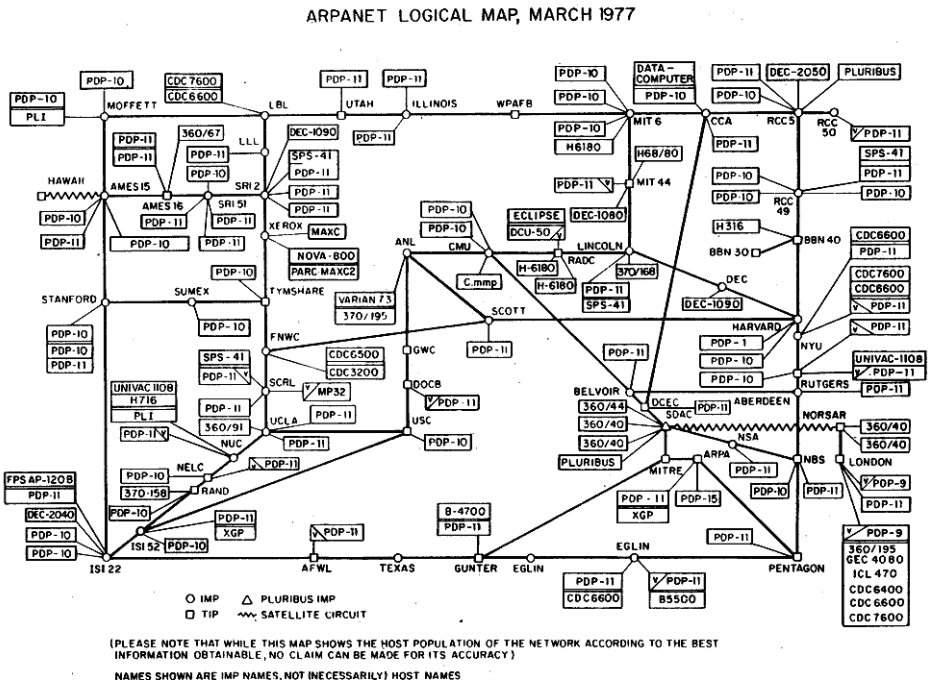
Εργαστηριακή Άσκηση 2
Δικτύωση συστημάτων στο VirtualBox

Τα δίκτυα υπολογιστικών συστημάτων μεγαλώνουν 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 που έφερε το διαδίκτυο οφείλεται και σε αυτή τη δυνατότητα.

Η αρχιτεκτονική στην οποία βασίζεται το Internet στη μορφή που το γνωρίζουμε σήμερα βασίζεται στο πρωτόκολλο 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 ήταν ιδιαίτερα σημαντικό, επειδή εισήγαγε την έννοια της διαδικτύωσης (internetworking), όπου πολλαπλά ξεχωριστά δίκτυα ενώθηκαν σε ένα ενιαίο δίκτυο-δικτύων. Το δίκτυο αυτό ήταν η βάση της δημιουργίας του διαδικτύου, το οποίο με την πάροδο των χρόνων εξαπλώθηκε σε όλο τον κόσμο.



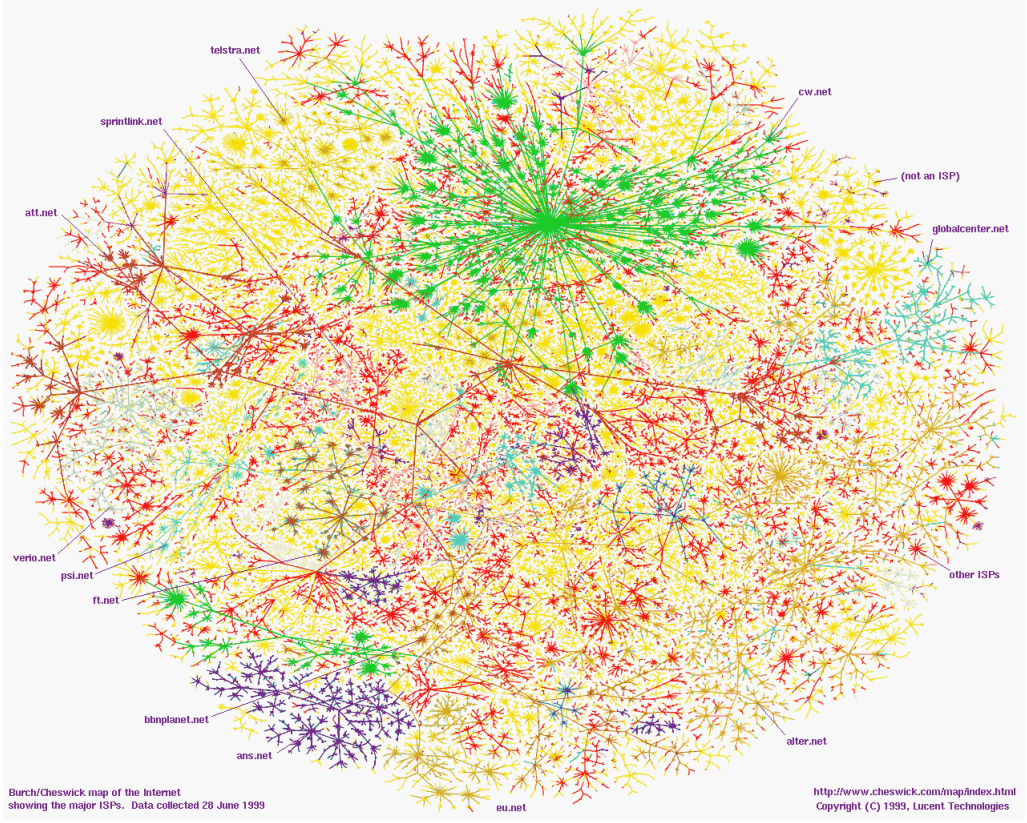
Σχηματική απεικόνιση του ARPANET το 1977

Σήμερα γινόμαστε μάρτυρες μιας νέας τάσης, της διαδικτύωσης αντικειμένων ή “πραγμάτων” σε αυτό που αποκαλείται Internet of Things (IoT), δηλαδή, ένα δίκτυο μεταξύ ηλεκτρονικών συσκευών, εφοδιασμένων με αισθητήρες και ενσωματωμένο λογισμικό. Ως διασυνδεδεμένα τα “πράγματα” μπορούν να ανταλλάξουν πληροφορίες μεταξύ τους αλλά και με το διαδίκτυο. Έτσι αποκτούν μεγαλύτερη χρηστική αξία παρέχοντας καινοφανείς υπηρεσίες τόσο στους κατόχους τους όσο και στους κατασκευαστές τους. Τυπικά εμπορικά παραδείγματα αποτελούν οι έξυπνοι θερμοστάτες NEST της Google για τα σπίτια, οι έξυπνοι μετρητές (smart meters) στο δίκτυο διανομής ηλεκτρικής ενέργειας και, στο άμεσο μέλλον, τα διαδικτυωμένα αυτοκίνητα θα είναι το εξέχον παράδειγμα. Η εισαγωγή συσκευών με τέτοιες δυνατότητες στο διαδίκτυο υποθέτει τη χρήση μιας διεύθυνσης IP ως

μοναδικής τους ταυτότητας. Εκτιμάται ότι το 2030 θα υπάρχουν περί τα 32,1 δισεκατομμύρια διαδικτυωμένες συσκευές στο Internet of Things (δείτε προβλέψεις στην ιστοθέση https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/). Ο χώρος των διευθύνσεων του IPv4 (που επιτρέπει μόνο 4.3 δισεκατομμύρια μοναδικών διευθύνσεων) έχει ήδη εξαντληθεί. Τα αντικείμενα στο IoT θα πρέπει να χρησιμοποιήσουν το IPv6 λόγω του τεράστιου μεγέθους του απαιτούμενου χώρου διευθύνσεων. Έτσι η παγκόσμια διείσδυση του IPv6 θα αποτελέσει τον κρίσιμο παράγοντα για την επιτυχία του IoT στο μέλλον.

