάφορες τοπολογίες σε μικρογραφία. Η πιο απλή από αυτές είναι η τοπολογία ενιαίου τμήματος, όπως αυτή που θα δούμε παρακάτω. Όσοι έχουν στο σπίτι τους σύνδεση στο internet έχουν ήδη μια τέτοια τοπολογία σε λειτουργία, στο τοπικό δίκτυο μεταξύ του υπολογιστή και του router τους. Με τη βοήθεια του VirtualBox θα φτιάξουμε κάτι αντίστοιχο και στα επόμενα εργαστήρια θα έχουμε την ευκαιρία να ασχοληθούμε και με πιο πολύπλοκα δίκτυα.

Δικτύωση στο VirtualBox

Το VirtualBox είναι το εργαλείο που θα μας βοηθήσει να χτίσουμε μικρά δίκτυα. Το VirtualBox μπορεί για κάθε εικονικό μηχάνημα να εξομοιώσει έως 8[1] κάρτες δικτύου και η κάθε κάρτα μπορεί να λειτουργήσει με έναν από τους παρακάτω τρόπους: χωρίς σύνδεση, NAT, γεφύρωση, εσωτερικό δίκτυο, μόνο με το φιλοξενούν και γενική δικτύωση. Περισσότερες πληροφορίες για τους τρόπους δικτύωσης που προσφέρει το VirtualBox θα βρείτε στην ιστοσελίδα του εγχειριδίου

[1] Μέσω του γραφικού περιβάλλοντος μπορείτε να ορίσετε μόνο τις 4. Για τις υπόλοιπες πρέπει να χρησιμοποιήσετε την εντολή φλοιού `VboxManage`

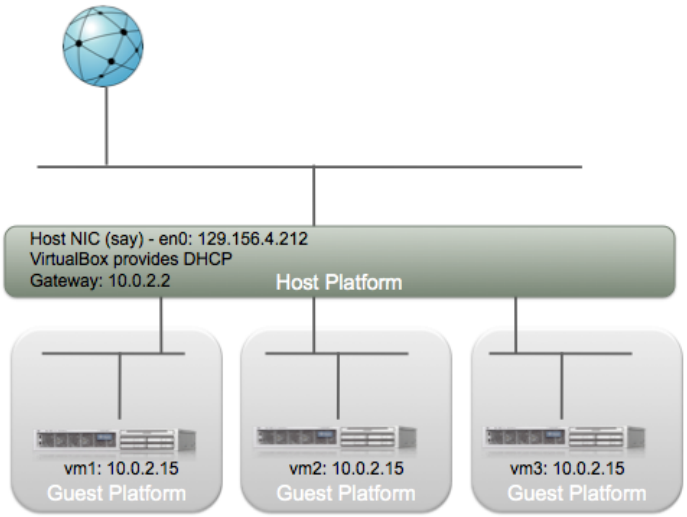
http://www.virtualbox.org/manual/ch06.html. Επίσης μια πολύ καλή περιγραφή υπάρχει στην ιστοσελίδα https://blogs.oracle.com/fatbloke/entry/networking_in_virtualbox1, από όπου έχουμε πάρει και τα επεξηγηματικά σχήματα που θα δείτε πιο κάτω. Τέλος, αρκετές χρήσιμες πληροφορίες, όχι μόνο για τη δικτύωση στο VirtualBox, θα βρείτε στην http://www.dedoimedo.com/computers/virtualbox-network-sharing.html όπως και στην http://www.thegeekstuff.com/2012/03/virtualbox-guest-additions/. Στη συνέχεια παρατίθεται μια σύντομη περιγραφή των διαθέσιμων τρόπων δικτύωσης.

Χωρίς σύνδεση (Not attached)

Σε αυτόν τον τρόπο δικτύωσης το VirtualBox δηλώνει στο φιλοξενούμενο μηχάνημα την ύπαρξη κάρτας δικτύου, η οποία όμως δεν είναι συνδεδεμένη, σα να έχετε αποσυνδέσει το καλώδιο Ethernet. Με αυτόν τον τρόπο λειτουργίας μπορείτε να εξομοιώσετε την αφαίρεση του καλωδίου από ένα μηχάνημα, πράγμα που θα οδηγήσει το λειτουργικό του σύστημα σε επανακαθορισμό των δικτυακών ρυθμίσεων.

NAT (Network Address Translation)

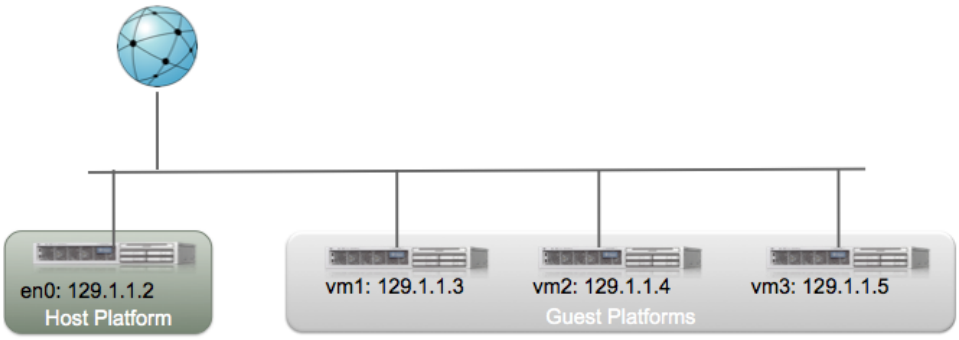
Αυτή είναι η προεπιλεγμένη λειτουργία για νέα εικονικά μηχανήματα, κατάλληλη για απλές περιπτώσεις δικτύωσης, όπου το εικονικό μηχάνημα χρειάζεται να κάνει μόνο εξερχόμενες συνδέσεις (τύπου πελάτη). Π.χ. για ένα PC που θέλει να επισκεφτεί μια σελίδα στο διαδίκτυο. Κατά την εκκίνηση, το φιλοξενούμενο μηχάνημα χρησιμοποιεί DHCP για να ζητήσει διεύθυνση IP. Το VirtualBox παρέχει πάντα τη διεύθυνση 10.0.2.15 και έτσι το κάθε φιλοξενούμενο μηχάνημα έχει την εντύπωση ότι βρίσκεται στο δικό του ξεχωριστό δίκτυο όπως φαίνεται στο σχήμα. Η προεπιλεγμένη πύλη είναι το VirtualBox στο φιλοξενούν μηχάνημα, έχοντας ως διεύθυνση IP την 10.0.2.2. Όταν το φιλοξενούμενο μηχάνημα στέλνει κίνηση μέσω της πύλης προς το διαδίκτυο, το VirtualBox μεταφράζει τις διευθύνσεις IP ώστε τα πακέτα να φαίνονται ότι ξεκινούν από το φιλοξενούν μηχάνημα. Η έναρξη επικοινωνίας από το διαδίκτυο προς το φιλοξενούμενο μηχάνημα δεν είναι εφικτή.