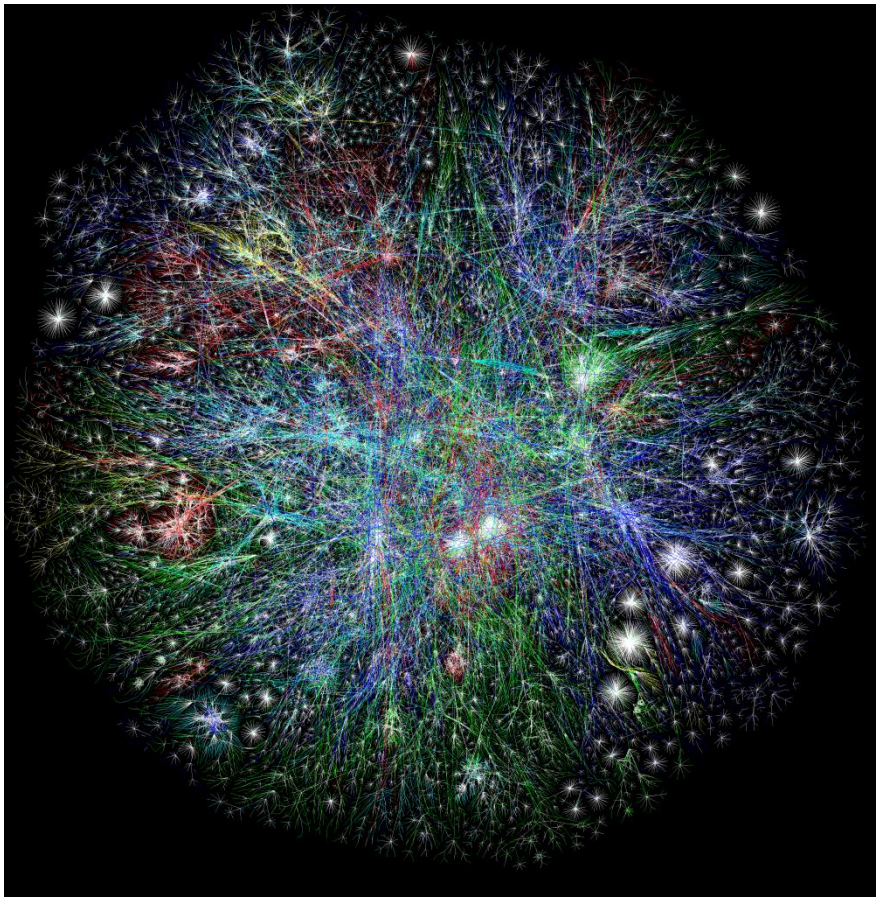
Όμως ο τρόπος λειτουργίας ενός δικτύου TCP/IP παραμένει ο ίδιος, ανεξάρτητα από το μέγεθός του. Αυτό μας διευκολύνει ιδιαίτερα στη μελέτη του, φτιάχνοντας και δοκιμάζοντας διάφορες τοπολογίες σε μικρογραφία. Η πιο απλή από αυτές είναι η τοπολογία ενιαίου τμήματος, όπως αυτή που θα δούμε παρακάτω. Στο οικιακό περιβάλλον η σύνδεση με το διαδίκτυο είναι μια τέτοια τοπολογία σε λειτουργία, δηλαδή, το τοπικό δίκτυο μεταξύ του υπολογιστή και του δρομολογητή (router). Με τη βοήθεια του VirtualBox θα φτιάξετε κάτι αντίστοιχο και στα επόμενα εργαστήρια θα έχετε την ευκαιρία να ασχοληθείτε και με πιο πολύπλοκα δίκτυα.

Περισσότερες πληροφορίες για την ιστορία του διαδικτύου μπορείτε να βρείτε στους παρακάτω συνδέσμους: http://www.columbia.edu/~rh120/other/tcpdigest_paper.txt, https://www.livinginternet.com/internet/i/ii_arpanet.htm, https://www.internetsociety.org/internet/history-internet/brief-history-internet/, https://www.computerhistory.org/internethistory/, και https://mountpeaks.wordpress.com/2012/03/06/what-has-the-internet-evolved-into-nowadays/ από όπου η απεικόνιση του 2012 στην επόμενη σελίδα.



Σχηματική απεικόνιση του Internet το 1999

Όσον αφορά το φυσικό στρώμα, απεικονίσεις των καλωδιακών διασυνδέσεων υπάρχουν στα https://global-internet-map-2022.telegeography.com/ και https://www.submarinecablemap.com/. Δείτε επίσης στο https://www.opte.org/the-internet/ ενδιαφέροντα βίντεο που οπτικοποιούν την εξέλιξη του διαδικτύου από το 1997 μέχρι το 2021.



Μια πιο πρόσφατη απεικόνιση του Internet το 2012

Δικτύωση στο VirtualBox

Το VirtualBox είναι το εργαλείο που θα σας βοηθήσει να χτίσετε μικρά εικονικά δίκτυα. Είναι ένας hypervisor ανοικτού κώδικα που επιτρέπει τη δημιουργία και διαχείριση φιλοξενούμενων (guest) εικονικών μηχανών στο περιβάλλον ενός φιλοξενούντος (host) μηχανήματος Το VirtualBox μπορεί για κάθε εικονικό μηχάνημα να εξομοιώσει έως 8[1] κάρτες δικτύου. Οι διαθέσιμες επιλογές για κάρτες είναι: PCnet-PCI II (Am79C970A), PCnet-Fast III (Am79C973), Intel PRO/1000 MT Desktop (82540EM), Intel PRO/1000 T Server (82543GC), Intel PRO/1000 MT Server (82545EM) και Paravirtualized Network (virtio-net). Η επιλογή της κάρτας δικτύου σχετίζεται με την ύπαρξη σχετικού οδηγού (driver) στο εικονικό μηχάνημα. Η προκαθορισμένη επιλογή PCNet FAST III για μηχανές x86 υποστηρίζεται σχεδόν από όλα τα λειτουργικά συστήματα πλην των νεότερων εκδόσεων των Windows. Η virtio-net είναι εξαίρεση με την έννοια ότι το VirtualBox δεν την εξομοιώνει, αλλά αναμένει την ύπαρξη οδηγών εικονικοποίησης από το φιλοξενούμενο μηχάνημα.

Κάθε κάρτα δικτύου μπορεί να λειτουργήσει με έναν από τους παρακάτω τρόπους: *χωρίς σύνδεση*, *NAT*, *δίκτυο NAT*, *γεφύρωση*, *εσωτερικό δίκτυο*, *μόνο με το φιλοξενούν*, *δίκτυο cloud* και *γενική δικτύωση*. Στη συνέχεια παρατίθεται μια σύντομη περιγραφή των διαθέσιμων τρόπων δικτύωσης.