Σε αυτόν τον τρόπο δικτύωσης, το φιλοξενούμενο μηχάνημα θα συνεχίσει να λειτουργεί ακόμα και αν το φιλοξενούν αλλάξει δίκτυο, π.χ. ένας φορητός υπολογιστής που αλλάζει μεταξύ Wi-Fi και καλωδίου ή 3G. Η τεχνική NAT χρησιμοποιείται ευρέως και στα πραγματικά δίκτυα, όπως π.χ. στον δρομολογητή DSL ενός τυπικού οικιακού δικτύου για τον διαμοιρασμό της σύνδεσης προς το διαδίκτυο.

Γεφύρωση (Bridged Networking)

Στην δικτύωση NAT κάποιος από έξω δεν μπορεί να εγκαταστήσει επικοινωνία με το φιλοξενούμενο μηχάνημα. Π.χ. εάν το φιλοξενούμενο μηχάνημα είναι ένας εξυπηρετητής ιστού, αυτός δεν θα είναι προσβάσιμος από το διαδίκτυο. Σε τέτοιες περιπτώσεις χρησιμοποιείται η γεφύρωση. Με τη γεφύρωση το εικονικό σύστημα φαίνεται να είναι συνδεδεμένο ως εάν ήταν φυσικό μηχάνημα, ισότιμο με το φιλοξενούν. Η εικονική κάρτα δικτύου γεφυρώνεται με την πραγματική όπως φαίνεται στο σχήμα.

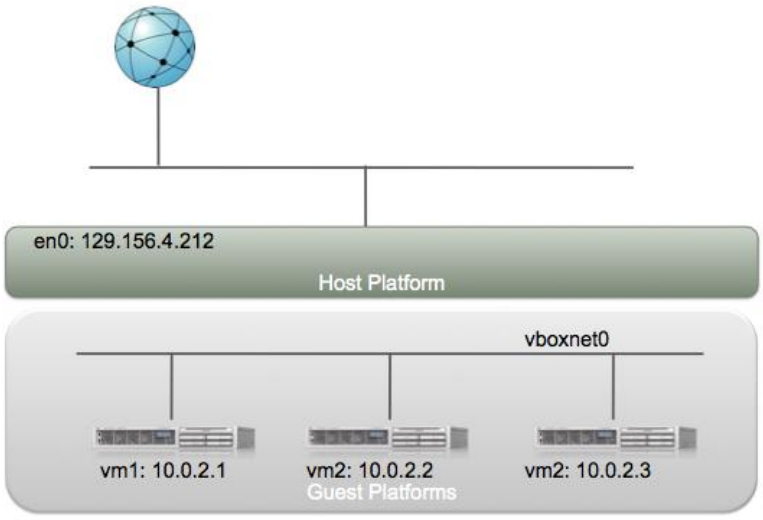


Το αποτέλεσμα είναι ότι τα μηχανήματα (φιλοξενούν και φιλοξενούμενα) βρίσκονται στο ίδιο τοπικό δίκτυο, έχοντας πρόσβαση στις ίδιες υπηρεσίες του πραγματικού δικτύου, όπως εξωτερικοί εξυπηρετητές DHCP, DNS και προεπιλεγμένες πύλες για δρομολόγηση IP. Το μειονέκτημα αυτής της λειτουργίας είναι ότι για κάθε εικονικό μηχάνημα απαιτείται μια διεύθυνση IP από το υποδίκτυο στο οποίο βρίσκεται το φιλοξενούν μηχάνημα. Εάν δημιουργηθούν πολλά εικονικά μηχανήματα, καθώς όλα θα ανήκουν στο ίδιο υποδίκτυο, ίσως υπάρξει πρόβλημα στην απόδοση διευθύνσεων IP είτε δυναμικά μέσω DHCP είτε στατικά. Επίσης αν το φιλοξενούν μηχάνημα έχει πολλαπλές κάρτες δικτύου, π.χ. είναι φορητός υπολογιστής με ασύρματη και ενσύρματη κάρτα, σε περίπτωση αλλαγής δικτύου θα πρέπει να γίνει ρύθμιση της γεφύρωσης εκ νέου.

Στις ασκήσεις δεν θα χρησιμοποιήσουμε αυτόν τον τρόπο λειτουργίας καθώς θα εξαντλούσαμε τις διαθέσιμες διευθύνσεις του Εργαστηρίου Προσωπικών Υπολογιστών που αποδίδονται δυναμικά με DHCP. Μπορείτε όμως άνετα να το δοκιμάσετε στο σπίτι σας, σε συνδυασμό με έναν δρομολογητή DSL.

Εσωτερικό δίκτυο (Internal Networking)

Με αυτόν καθώς και τον επόμενο τρόπο λειτουργίας μπορείτε να κάνετε δοκιμές και πειράματα, χωρίς να υπάρχει πιθανότητα να δημιουργηθούν προβλήματα στα εξωτερικά δίκτυα ή να χρειαστεί να έρθετε σε επαφή με τους διαχειριστές των δικτύων αυτών. Στην περίπτωση εσωτερικού δικτύου, το VirtualBox μας εξασφαλίζει ότι όλη η κίνηση από τα εικονικά μηχανήματα θα παραμείνει εσωτερικά στο φιλοξενούν μηχάνημα και θα είναι ορατή μόνο στα άλλα εικονικά μηχανήματα του ίδιου εσωτερικού δικτύου. Το επόμενο σχήμα δείχνει μια τοπολογία εσωτερικού δικτύου στο VirtualBox.

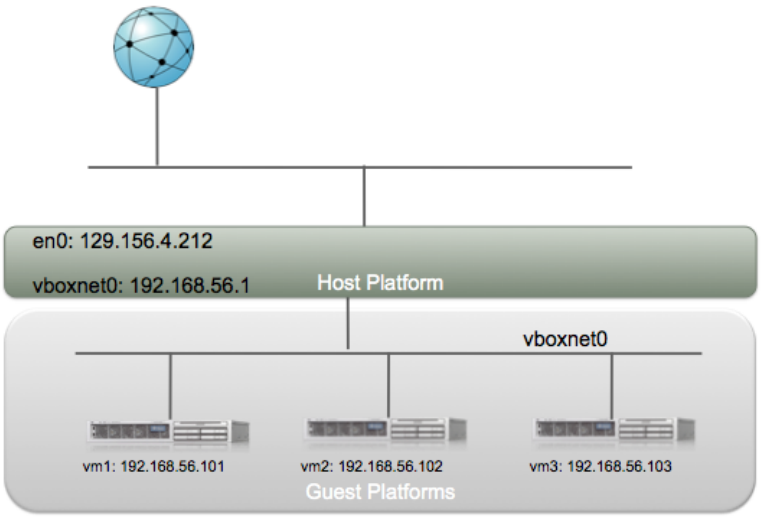


Μπορείτε να ορίσετε όσα εσωτερικά δίκτυα θέλετε ορίζοντας διαφορετικά ονόματα δικτύου. Τα εσωτερικά δίκτυα (στο παράδειγμα "vboxnet0") βρίσκονται εντελώς απομονωμένα, κάτι το οποίο είναι ιδιαίτερα βολικό για δοκιμές ή όταν χρειαζόμαστε ένα ξεχωριστό, καθαρό δίκτυο για να δημιουργήσουμε δικές μας τοπολογίες. Μπορείτε να εγκαταστήσετε εξυπηρετητές για DHCP, DNS, Active Directory, δρομολόγηση, κλπ. Πρέπει να σημειωθεί ότι σε αυτό τον τρόπο δικτύωσης το φιλοξενούν μηχάνημα δεν συμμετέχει, κάτι το οποίο μπορεί να είναι χρήσιμο σε περιπτώσεις που δεν υπάρχει φυσικό δίκτυο π.χ. σε αεροπορικό ταξίδι και τα εικονικά μηχανήματα δεν θα μπορούσαν να λειτουργήσουν διαφορετικά.

Στην εσωτερική δικτύωση το VirtualBox δεν προσφέρει βοηθητικές υπηρεσίες όπως DHCP, οπότε τα εικονικά μηχανήματα πρέπει να είναι στατικά ρυθμισμένα ή κάποιο από όλα να παρέχει τις απαραίτητες υπηρεσίες (συνήθως DHCP και DNS). Είναι επίσης δυνατό να δημιουργηθούν πολλαπλά εσωτερικά δίκτυα και τα εικονικά μηχανήματα με πολλαπλές κάρτες να βρίσκονται σε παραπάνω από ένα, παρέχοντας δρομολόγηση εάν αυτό χρειάζεται.

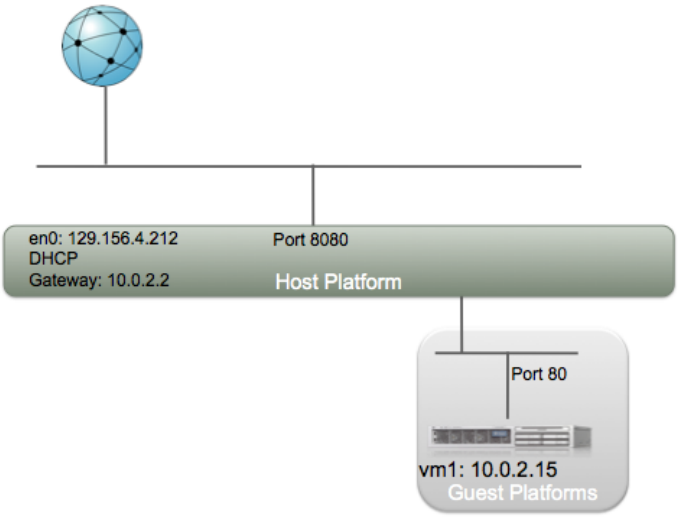
Μόνο με το φιλοξενούν (Host-only)

Αντίστοιχα με την εσωτερική δικτύωση, αλλά για πιο απλή χρήση, διατίθεται η δυνατότητα δικτύωσης μόνο με το φιλοξενούν μηχάνημα. Ο τρόπος αυτός μοιάζει με το εσωτερικό δίκτυο, με τη διαφορά ότι στο δίκτυο συμμετέχει και το φιλοξενούν μηχάνημα, με μια εικονική κάρτα δικτύου με διεύθυνση IP την 192.168.56.1 όπως φαίνεται στο επόμενο σχήμα. Όλα τα εικονικά μηχανήματα έχουν επικοινωνία μεταξύ τους όπως και με το φιλοξενούν. Εξωτερικά συστήματα όμως δεν μπορούν να επικοινωνήσουν με τα εσωτερικά, εξ ου και η ονομασία. Επειδή το φιλοξενούν μηχάνημα έχει επαφή με το εσωτερικό δίκτυο, μπορεί να παρέχει την υπηρεσία DHCP. Οι ρυθμίσεις για τον εξυπηρετητή DHCP μπορούν να γίνουν από το μενού File-->Preferences --> Network του VirtualBox κάνοντας κλικ στον εμφανιζόμενο Host Only Ethernet Adapter.