1. Χωρίς σύνδεση (Not attached)

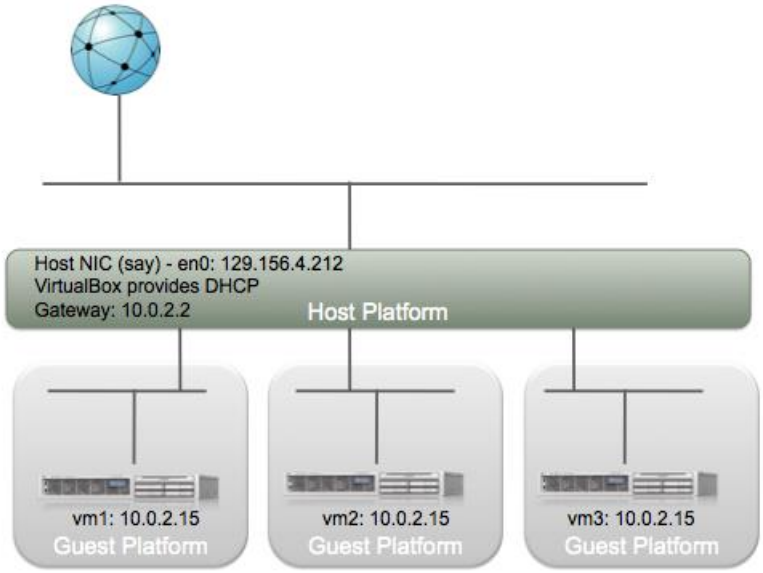
Σε αυτόν τον τρόπο δικτύωσης το VirtualBox δηλώνει στο φιλοξενούμενο μηχάνημα την ύπαρξη κάρτας δικτύου, η οποία όμως δεν είναι συνδεδεμένη, σαν να έχετε αποσυνδέσει το καλώδιο

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

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. Στους άλλους τρόπους δικτύωσης μπορείτε να πετύχετε το ίδιο αποτέλεσμα μη επιλέγοντας το Cable Connected στο μενού Advanced των ρυθμίσεων δικτύου. Αυτό μπορεί να γίνει και όταν το εικονικό μηχάνημα τρέχει.

2. 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 IPv4. Το VirtualBox παρέχει πάντα τη διεύθυνση 10.0.2.15. Η προεπιλεγμένη πύλη (και εξυπηρετητής DHCP) είναι το φιλοξενούν μηχάνημα, έχοντας ως διεύθυνση IPv4 την 10.0.2.2. Έτσι το κάθε φιλοξενούμενο μηχάνημα έχει την εντύπωση ότι βρίσκεται στο δικό του ξεχωριστό δίκτυο όπως φαίνεται στο σχήμα. Καθώς επιτρέπεται να χρησιμοποιηθούν περισσότερες της μίας κάρτες δικτύου σε λειτουργία NAT, η δεύτερη θα βρίσκεται στο δίκτυο 10.0.3.0/24 και το φιλοξενούμενο μηχάνημα θα έχει διεύθυνση 10.0.3.15, κ.ο.κ.

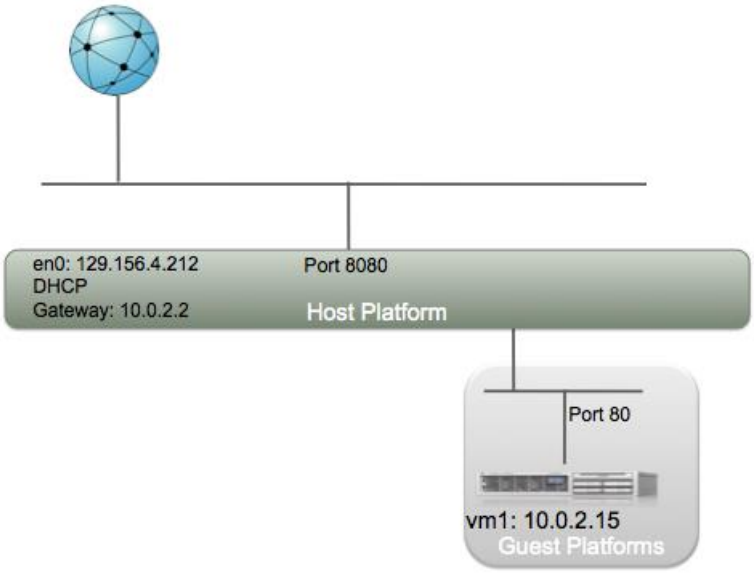


Η τεχνική NAT χρησιμοποιείται ευρέως στα πραγματικά δίκτυα, όπως π.χ. στον δρομολογητή xDSL ενός τυπικού οικιακού δικτύου για τον διαμοιρασμό της σύνδεσης προς το διαδίκτυο. Στην πιο απλή εκδοχή της συνίσταται σε μετάφραση διευθύνσεων IPv4, αλλά στην πιο συχνή εφαρμογή της γίνεται συνδυασμένη μετάφραση διευθύνσεων IPv4 και θυρών TCP ή UDP. Στη δικτύωση NAT του VirtualBox, όταν το φιλοξενούμενο μηχάνημα στέλνει κίνηση μέσω της πύλης προς το διαδίκτυο, οι διευθύνσεις IPv4 των πακέτων μεταφράζονται ώστε να φαίνεται ότι αυτά ξεκινούν από το φιλοξενούν μηχάνημα και όχι από το φιλοξενούμενο, τα δε πακέτα που προκύπτουν σε απάντηση επιστρέφονται στο φιλοξενούμενο μηχάνημα ως εάν προέρχονταν από το διαδίκτυο. Το αντίστροφο, δηλαδή, η έναρξη επικοινωνίας από το διαδίκτυο προς το φιλοξενούμενο μηχάνημα δεν είναι εφικτή εκτός και εάν χρησιμοποιηθεί Port Forwarding (δείτε πιο κάτω).

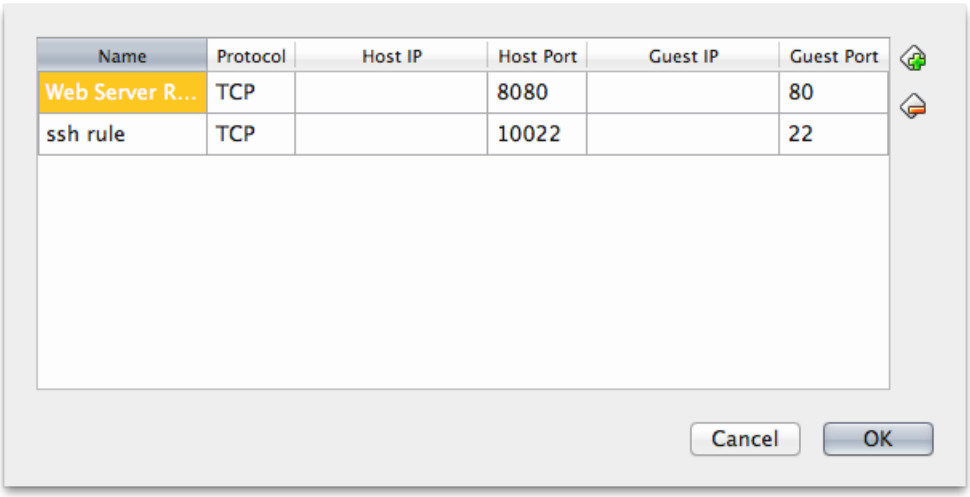
Σε αυτόν τον τρόπο δικτύωσης, το φιλοξενούμενο μηχάνημα θα συνεχίσει να λειτουργεί ακόμα και αν το φιλοξενούν αλλάξει δίκτυο, π.χ. ένας φορητός υπολογιστής που αλλάζει μεταξύ Ethernet, Wi-Fi ή 3/4/5G. Επιπλέον το NAT προσφέρει ως εξυπηρετητές DNS στο φιλοξενούμενο μηχάνημα τους ίδιους με αυτούς που χρησιμοποιεί το φιλοξενούν μηχάνημα. Επίσης παρέχει ένα proxy DNS εξυπηρετητή στη διεύθυνση 10.0.2.3 και έναν εξυπηρετητή tftp στη διεύθυνση 10.0.2.4 για εκκίνηση του φιλοξενούμενου μηχανήματος από το δίκτυο.