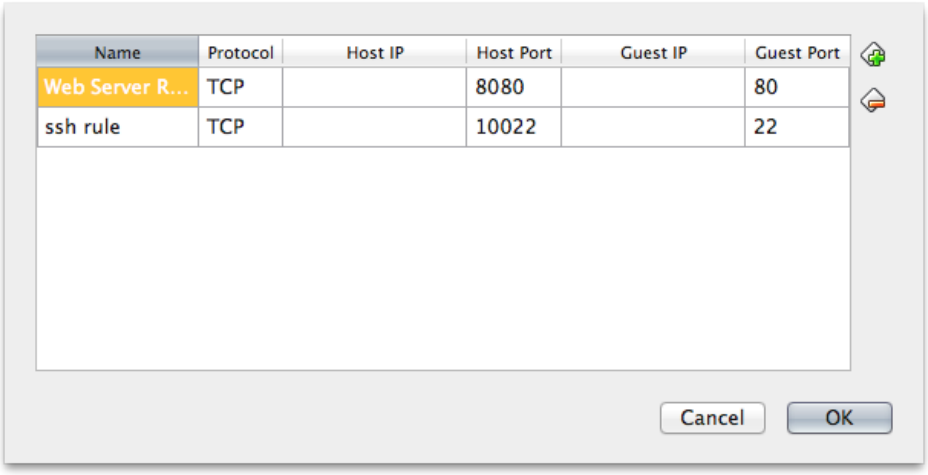
NAT και Port-Forwarding

Αποτελεί επέκταση της λειτουργικότητας του NAT. Αν και η συγκεκριμένη λειτουργία δε θα μας χρειαστεί στα πλαίσια του εργαστηρίου, μπορεί να χρησιμεύσει αλλού, όπως σε περιπτώσεις που υπάρχει ανάγκη να αποκτηθεί πρόσβαση σε κάποιο από τα εικονικά μηχανήματα και το εξωτερικό δίκτυο αλλάζει συχνά (π.χ. σε έναν φορητό υπολογιστή που μετακινείται). Η λειτουργία NAT δεν θα μπορούσε να λειτουργήσει μόνη της, αφού πρέπει να υπάρχει επικοινωνία από έξω. Η λειτουργία γεφύρωσης θα μπορούσε, αλλά θα χρειαζόταν συνεχώς να αλλάζουν οι ρυθμίσεις δικτύου του εικονικού μηχανήματος για κάθε νέο δίκτυο. Οι λειτουργίες εσωτερικού δικτύου και host only δε θα μπορούσαν και αυτές, αφού τα εικονικά μηχανήματα δεν θα ήταν προσβάσιμα από έξω. Όμως η λειτουργία NAT που προσφέρει το VirtualBox μπορεί να συνδυαστεί με port-forwarding και να επιτρέψει δικτύωση όπως στο σχήμα.



Για τον σκοπό αυτό θα επιλέγατε το Advanced στο μενού δικτύωσης του εικονικού μηχανήματος και μετά θα κάνατε κλικ στο Port Forwarding. Εκεί εμφανίζεται ένα παράθυρο όπου μπορείτε να γράψετε τους επιθυμητούς κανόνες προώθησης. Για παράδειγμα στο επόμενο σχήμα βλέπετε δύο κανόνες που επιτρέπουν την προώθηση συνδέσεων από το φιλοξενούν μηχάνημα στις πόρτες 8080/tcp και 10022/tcp, προς το εικονικό στις πόρτες 80/tcp και 22/tcp, αντίστοιχα. Με τον τρόπο αυτό μπορείτε να εγκαταστήσετε ένα εξυπηρετητή ιστού στο εικονικό μηχάνημα καθώς και να

συνδεθείτε με SSH σε αυτό από τον έξω κόσμο. Σε περίπτωση ενεργοποιημένου firewall στο φιλοξενούν μηχάνημα όμως θα πρέπει να επιτραπούν οι επιθυμητές πόρτες αντίστοιχα.



Γενική δικτύωση (generic networking)

Πρόκειται για μια ειδική περίπτωση, όπου ο χρήστης παρέχει τον οδηγό δικτύωσης για το VirtualBox. Υποστηρίζονται δύο υποπεριπτώσεις: σήραγγες UDP και VDE (Virtual Distributed Ethernet).

Από όλα τα παραπάνω φαίνεται ότι το VirtualBox μπορεί να προσφέρει πολλές δυνατότητες δικτύωσης και να φιλοξενήσει πολύπλοκες δικτυακές τοπολογίες που μπορούν να βοηθήσουν στην καλύτερη κατανόηση των μηχανισμών που χρησιμοποιούνται στο διαδίκτυο.

Άσκηση 1: TCPDUMP

Ανάλυση δικτυακών πρωτοκόλλων

Για να μελετήσουμε τη συμπεριφορά των δικτύων σε βάθος θα χρησιμοποιήσουμε εργαλεία που μπορούν να καταγράψουν τη δικτυακή κίνηση και να την αποτυπώσουν σε αναγνώσιμη μορφή. Τέτοια εργαλεία αναφέρονται ως προγράμματα καταγραφής πακέτων ή προγράμματα ανάλυσης δικτυακών πρωτοκόλλων. Στο εργαστήριο θα χρησιμοποιήσουμε τα tcpdump και wireshark. Το wireshark είναι γνωστό από το μάθημα των Δικτύων Υπολογιστών. Το tcpdump είναι παρόμοιο, αλλά σε γραμμή εντολών UNIX. Σας επιτρέπει να συλλάβετε δικτυακή κίνηση και να εμφανίσετε τις επικεφαλίδες των πακέτων.