NAT και Port Forwarding

Αποτελεί επέκταση της λειτουργικότητας του NAT που προσφέρει το VirtualBox. Με τη λειτουργία προώθησης θυρών (port forwarding) επιτρέπεται η πρόσβαση στο φιλοξενούμενο μηχάνημα από άλλα εξωτερικά μηχανήματα. Αν και η συγκεκριμένη λειτουργία δε θα χρειαστεί στα πλαίσια του εργαστηρίου, μπορεί να χρησιμεύσει αλλού, όπως σε περιπτώσεις που υπάρχει ανάγκη να αποκτηθεί πρόσβαση σε κάποιο από τα εικονικά μηχανήματα από το εξωτερικό δίκτυο. Για τον σκοπό αυτό επιλέξτε το Expert στο μενού δικτύωσης του εικονικού μηχανήματος και μετά κλικ στο Port Forwarding. Εκεί εμφανίζεται ένα παράθυρο όπου μπορείτε να γράψετε τους επιθυμητούς κανόνες προώθησης.

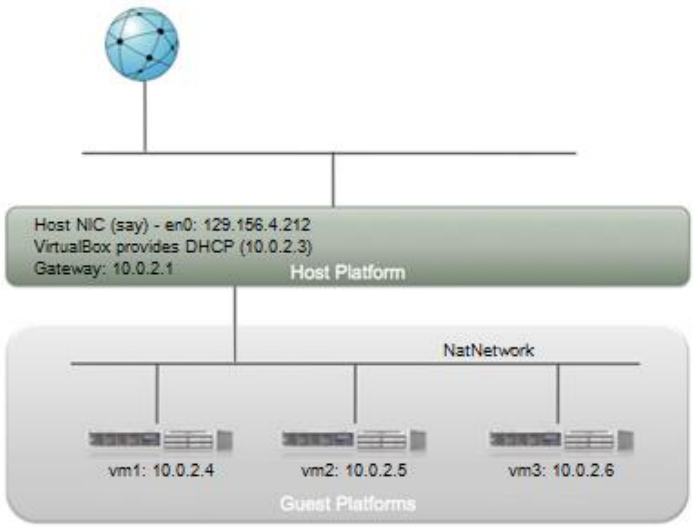


Στο επόμενο σχήμα βλέπετε ένα παράδειγμα με δύο κανόνες που επιτρέπουν την προώθηση συνδέσεων στις πόρτες 8080/tcp και 10022/tcp από το φιλοξενούν προς το εικονικό μηχάνημα στις πόρτες 80/tcp και 22/tcp, αντίστοιχα. Με τον τρόπο αυτό μπορείτε να εγκαταστήσετε έναν εξυπηρετητή ιστού στο εικονικό μηχάνημα καθώς και να συνδεθείτε με SSH σε αυτό από τον έξω κόσμο. Στην περίπτωση ενεργοποιημένου τείχους προστασίας (firewall) στο φιλοξενούν μηχάνημα όμως θα πρέπει να επιτραπεί η εισερχόμενη κίνηση στις πόρτες 8080 και 10022, αντίστοιχα.



3. Δίκτυο NAT (NAT Network)

Στο NAT Network έχουμε μια λειτουργία ανάλογη με αυτή του οικιακού δρομολογητή. Τα συστήματα εντός του ιδίου δικτύου NAT επικοινωνούν με το εξωτερικό δίκτυο χρησιμοποιώντας TCP και UDP πάνω από IPv4 και IPv6 αλλά και απευθείας μεταξύ τους. Συστήματα από το εξωτερικό δίκτυο δεν μπορούν να έχουν άμεση πρόσβαση εντός του δικτύου NAT (παρά μόνο μέσω προώθησης θυρών). Το δίκτυο NAT σχετίζεται με ένα εσωτερικό δίκτυο του VirtualBox που πρέπει να έχει προηγουμένως ορισθεί. Οι εικονικές μηχανές πρέπει συνδεθούν σε αυτό το δίκτυο NAT για να χρησιμοποιήσουν την εν λόγω υπηρεσία. Από το *File → Tools →Network Manager* στην καρτέλα NAT Networks μπορείτε να ορίσετε το όνομα του εσωτερικού δικτύου NAT, το υποδίκτυο IPv4 καθώς και το κατά πόσο υποστηρίζεται IPv6. Το VirtualBox παρέχει (εκτός και εάν απενεργοποιηθεί) τον εξυπηρετητή DHCP στα εικονικά μηχανήματα ώστε να λάβουν διευθύνσεις IPv4 (όπως ακριβώς κάνει ο οικιακός δρομολογητής). Η προκαθορισμένη πύλη είναι η 10.0.2.1, ο εξυπηρετητής DHCP έχει διεύθυνση 10.0.2.3 και τα εικονικά μηχανήματα παίρνουν διευθύνσεις από 10.0.2.4 και πάνω. Όπως και στην περίπτωση NAT η διεύθυνση IPv4 10.0.2.2 αντιστοιχεί στο φιλοξενούν μηχάνημα (το ίδιο και η 10.0.2.1). Επίσης υποστηρίζεται port forwarding τόσο για IPv4 όσο και για IPv6. Η σχετική ρύθμιση όμως αφορά το δίκτυο NAT και όχι το κάθε εικονικό μηχάνημα μεμονωμένα όπως στην περίπτωση του NAT.

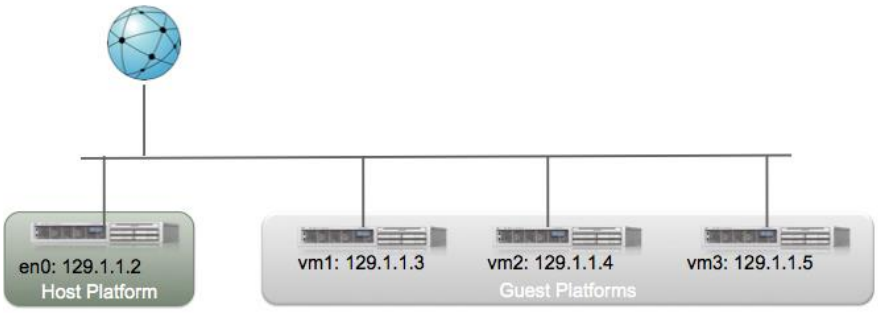


4. Γεφύρωση (Bridged)

Στις δικτυώσεις NAT χωρίς port forwarding 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 είναι χρήσιμη η λειτουργία της γεφύρωσης. Η εικονική κάρτα δικτύου γεφυρώνεται με τη φυσική και σε περίπτωση ύπαρξης πολλαπλών με μία εξ αυτών. Το εικονικό μηχάνημα χρησιμοποιεί την κάρτα δικτύου του φιλοξενούντος για την επικοινωνία του με τα άλλα μηχανήματα στο ίδιο φυσικό LAN, με το ίδιο το φιλοξενούν μηχάνημα και το διαδίκτυο. Με τη γεφύρωση το εικονικό σύστημα εμφανίζεται συνδεδεμένο ως εάν ήταν φυσικό μηχάνημα, ισότιμο με το φιλοξενούν, όπως φαίνεται στο σχήμα. Ο οδηγός της κάρτας σε αυτή την περίπτωση είναι ένα «δικτυακό φίλτρο» που επιτρέπει στο VirtualBox να συλλαμβάνει και εισάγει δεδομένα στη φυσική κάρτα δικτύου του φιλοξενούντος, δημιουργώντας έτσι μια νέα δικτυακή διεπαφή μέσω λογισμικού.