Τα προγράμματα αυτά θέτουν την κάρτα δικτύου σε ένα τρόπο λειτουργίας που ονομάζεται promiscuous mode, όπου η κάρτα δικτύου προωθεί στο λειτουργικό σύστημα για καταγραφή όλη την κίνηση που ακούει στο δίκτυο και όχι μόνο αυτήν που απευθύνεται στη συγκεκριμένη κάρτα. Συνήθως, μόνο ο διαχειριστής του συστήματος έχει δικαίωμα να τρέχει τέτοιου είδους προγράμματα, οπότε θα χρησιμοποιήσετε τον χρήστη “root” για καταγραφή.

Το tcpdump δημιουργήθηκε το 1987 στο εργαστήριο Lawrence Berkeley του Υπουργείου Ενέργειας των Ηνωμένων Πολιτειών της Αμερικής. Από το 1990 και έπειτα, διανέμεται ως λογισμικό ανοιχτού κώδικα και έχει ενσωματωθεί σχεδόν σε όλα τα λειτουργικά συστήματα τύπου UNIX. Θα βρείτε όλες τις πληροφορίες σχετικά με το tcpdump στην επίσημη ιστοσελίδα του

http://www.tcpdump.org/. Για μια σύντομη εισαγωγή στη χρήση του ανατρέξτε στην ιστοσελίδα http://danielmiessler.com/study/tcpdump/.

Χρησιμοποιείστε την εντολή man tcpdump για να δείτε πληροφορίες σχετικά με τη σύνταξή της. Στον παρακάτω πίνακα συνοψίζονται οι βασικές επιλογές.

-i interface	Καταγραφή στο συγκεκριμένο προσαρμογέα δικτύου. Σε συστήματα με μια κάρτα δικτύου μπορεί να παραλείπεται.
-n	Παραλείπει τις ερωτήσεις στους εξυπηρετητές DNS για μετάφραση των διευθύνσεων IP σε host/domain names. Γενικά ως επιλογή προτείνεται, γιατί χωρίς αυτή το tcpdump δημιουργεί από μόνο του δικτυακή κίνηση.
-x	Τυπώνει στην οθόνη τα πρώτα 68 bytes κάθε πακέτου σε δεκαεξαδική μορφή.
-l	Μπορεί να χρησιμοποιηθεί σε συνδυασμό με εντολές ανακατεύθυνσης για να καταγραφεί το αποτέλεσμα σε αρχείο.
-w	Αποθήκευση σε αρχείο. Τα αρχεία αυτά είναι συμβατά με όλα τα αντίστοιχα εργαλεία, συμπεριλαμβανομένου και του wireshark.
-r	Ανάγνωση από αρχείο.

Στην πραγματικότητα, για τη σύλληψη πακέτων από την κάρτα δικτύου το tcpdump χρησιμοποιεί τη βιβλιοθήκη σύλληψης πακέτων pcap (Packet Capture Library). Για να συλλάβει πακέτα η pcap απαιτούνται δικαιώματα διαχειριστή. Χρησιμοποιείστε την εντολή man pcap για περισσότερες πληροφορίες. Μπορείτε να περιορίσετε την κίνηση που θα καταγράψει το tcpdump χρησιμοποιώντας φίλτρα, όπως και στο wireshark. Τα φίλτρα ορίζονται μέσω του ορισμού μιας έκφρασης (expression). Η έκφραση αποτελείται από μία ή περισσότερες στοιχειώδεις προτάσεις (primitives). Δείτε man pcap-filter για τις λεπτομέρειες. Στον παρακάτω πίνακα έχουν αποτυπωθεί οι πιο σημαντικές:

type	Δηλώνει το είδος ταυτότητας (αριθμό ή όνομα) στο οποίο αναφέρεται. Το type μπορεί να είναι: host για υπολογιστή, net για δίκτυο, port για θύρα και portrange για περιοχή τιμών θυρών. Εάν δεν δηλώσετε τίποτε υπονοείται host.
dir	Δηλώνει την κατεύθυνση από ή προς. Το dir μπορεί να είναι scr όταν ορίζουμε την ταυτότητα της πηγής, dst για την ταυτότητα προορισμού, src or dst, src and dst, κλπ. Εάν παραληφθεί, υπονοείται src or dst.
proto	Δηλώνει το είδος πρωτοκόλλου, π.χ. με icmp περιορίζουμε τη σύλληψη κίνησης σε πακέτα πρωτοκόλλου ICMP, με ip σε πακέτα IP, με ether σε πλαίσια Ethernet. Άλλες επιλογές είναι ipv6, arp, rarp, tcp, upd, κλπ.

Μπορείτε να συνδυάσετε τις προτάσεις με τέτοιο τρόπο ώστε να συλλάβετε μόνο την κίνηση που σας ενδιαφέρει χρησιμοποιώντας τους τελεστές:

1. AND (“and” or “&&”)
2. OR (“or” or “||”)
3. EXCEPT (“not” or “!”)

είτε ομαδοποιώντας τες. Για παράδειγμα, με tcpdump 'src 10.0.5.5 and (dst port 3389 or 22)' θα καταγράψετε κίνηση από τον υπολογιστή 10.0.5.5 που προορίζεται για τις θύρες 3389 (απομακρυσμένη επιφάνεια εργασίας) ή 22 (SSH).

Με τη βοήθεια των προηγουμένων απαντήστε τις παρακάτω ερωτήσεις.

1.1 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε όλα τα πακέτα από την κάρτα δικτύου em0;
1.2 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε όλα τα πακέτα από την κάρτα δικτύου em0 και να εμφανίσετε τα πρώτα 68 bytes κάθε πακέτου;
1.3 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε πακέτα ICMP με αποστολέα ή παραλήπτη την IP διεύθυνση 10.0.0.1;
1.4 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε πακέτα IP μεταξύ δύο συστημάτων με διευθύνσεις IP 10.0.0.1 και 10.0.0.2 στην κάρτα δικτύου em0;
1.5 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε IP πακέτα εκπομπής;
1.6 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε τεμάχια TCP με διεύθυνση αποστολέα ή παραλήπτη 10.0.0.10;
1.7 Τροποποιήστε την εντολή της παραπάνω ερώτησης, ώστε να εμφανίζονται μόνο όσα τεμάχια εξ αυτών προορίζονται για την TCP θύρα 23, και τα αποτελέσματα να αποθηκεύονται στο αρχείο "sample_capture".
1.8 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε τεμάχια TCP που περιέχουν **μόνο** τη σημαία SYN;
1.9 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε τα πρώτα δύο τεμάχια της τριμερούς χειραψίας TCP;

Άσκηση 2: Δικτύωση Host-only

Εντοπίστε στην επιφάνεια εργασίας τη συντόμευση για το VirtualBox και ξεκινήστε το. Ακολουθείστε την διαδρομή *File --> Import Appliance ...* και στην οθόνη που θα εμφανισθεί κάντε κλικ στο *Open appliance ...* . Αναζητείστε τον φάκελο *C:\VMs* και επιλέξτε το αρχείο FreeBSD. Κάντε κλικ στο Next και μετά στο Import. Στην καρτέλα που θα εμφανισθεί, αλλάξτε το όνομα της συσκευής σε PC1 και επιλέξτε τη ρύθμιση "Reinitialize the MAC address". Επαναλάβετε την ίδια διαδικασία θέτοντας τη δεύτερη φορά το όνομα σε PC2. Το VirtualBox θα φορτώσει δύο εικονικά μηχανήματα που θα φαίνονται με ονόματα PC1 και PC2. Ξεκινήστε και τα δύο και κάντε login ως διαχειριστής "root" με συνθηματικό "ntua".

Απαντήστε τις κατωτέρω ερωτήσεις καταγράφοντας παράλληλα, όπου απαιτήθηκε, την ακριβή σύνταξη των εντολών που χρησιμοποιήσατε.

2.1 Ποιες είναι οι διευθύνσεις IPv4 που έχει αποδώσει το VirtualBox στα μηχανήματα;
2.2 Πώς θα καταλάβετε αν τα δύο μηχανήματα επικοινωνούν μεταξύ τους;
2.3 Πώς θα καταλάβετε αν το φιλοξενούν μηχάνημα επικοινωνεί με τα δύο μηχανήματα;
2.4 Ποια είναι η σύνταξη της εντολής που θα σας δείξει την προεπιλεγμένη πύλη;

2.5 Υπάρχει προεπιλεγμένη πύλη στην συγκεκριμένη κατάσταση δικτύωσης; Τεκμηριώστε την απάντησή σας.

2.6 Ποιο είναι το όνομα των μηχανημάτων όπως το αντιλαμβάνεται το λειτουργικό τους σύστημα;

2.7 Αλλάξετε τα ονόματα, όπως τα αντιλαμβάνεται το λειτουργικό τους σύστημα, των δυο εικονικών συστημάτων ώστε να ταυτιστούν με τα ονόματα PC1 και PC2, αντίστοιχα, που έχουν στο VirtualBox.

Χρησιμοποιήστε τον συνδυασμό πλήκτρων CTRL+D ή την εντολή "exit" για να εξέλθετε και εισέλθετε πάλι (login).

2.8 Χωρίς χρήση κάποιας εντολής, επιβεβαιώστε ότι το όνομα άλλαξε. Που εμφανίζεται αυτό στον φλοιό;

2.9 Περιέχει το αρχείο παραμετροποίησης /etc/rc.conf στο PC1 το νέο όνομα; Σε ενδεχόμενη επανεκκίνηση του PC1 ποιο θα είναι το όνομά του;

2.10 Τι πρέπει να κάνετε, ώστε στην επόμενη επανεκκίνηση τα μηχανήματα να έχουν τα νέα ονόματα;

2.11 Τι πρέπει να προσθέσετε και σε ποια αρχεία για να μπορείτε να χρησιμοποιείτε τα ονόματα των μηχανημάτων αντί των IP διευθύνσεών τους στις διάφορες δικτυακές εντολές;

2.12 Γράψτε ένα παράδειγμα σύνταξης κάποιας εντολής, στην οποία χρησιμοποιείται η λειτουργία που προσφέρει το αρχείο hosts, ώστε να μη χρειάζεται να ορίσουμε διεύθυνση IP.

Θα χρησιμοποιήσετε τώρα το tcpdump για να δείτε την κίνηση που παράγεται όταν εκτελείτε την εντολή ping. Στο PC2 ξεκινήστε το tcpdump ώστε να συλλαμβάνει όλα τα πακέτα ICMP που περιέχουν τη διεύθυνση IP του PC1. Στο PC1 εκτελέστε την εντολή "ping -c 4 PC2". Στο PC2 παρατηρείστε στην οθόνη και καταγράψτε σε αρχείο με όνομα test την κίνηση που παράγει η εντολή ping.

2.13 Καταγράψτε δύο τρόπους με τους οποίους μπορείτε να χρησιμοποιήσετε την εντολή tcpdump ώστε να καταγράφετε την κίνηση σε αρχείο ενώ παράλληλα την παρατηρείτε στην οθόνη. *[Υποδ.: Αναζητήστε στις σελίδες man του tcpdump τη χρήση της επιλογής -l]*.

2.14 Ποιο είναι το μήκος και ποια είναι η τιμή του πεδίου TTL των πακέτων ICMP που ανταλλάσσουν τα δύο μηχανήματα.

2.15 Κάντε τώρα ping στη διεύθυνση του φιλοξενούντος μηχανήματος. Ποια είναι η τιμή του πεδίου TTL;

Ξεκινήστε τώρα μια νέα καταγραφή στο PC2 ώστε να συλλαμβάνετε μόνο πακέτα ICMP και να τα εμφανίζετε με όσο πιο πολλές λεπτομέρειες. Στη συνέχεια ανοίξτε ένα παράθυρο εντολών στο φιλοξενούν μηχάνημα και κάντε ping στη διεύθυνση IP του PC2.