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 προεπιλεγμένη πύλη για δρομολόγηση. Το μειονέκτημα αυτής της λειτουργίας είναι ότι για κάθε εικονικό μηχάνημα απαιτείται μια διεύθυνση IP από το υποδίκτυο στο

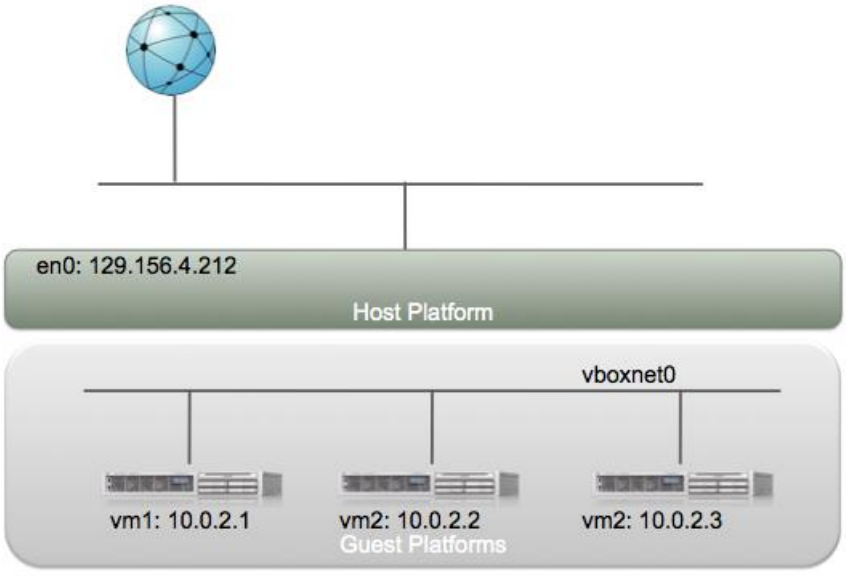
οποίο βρίσκεται το φιλοξενούν μηχάνημα. Εάν δημιουργηθούν πολλά εικονικά μηχανήματα, καθώς όλα θα ανήκουν στο ίδιο υποδίκτυο, ίσως υπάρξει πρόβλημα στην απόδοση διευθύνσεων IPv4 είτε δυναμικά μέσω DHCP είτε στατικά. Επίσης, αν το φιλοξενούν μηχάνημα έχει πολλαπλές κάρτες δικτύου, π.χ. είναι φορητός υπολογιστής με ασύρματη και ενσύρματη κάρτα, σε περίπτωση αλλαγής δικτύου θα πρέπει να γίνει ρύθμιση της γεφύρωσης εκ νέου.



Στις ασκήσεις δεν θα χρησιμοποιήσετε αυτόν τον τρόπο λειτουργίας, μπορείτε όμως άνετα να το δοκιμάσετε στο σπίτι σας, σε συνδυασμό με έναν δρομολογητή DSL.

5. Εσωτερικό δίκτυο (Internal Networking)

Με αυτόν καθώς και τον επόμενο τρόπο λειτουργίας μπορείτε να κάνετε δοκιμές και πειράματα, χωρίς 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 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. Δεν υπάρχει επικοινωνία με το φιλοξενούν μηχάνημα και το διαδίκτυο Το επόμενο σχήμα δείχνει μια τοπολογία εσωτερικού δικτύου στο VirtualBox.



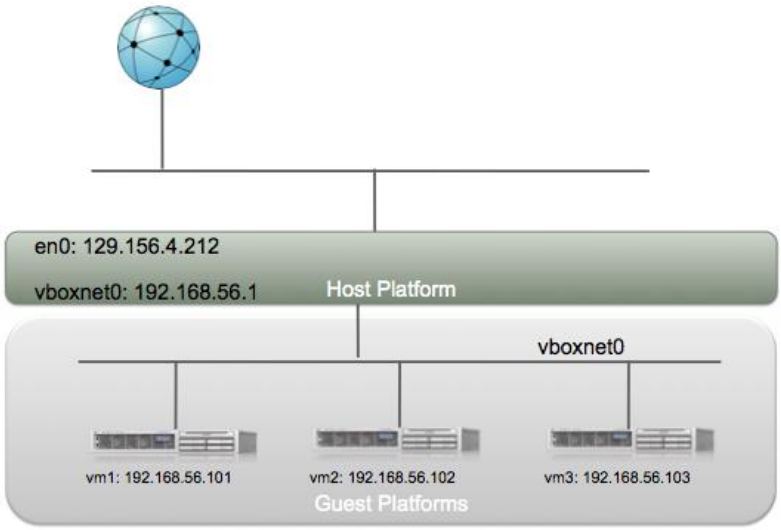
Μπορείτε να ορίσετε όσα εσωτερικά δίκτυα θέλετε δίνοντάς τους διαφορετικά ονόματα δικτύου. Τα εσωτερικά δίκτυα ταυτοποιούνται μόνο από το όνομά τους. Τα εσωτερικά δίκτυα (στο παράδειγμα vboxnet0) βρίσκονται εντελώς απομονωμένα, κάτι το οποίο είναι ιδιαίτερα βολικό για δοκιμές ή όταν χρειάζεστε ένα ξεχωριστό, καθαρό δίκτυο για να δημιουργήσετε δικές σας τοπολογίες. Μπορείτε να εγκαταστήσετε εξυπηρετητές για DHCP, DNS, Active Directory, κλπ. Πρέπει να σημειωθεί ότι σε αυτό τον τρόπο δικτύωσης το φιλοξενούν μηχάνημα δεν συμμετέχει, κάτι το οποίο μπορεί να είναι

χρήσιμο σε περιπτώσεις όπου δεν υπάρχει φυσικό δίκτυο π.χ. κατά τη διάρκεια ενός ταξιδιού 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 αυτά 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.

6. 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, Host-Only Ethernet adapter, που δημιουργείται κατά την εγκατάσταση του VirtualBox. Όλα τα εικονικά μηχανήματα έχουν επικοινωνία μεταξύ τους και με το φιλοξενούν, όπως φαίνεται στο επόμενο σχήμα. Εξωτερικά συστήματα δεν μπορούν να επικοινωνήσουν με τα εσωτερικά, εξ ου και η ονομασία, ούτε ορίζεται προκαθορισμένη πύλη. Επειδή το φιλοξενούν μηχάνημα έχει επαφή με το εσωτερικό δίκτυο, μπορεί να παρέχει τον εξυπηρετητή DHCP.



Στο φιλοξενούν μηχάνημα μπορεί να δημιουργηθούν περισσότερες από μία εικονικές διεπαφές Host-only επιλέγοντας από το μενού *File → Tools → Network Manager* την καρτέλα για Host-Only Networks. Για κάθε διεπαφή Host-only μπορείτε να ορίσετε το υποδίκτυο IPv4 όπου αυτή βρίσκεται μέσω της διεύθυνσης IPv4 (προκαθορισμένη τιμή 192.168.56.1) και της μάσκας υποδικτύου της, τη διεύθυνση IPv4 του εξυπηρετητή DHCP (προκαθορισμένη τιμή 192.168.56.100) καθώς και το εύρος των αποδιδόμενων διευθύνσεων (προκαθορισμένο εύρος 192.168.56.101 – 254).

7. Δίκτυο Cloud

Χρησιμοποιώντας δικτύωση cloud, ένα τοπικό εικονικό μηχάνημα μπορεί να συνδεθεί στο υποδίκτυο απομακρυσμένου εικονικού μηχανήματος στο Oracle Cloud Infrastructure. Η δημιουργία δικτύων cloud γίνεται από το μενού *File → Tools → Network Manager* καρτέλα Cloud Networks.

8. 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). Οι σήραγγες UDP επιτρέπουν τη διασύνδεση εικονικών μηχανημάτων που τρέχουν σε

διαφορετικά φιλοξενούντα μηχανήματα πάνω από την υπάρχουσα δικτυακή υποδομή. Αυτό γίνεται ενθυλακώνοντας τα πλαίσια Ethernet που στέλνονται ή λαμβάνονται από το δίκτυο των φιλοξενούμενων σε πακέτα UDP/IP που στέλνονται σε οποιοδήποτε δίκτυο είναι διαθέσιμο στο φιλοξενούν μηχάνημα. Με τη δικτύωση VDE το φιλοξενούμενο μηχάνημα μπορεί να συνδεθεί σε έναν εικονικό μεταγωγέα VDE (δείτε http://wiki.virtualsquare.org/) συμμετέχοντας έτσι σε μια εικονική υποδομή που μπορεί να εκτείνεται σε πολλά φιλοξενούντα μηχανήματα.