2.16 Ποια είναι η σύνταξη της εντολής tcpdump που χρησιμοποιήσατε;

2.17 Ποιο είναι το μήκος των πακέτων ICMP που παράγει το φιλοξενούν μηχάνημα; Γιατί διαφέρει από το μήκος που παρατηρήσατε πριν;

2.18 Ποια είναι η τιμή του πεδίου TTL των πακέτων ICMP που ανταλλάσσουν τα δύο μηχανήματα; Συμφωνεί με τις τιμές που βρήκατε προηγουμένως;

Άσκηση 3: Δικτύωση Internal

Από τη διαδρομή *Machine* --> *Settings* --> *Network* αλλάξτε τις ρυθμίσεις δικτύου του PC2 από "Host Only" σε "Internal Network".

Απαντήστε τις παρακάτω ερωτήσεις καταγράφοντας παράλληλα, όπου απαιτήθηκε, την ακριβή σύνταξη των εντολών που χρησιμοποιήσατε.

3.1 Από το φιλοξενούν μηχάνημα μπορείτε να επικοινωνήσετε με κάποιο από τα δύο εικονικά μηχανήματα;
3.2 Επικοινωνούν τα δύο εικονικά μηχανήματα μεταξύ τους;
3.3 Αλλάξτε και τις ρυθμίσεις δικτύου του PC1 μηχανήματος αντίστοιχα με το PC2. Επικοινωνούν τώρα τα δυο εικονικά μηχανήματα;
3.4 Από το φιλοξενούν μηχάνημα μπορείτε να επικοινωνήσετε με κάποιο από τα δύο εικονικά μηχανήματα; Τεκμηριώστε την απάντησή σας.
3.5 Ξεκινήστε μια καταγραφή με tcpdump στο PC1 ώστε να εμφανίζεται όλη η κίνηση που διέρχεται στο εσωτερικό δίκτυο. Στη συνέχεια στο PC2, αφού αδειάσετε τον πίνακα arp (δείτε σχετική σελίδα man), κάντε ping στη διεύθυνση του φιλοξενούντος μηχανήματος. Τι είδους μηνύματα παρατηρείτε ότι παράγει το PC2;
3.6 Πώς εξηγείτε το μήνυμα host is down που επιστρέφει το ping;
3.7 Αλλάξτε τη διεύθυνση IP των δύο συστημάτων χρησιμοποιώντας τις τελευταίες 2 διαθέσιμες διευθύνσεις IP από το υποδίκτυο 10.10.10.0/25.
3.8 Τι σημαίνει το μήνυμα λάθους που βλέπετε;
3.9 Επικοινωνούν τώρα τα δύο εικονικά μηχανήματα μεταξύ τους;

Άσκηση 4: Δικτύωση NAT

Δημιουργήστε ένα τρίτο εικονικό σύστημα με όνομα GW, επιλέγοντας πάλι το αρχείο FreeBSD στο φάκελο C:\VMs. Επαναλάβετε τη διαδικασία Import Appliance, αλλάζοντας το όνομα σε GW και επιλέξτε τη ρύθμιση "Reinitialize the MAC address" όπως και πριν. Στις ρυθμίσεις δικτύου του συστήματος αλλάξτε τον Adapter 1 από Host-only σε NAT. Ξεκινήστε το νέο μηχάνημα και κάντε login με τα ίδια στοιχεία.

4.1 Ποια διεύθυνση IP έχει λάβει το μηχάνημα;
4.2 Ποια είναι η προεπιλεγμένη πύλη στον πινάκα δρομολόγησης;
4.3 Επικοινωνεί το νέο εικονικό μηχάνημα με το Internet; Τεκμηριώστε την απάντησή σας.
4.4 Επικοινωνεί το νέο εικονικό μηχάνημα με τα άλλα δύο εικονικά μηχανήματα; Τεκμηριώστε την απάντησή σας.

Στο φιλοξενούν μηχάνημα, κάνοντας χρήση του wireshark με κατάλληλο φίλτρο σύλληψης, ξεκινήστε καταγραφή της κίνησης ICMP της πραγματικής κάρτας Ethernet. Από το εικονικό μηχάνημα, κάνοντας χρήση του tcpdump -n με κατάλληλο φίλτρο ξεκινήστε καταγραφή της

κίνησης ICMP του προσαρμογέα em0 στο αρχείο "data". Στη συνέχεια πατήστε ALT+F2 για να ανοίξει μια δεύτερη κονσόλα[2,3] και εκτελέστε την εντολή `traceroute -I -n -q 1 147.102.222.210`. Όταν ολοκληρωθεί η εκτέλεση της εντολής σταματήστε τις καταγραφές στο φιλοξενούν μηχάνημα και στο εικονικό επιστρέφοντας με ALT+F1 στην αρχική κονσόλα και ανοίξτε το αρχείο "data".

4.5 Ποιά η σημασία των παραμέτρων στην εντολή traceroute;
4.6 Ποιά είναι η διεύθυνση IP πηγής των μηνυμάτων που παράγει η traceroute, όπως αυτά εμφανίζονται στην καταγραφή του tcpdump;
4.7 Ποιά είναι η διεύθυνση IP πηγής των αντίστοιχων μηνυμάτων, όπως αυτά εμφανίζονται στην καταγραφή του wireshark;
4.8 Ποιά η διεύθυνση IP πηγής των μηνυμάτων ICMP TTL exceeded in transit που εμφανίζονται στο tcpdump;
4.9 Εμφανίζονται αυτά τα πακέτα και στο wireshark; Αιτιολογήστε.
4.10 Παρατηρήστε τα πακέτα ICMP TTL exceeded in transit που εμφανίζονται στο wireshark. Υπάρχουν τα αντίστοιχα πακέτα και στην καταγραφή του tcpdump; Αιτιολογήστε.
4.11 Αν εκτελέσετε την εντολή tracert 147.102.222.210 από το φιλοξενούν μηχάνημα, ποιό θα είναι το πλήθος των αναπηδήσεων (hops) που θα προκύψει, σε σχέση με αυτό που εμφάνισε η traceroute στο εικονικό μηχάνημα; Αιτιολογήστε.

Άσκηση 5: Απλή δρομολόγηση

Τα λειτουργικά συστήματα UNIX έχουν συγκεκριμένα αρχεία παραμετροποίησης, όπου ο διαχειριστής μπορεί να ορίσει μεταβλητές περιβάλλοντος που επηρεάζουν τον τρόπο λειτουργίας του συστήματος. Για παράδειγμα, εάν θέλετε να λειτουργήσει το PC σας ως δρομολογητής IP, απλά αρκεί να αλλάξετε μια γραμμή σε ένα από τα αρχεία παραμετροποίησης. Η μελέτη των αρχείων αυτών είναι ένας τρόπος για να μάθετε τις διαθέσιμες επιλογές δικτύωσης.

Στο μηχάνημα GW προσθέστε στο αρχείο /etc/rc.conf τις παρακάτω γραμμές:

gateway_enable="YES"
firewall_enable="YES"
firewall_type="OPEN"
firewall_nat_enable="YES"
firewall_nat_interface="em0"

[2] Τα λειτουργικά συστήματα BSD και Linux συνήθως διαθέτουν πολλαπλές κονσόλες διαχείρισης, για εκτέλεση πολλών εντολών ταυτόχρονα χωρίς να χρειάζεται γραφικό/παραθυρικό περιβάλλον. Αυτές οι κονσόλες είναι διαθέσιμες με το συνδυασμό πλήκτρων ALT+F1 έως ALT+F4 (ή και παραπάνω κάποιες φορές).

[3] Εναλλακτικά, μπορείτε να στείλετε στο παρασκήνιο (background) την εντολή προσθέτοντας ένα "&" στο τέλος της με κενό ενδιάμεσα. Αυτή τότε ξεκινά να εκτελείται στο παρασκήνιο, αφήνοντας τον φλοιό ελεύθερο για να δώσουμε την επόμενη εντολή. Με την εντολή jobs βλέπουμε τις εργασίες που τρέχουν στο παρασκήνιο. Με την εντολή "fg %<n>" φέρνουμε την n-οστή εργασία στο προσκήνιο (foreground). Με Ctrl+Z η εργασία που τρέχει στο προσκήνιο παγώνει και μπαίνει στο παρασκήνιο με "bg". Με Ctrl+C η εργασία που τρέχει στο προσκήνιο τερματίζεται. Μπορούμε να τερματίσουμε οποιαδήποτε διεργασία με την εντολή kill %<n>" ή kill <pid>, όπου <pid> το αναγνωριστικό διεργασίας (process id) όπως αυτό φαίνεται με την εντολή "ps -a".

Με αυτές τις εντολές ενεργοποιείται η δρομολόγηση IP και το NAT, το οποίο είναι μέρος του firewall. Κλείστε το μηχάνημα χρησιμοποιώντας την εντολή poweroff[4]. Από τις ρυθμίσεις δικτύου του GW στο Virtualbox, ενεργοποιήστε τον Adapter 2 με ρύθμιση Internal Network (intnet) και εκκινήστε πάλι το εικονικό μηχάνημα, το οποίο διαθέτει πλέον δυο κάρτες δικτύου.

5.1 Τι σημαίνει η τελευταία γραμμή που προσθέσατε στο αρχείο rc.conf;

5.2 Ποια η σύνταξη της εντολής που θα σας επιτρέψει να ορίσετε ως διεύθυνση IP στη δεύτερη κάρτα δικτύου την 10.10.10.1/25;

5.3 Ποια η σύνταξη της εντολής που θα σας επιτρέψει να ορίσετε ως προεπιλεγμένη πύλη στο PC2 τη διεύθυνση IP που βάλατε παραπάνω; *[Υπόδ.: man route]*

5.4 Φτιάξτε ένα σχεδιάγραμμα που περιλαμβάνει το πραγματικό (φιλοξενούν) μηχάνημα, τα εικονικά μηχανήματα και τα πραγματικά και εικονικά interfaces τους, μαζί με τις IP διευθύνσεις και τις μάσκες υποδικτύου που τους έχουν αποδοθεί.

5.5 Μπορεί να επικοινωνήσει το PC2 με το διαδίκτυο; Τεκμηριώστε την απάντησή σας.

5.6 Μπορεί να επικοινωνήσει το PC1 με το διαδίκτυο; Τεκμηριώστε την απάντησή σας.

[4] Κατά τον τερματισμό λειτουργίας ενός εικονικού μηχανήματος δεν πρέπει να χρησιμοποιείτε ποτέ την επιλογή "Power off the machine" καθώς αυτό είναι αντίστοιχο με το να τραβάτε το καλώδιο ρεύματος δημιουργώντας πιθανό πρόβλημα στο σύστημα αρχείων. Θα πρέπει να τρέχετε την εντολή poweroff από τον φλοιό ή, σε ανάγκη, "Send the shutdown signal" που είναι αντίστοιχο με το ACPI shutdown (σα να πατάτε στιγμιαία το κουμπί του υπολογιστή, ενημερώνοντας το λειτουργικό σύστημα ότι επιθυμείτε να το κλείσετε).

Ονοματεπώνυμο:	**Όνομα PC:**
Ομάδα:	**Ημερομηνία:**
Διεύθυνση IP: . . .	**Διεύθυνση MAC: - - - - -**

Εργαστηριακή Άσκηση 1
Δικτύωση συστημάτων

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

1

1.1 .....

1.2 .....

1.3 .....

1.4 .....

1.5 .....

1.6 .....

1.7 .....

1.8 .....

1.9 .....

2

2.1 .....

2.2 .....

2.3 .....

2.4 .....

2.5 .....

.....

2.6 .....

2.7 .....

2.8 .....

2.9 .....

2.10 .....

2.11 .....

.....

.....

2.12 .....

2.13 .....

.....

2.14 .....