Promiscuous mode

Ο συνήθης τρόπος λειτουργίας μιας κάρτας δικτύου είναι να δέχεται μόνο πλαίσια που περιλαμβάνουν τη διεύθυνση MAC αυτής. Εξαιρουμένων των πλαισίων εκπομπής, πλαίσια με προορισμό διαφορετικές MAC απορρίπτονται. Για τη σύλληψη και καταγραφή πλαισίων, όπως στο Wireshark, η φυσική κάρτα πρέπει να λειτουργήσει σε promiscuous mode, δηλαδή, να δέχεται όλα τα πλαίσια ανεξαρτήτως της διεύθυνσης προορισμού. Αντίστοιχα με τις φυσικές κάρτες δικτύου, το VirtualBox επιτρέπει τον ορισμό του τρόπου λειτουργίας της εικονικής κάρτας στις περιπτώσεις δίκτυο NAT, γεφύρωση, μόνο με το φιλοξενούν και εσωτερικό δίκτυο. Κατά τον προκαθορισμένο τρόπο, άρνηση (deny), όποια κίνηση δεν προορίζεται για την εικονική κάρτα, αποκρύπτεται από το εικονικό μηχάνημα. Με την επιλογή Allow VMs, παραδίδεται στην κάρτα και η κίνηση που αφορά τα άλλα VMs στο ίδιο δίκτυο, ενώ με την επιλογή Allow All δεν τίθεται κανένας περιορισμός και η εικονική κάρτα μπορεί να δει όλη την κίνηση.

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. Περισσότερες πληροφορίες για τους τρόπους δικτύωσης που προσφέρει το VirtualBox θα βρείτε στην ιστοσελίδα του εγχειριδίου https://www.virtualbox.org/manual/ch06.html. Επίσης μια πολύ καλή περιγραφή υπάρχει στην ιστοσελίδα https://www.nakivo.com/blog/virtualbox-network-setting-guide/. Τέλος, αρκετές χρήσιμες πληροφορίες, όχι μόνο για τη δικτύωση στο VirtualBox, θα βρείτε στην ιστοθέση https://www.dedoimedo.com/virtualization.html.

Δικτύωση στο FreeBSD

Στην άσκηση αυτή θα χρησιμοποιήσετε εικονικές μηχανές FreeBSD για να εξοικειωθείτε με τους διάφορους τρόπους δικτύωσης που προσφέρει το VirtualBox. Το FreeBSD ως λειτουργικό σύστημα παρέχει πάρα πολλές δυνατότητες στον διαχειριστή όσον αφορά στη διάρθρωση των καρτών δικτύου και των δικτυακών υπηρεσιών. Υποστηρίζει πληθώρα πρωτοκόλλων δικτύωσης, IPv4, IPv6, SCTP, IPSec και ασύρματων δικτύων WiFi. Η δε υλοποίηση της στοίβας TCP/IP που βασίζεται στην έκδοση 4.2 BSD συνέβαλε σημαντικά στη διάδοση αυτών. Η ρύθμιση της λειτουργίας των καρτών δικτύων μπορεί να γίνει μέσω εντολών, όπως ifconfig, dhclient, κλπ, αλλά οι ρυθμίσεις δεν παραμένουν μετά την επανεκκίνηση, εκτός και εάν προστεθούν οι κατάλληλες εντολές στο αρχείο /etc/rc.conf.

Η εντολή ifconfig

Με την εντολή “ifconfig” του FreeBSD μπορείτε να δείτε την κατάσταση των δικτυακών διεπαφών ή να ορίσετε διευθύνσεις IPv4 και μάσκες υποδικτύου στις κάρτες δικτύου. Η εντολή ifconfig χωρίς ορίσματα χρησιμοποιείται για να δούμε την κατάσταση των δικτυακών διεπαφών. Εάν προσδιορίσουμε το όνομα της διεπαφής, ifconfig *interface*, η πληροφορία αφορά τη διεπαφή *interface*. Π.χ. με ifconfig em0 βλέπουμε την πληροφορία για τη διεπαφή em0 ως εξής:

```
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=9b<RXCSUM, TXCSUM, VLAN_MTU,VLAN_HWTAGGING, VLAN_HWCSUM>
    ether 00:a0:cc:da:da:da
```

```
inet 192.168.1.1 netmask 0xffffff00 broadcast 192.168.1.255
media: Ethernet autoselect (1000baseTX <full-duplex>)
status: active
```

Οι πρώτες δύο γραμμές περιγράφουν ιδιότητες της κάρτας. Οι σημαίες UP και RUNNING δηλώνουν ότι η διεπαφή είναι ενεργοποιημένη και μπορεί να στείλει και δεχθεί πακέτα. Η σημαία BROADCAST υποδηλώνει ότι έχει ορισθεί διεύθυνση εκπομπής και η MULTICAST ότι η κάρτα μπορεί να στείλει και δεχθεί κίνηση πολλαπλής διανομής. Η SIMPLEX δηλώνει ότι η κάρτα δεν μπορεί να ακούσει τις δικές της μεταδόσεις. Η τιμή της MTU δείχνει το μέγεθος της μέγιστης μονάδας μετάδοσης για τη διεπαφή και το metric είναι μια τιμή που χρησιμοποιείται από τα πρωτόκολλα δρομολόγησης. Στη δεύτερη γραμμή δηλώνονται ως επιλογές (options) διάφορες δυνατότητες της κάρτας, όπως του υπολογισμού checksum και υποστήριξης εικονικών LAN (VLAN). Στην τρίτη γραμμή φαίνεται η διεύθυνση MAC της κάρτας (ether). Στην τέταρτη γραμμή φαίνεται η διεύθυνση IPv4 (inet), η μάσκα υποδικτύου (netmask), όπου το 0xffffff00 είναι το ίδιο με 255.255.255.0, καθώς και η διεύθυνση εκπομπής (broadcast). Στην πέμπτη γραμμή δηλώνεται το είδος του φυσικού μέσου Ethernet, καθώς και η ταχύτητα λειτουργίας (1000 Mbps) και ο τρόπος λειτουργίας, πλήρως αμφίδρομο (Full Duplex – FD) Ethernet, όπως αμφότερα προκύπτουν ως αποτέλεσμα της αυτόματης επιλογής (autoselection). Στην τελευταία γραμμή δηλώνεται η κατάσταση της κάρτας ως ενεργή (active) εάν ανιχνεύεται σήμα στο φυσικό μέσο, και ως no carrier εάν το καλώδιο είναι αποσυνδεδεμένο.

Όπως θα διαπιστώσετε από τις σελίδες του εγχειριδίου για την εντολή ifconfig υπάρχει πληθώρα επιλογών για να ρυθμίσετε τη λειτουργία μιας διεπαφής. Μερικές από τις πιο χρήσιμες είναι:

ifconfig em0 down για να απενεργοποιήσετε τη διεπαφή em0
ifconfig em0 up για να ενεργοποιήσετε τη διεπαφή em0
ifconfig em0 192.168.1.1 netmask 255.255.255.0 broadcast 192.168.1.255 ή απλούστερα
ifconfig em0 192.168.1.1/24 για να ορίσετε διεύθυνση IPv4, μάσκα και διεύθυνση εκπομπής
ifconfig em0 delete για να διαγράψετε τη διεύθυνση IPv4 από τη διεπαφή em0
ifconfig em0 mtu 1000 για να αλλάξετε την MTU
ifconfig em0 media 100baseTX mediaopt full-duplex για να ορίσετε πλήρως αμφίδρομη λειτουργία στα 100 Mbps
ifconfig em0 ether 08:00:26:3b:27:ab για να ορίσετε στην κάρτα τη συγκεκριμένη διεύθυνση MAC

Σε περίπτωση που χρειαστεί για οποιοδήποτε λόγο να ακυρώσετε ρυθμίσεις, απενεργοποιήστε και ενεργοποιήστε την κάρτα. Σε έσχατη ανάγκη επανεκκινήστε την υπηρεσία δικτύωσης ως εξής:

service netif restart ή /etc/rc.d/netif restart

Η εντολή dhclient

Το πρωτόκολλο DHCP επιτρέπει σε ένα host να επικοινωνήσει με ένα εξυπηρετητή που διατηρεί μια λίστα διευθύνσεων IPv4 και να ζητήσει ως δάνειο για προσωρινή χρήση μία από αυτές. Με την εντολή dhclient του FreeBSD μπορείτε να ρυθμίσετε δυναμικά μέσω DHCP τις δικτυακές παραμέτρους των καρτών. Το όνομα της κάρτας δικτύωσης πρέπει να δοθεί ως όρισμα. Π.χ. με dhclient em0 θα πάρετε ως απόκριση κάτι παρόμοιο με:

```
DHCPDISCOVER on em0 to 255.255.255.255 port 67 interval 9
DHCPOFFER from 10.0.2.3
DHCPREQUEST on em0 to 255.255.255.255 port 67
DHCPACK from 10.0.2.3
bound to 10.0.2.4 -- renewal in 300 seconds.
```

όπου ο εξυπηρετητής DHCP δίνει στον πελάτη την IPv4 διεύθυνση 10.02.3 για χρονικό διάστημα 300 s. Στο FreeBSD ο πελάτης διατηρεί, και μετά την επανεκκίνηση, μια λίστα με τα δάνεια που έχει λάβει σε αρχεία /var/db/dhclient.leases.IFNAME, ένα για κάθε διεπαφή, όπου το IFNAME είναι το όνομα της κάρτας, π.χ. em0. Τα παλιά δάνεια χρησιμοποιούνται σε περίπτωση που ο εξυπηρετητής DHCP δεν είναι διαθέσιμος, οπότε παλιά δάνεια που δεν έχουν λήξει μπορούν να χρησιμοποιηθούν μέχρι τη λήξη τους ή μέχρι να επανέλθει ο εξυπηρετητής DHCP.

Επιπλέον το πρωτόκολλο DHCP παρέχει ένα μηχανισμό μέσω του οποίου ο πελάτης μπορεί να μάθει επιπλέον σημαντικές παραμέτρους για τη δικτύωση, όπως τον προκαθορισμένο δρομολογητή και τον εξυπηρετητή DNS. Στο FreeBSD η εντολή dhclient ξαναγράφει το αρχείο /etc/resolv.conf με πληροφορία που λαμβάνει από τον εξυπηρετητή DHCP. Το περιεχόμενο του αρχείου χρησιμοποιείται για την επίλυση ονομάτων σε διευθύνσεις IP, δηλαδή, ορίζονται οι εξυπηρετητές DNS που θα ερωτηθούν. Ένα τυπικό αρχείο /etc/resolv.conf είναι:

```
search ntua.gr
nameserver 147.102.222.210
nameserver 147.102.7.1
```

όπου:

nameserver	Διεύθυνση IP του εξυπηρετητή DNS. Μπορούν να ορισθούν μέχρι τρεις εξυπηρετητές που θα ερωτηθούν με τη σειρά που ορίζονται.
search	Λίστα για αναζήτηση ονομάτων host. Τυπικά προσδιορίζεται από το όνομα περιοχής του τοπικού host.

Η εντολή tcpdump

Για να μελετήσετε τη συμπεριφορά των δικτύων σε βάθος χρειάζονται 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 χρησιμοποιήσετε τα tcpdump και Wireshark. Το Wireshark είναι γνωστό από το μάθημα των Δικτύων Υπολογιστών. Το tcpdump είναι παρόμοιο, αλλά σε γραμμή εντολών φλοιού UNIX. Σας επιτρέπει να συλλάβετε δικτυακή κίνηση και να εμφανίσετε τις επικεφαλίδες των πακέτων. Τα προγράμματα αυτά θέτουν την κάρτα δικτύου στον τρόπο λειτουργίας promiscuous mode που προαναφέρθηκε, 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 https://www.tcpdump.org/. Για μια σύντομη εισαγωγή και παραδείγματα χρήσης του ανατρέξτε στις ιστοσελίδες https://danielmiessler.com/study/tcpdump/ και https://support.f5.com/csp/article/K2289/. 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.

-e	Εμφανίζει στην οθόνη για κάθε πακέτο την επικεφαλίδα στρώματος ζεύξης δεδομένων (εν γένει Ethernet).
-x	Εμφανίζει στην οθόνη τα περιεχόμενα (πλην της επικεφαλίδας στρώματος ζεύξης δεδομένων) του πακέτου σε δεκαεξαδική μορφή.
-v	Εμφανίζει στην οθόνη επιπλέον λεπτομέρειες για τις επικεφαλίδες των ενθυλακωμένων πρωτοκόλλων. Π.χ. για πακέτα IP, εμφανίζει το TTL, το μήκος πακέτου κλπ, για τεμάχια TCP τα flags, κλπ.
-s snaplen	Συλλαμβάνει snaplen byte του πακέτου, αντί του εξ ορισμού μέγιστου (262144).
-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. Μπορείτε να περιορίσετε την κίνηση που θα καταγραφεί χρησιμοποιώντας φίλτρα, όπως και στο Wireshark. Τα φίλτρα ορίζονται μέσω του ορισμού μιας έκφρασης (expression) που αποτελείται από μία ή περισσότερες στοιχειώδεις προτάσεις (primitives). Οι στοιχειώδεις προτάσεις συνήθως συνίστανται από μια ταυτότητα id (αριθμό ή όνομα) της οποίας προηγούνται διάφοροι προσδιορισμοί. Στον παρακάτω πίνακα έχουν αποτυπωθεί οι πιο σημαντικοί:

type	Δηλώνει το είδος ταυτότητας 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 δηλωθεί, υπονοείται host.
dir	Δηλώνει την κατεύθυνση από και/ή προς. Το dir μπορεί να είναι src όταν ορίζουμε την ταυτότητα της πηγής, dst για την ταυτότητα προορισμού, src or dst, src and dst. Εάν παραληφθεί, υπονοείται src or dst.
proto	Δηλώνει το είδος πρωτοκόλλου ether, fddi, tr, wlan, ip, ip6, arp, rarp, decnet, tcp και udp, Π.χ. με ip περιορίζουμε τη σύλληψη κίνησης σε πακέτα IPv4, arp σε πακέτα ARP, tcp σε τεμάχια TCP και με icmp σε μηνύματα ICMP.
expr1 relop expr2	Δηλώνει οτιδήποτε ικανοποιεί τη λογική έκφραση, όπου relop είναι ένα από τα >, <, >=, <=, =, != και expr1, expr2 αριθμητικές εκφράσεις που περιλαμβάνουν ακέραιους αριθμούς (σύμφωνους με τη σύνταξη της C), τους συνήθεις δυαδικούς τελεστές [+, -, *, /, %, &, |, ^, <<, >>], το μήκος του πακέτου ή τιμές πεδίων της επικεφαλίδας του. Το μήκος του πακέτου προσδιορίζεται με τον τελεστή μήκους len. Για συγκεκριμένες τιμές στα πεδία των επικεφαλίδων πρωτοκόλλων χρησιμοποιείται η σύνταξη: proto[expr:size] όπου expr είναι η απόσταση σε byte του πεδίου του πρωτοκόλλου proto από την αρχή και το size, εάν ορισθεί, είναι το μήκος σε byte του πεδίου της επικεφαλίδας που ενδιαφέρει.

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

and ή &&
or ή ||
not ή !

είτε ομαδοποιώντας τες εντός παρενθέσεων.

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). Δείτε και άλλα παραδείγματα στο https://blog.wains.be/2007/2007-10-01-tcpdump-advanced-filters/. Για μια πλήρη περιγραφή της σύνταξης των φίλτρων δείτε https://www.tcpdump.org/manpages/pcap-filter.7.html.

Άσκηση 1 (προετοιμασία): Δημιουργία εικονικού μηχανήματος FreeBSD

Ως προετοιμασία στο σπίτι και προτού έρθετε στο εργαστήριο, θα δημιουργήσετε ένα εικονικό μηχάνημα FreeBSD έκδοση 13.4. Στη συνέχεια θα το χρησιμοποιήσετε προκειμένου να εξοικειωθείτε με τις λειτουργίες δικτύωσης του VirtualBox καθώς και τις εντολές tcpdump, ifconfig και dhclient. Για τη δημιουργία του εικονικού μηχανήματος FreeBSD, ακολουθήστε τις παρακάτω οδηγίες.

1. Επισκεφτείτε την ιστοσελίδα https://download.freebsd.org/ftp/releases/VM-IMAGES/13.4-RELEASE/. Εντοπίστε τα Virtual Machine Images για την έκδοση 13.4-RELEASE του FreeBSD για επεξεργαστές i386.
2. Κατεβάστε το αρχείο FreeBSD-13.4-RELEASE-i386.vhd.xz που περιέχει τον δίσκο του εικονικού μηχανήματος και αποσυμπιέστε το.
3. Στο VirtualBox από το μενού Machine → New δημιουργήστε ένα νέο εικονικό μηχάνημα τύπου BSD με όνομα FreeBSD13.4, λειτουργικό σύστημα FreeBSD (32 bit), 1 CPU, μνήμη 256 MB και δίσκο το αρχείο .vhd που αποσυμπιέσατε προηγουμένως.
4. Στη συνέχεια από το γραφικό περιβάλλον του VirtualBox δηλώστε στο Display μνήμη γραφικών 12MB, στο USB επιλέξτε τον ελεγκτή USB 1.1 και στο Network επιλέξτε NAT.
5. Ξεκινήστε το εικονικό μηχάνημα, από το μενού View → Virtual Screen 1 επιλέξτε μια κατάλληλη μεγέθυνση, και εισέλθετε ως διαχειριστής root. Δεν θα σας ζητηθεί συνθηματικό.
6. Με τη βοήθεια της εντολής passwd ορίστε συνθηματικό ntua για τον διαχειριστή root.
7. Στη συνέχεια με τη βοήθεια της εντολής adduser δημιουργήστε ένα νέο χρήστη lab, που να ανήκει στην ομάδα wheel, με κέλυφος το csh και συνθηματικό ntua.
8. Στο αρχείο /etc/rc.conf προσθέστε τις επόμενες γραμμές (διαγράφοντας ό,τι υπάρχει):

   sshd_enable="YES" # to enable the ssh daemon
   hostname="PC.ntua.lab" # to assign the host name
   syslogd_flags=”-scc” # to disable compression of repeated messages

9. Δημιουργήστε το αρχείο /boot/loader.conf με την ακόλουθη εντολή για επιτάχυνση της διαδικασίας εκκίνησης:

   autoboot_delay=”3”

10. Επανεκκίνηστε το FreeBSD. Εάν σε Windows στην γραμμή κατάστασης του εικονικού μηχανήματος παρατηρήσετε το σύμβολο  αντί του  , αυτό σημαίνει ότι στο φιλοξενούν μηχάνημα είναι ενεργό το Hyper-V και ίσως χρειαστεί να το απενεργοποιήσετε πλήρως.

11. Αφού επανεκκίνησετε το εικονικό μηχάνημα, βεβαιωθείτε ότι δεν εμφανίζεται[2] κάποιο λάθος και ότι η υπηρεσία sshd τρέχει.
12. Διαγράψτε όποια αρχεία /etc/resolv.conf και /var/db/dhclient.leases.* έχουν δημιουργηθεί κατά την εκκίνηση.
13. Διαγράψτε το ιστορικό των εντολών που δώσατε μέχρι το σημείο αυτό (δείτε σύνταξη εντολής history στις σελίδες man για τον φλοιό csh).
14. Κλείστε το εικονικό μηχάνημα με την εντολή poweroff.
15. Από τη διαδρομή *File→Export Appliance…* στο VirtualBox δημιουργήστε ένα αρχείο FreeBSD13.4.ova σε φάκελο που θα ορίσετε στο μενού του Format Settings.
16. Διατηρήστε το αρχείο .ova για να μπορείτε να δημιουργείτε στο μέλλον εικονικά μηχανήματα και διαγράψτε το αρχείο .vhd (δεν χρειάζεται πλέον).

Άσκηση 2: Ανάλυση δικτυακών πρωτοκόλλων με το TCPDUMP

Για να εξοικειωθείτε με τον τρόπο χρήσης της tcpdump θα φτιάξετε ένα εικονικό μηχάνημα FreeBSD που θα το ονομάσετε PC1. Εντοπίστε στην επιφάνεια εργασίας τη συντόμευση για το VirtualBox και ξεκινήστε το. Ακολουθήστε τη διαδρομή *File → Import Appliance* ... και στην οθόνη που θα εμφανισθεί, μενού Source, αναζητήστε το αρχείο FreeBSD13.4.ova που δημιουργήσατε. Στο μενού Settings αλλάξτε το όνομα της συσκευής σε PC1 και στο MAC Address Policy επιλέξτε τη ρύθμιση "Generate new MAC addresses for all network adapters". Τέλος, κάντε κλικ στο Finish. Το VirtualBox θα δημιουργήσει ένα εικονικό μηχάνημα με όνομα PC1. Ξεκινήστε το και κάντε login ως διαχειριστής "root" με συνθηματικό "ntua". Με τη βοήθεια των προηγουμένων απαντήστε τις παρακάτω ερωτήσεις. Δεν χρειάζεται να κάνετε σύλληψη πακέτων, απλώς ελέγξετε την ορθότητα της σύνταξης της εντολής σας.

2.1 Με ποια εντολή φλοιού μπορείτε να δείτε ποιες κάρτες δικτύου διαθέτει το εικονικό μηχάνημα καθώς και την κατάστασή τους;

2.2 Με ποιες εντολές μπορείτε να απενεργοποιήσετε και στη συνέχεια ενεργοποιήσετε την κάρτα δικτύου em0.

2.3 Με ποιες εντολές φλοιού μπορείτε να βρείτε περισσότερες πληροφορίες για τα tcpdump, pcap και pcap-filter;

2.4 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε όλα τα πλαίσια από την κάρτα δικτύου em0 χωρίς επίλυση διευθύνσεων IP;

2.5 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε όλα τα πλαίσια από την κάρτα δικτύου em0 και να εμφανίσετε τα περιεχόμενα των σε ASCII και δεκαεξαδική μορφή;

2.6 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να βλέπετε και τις διευθύνσεις MAC πηγής, προορισμού των πλαισίων που συλλάβατε;

2.7 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε από την κάρτα δικτύου em0 τα πρώτα 68 byte όλων των πλαισίων;

2.8 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε πακέτα IPv4 με διεύθυνση 10.0.0.1 και να δείτε τις λεπτομέρειες της επικεφαλίδας τους;

[2] Εάν κάποιο μέρος των αποτελεσμάτων δεν φαίνεται στην οθόνη και θέλετε να το δείτε, πιέστε το πλήκτρο Scroll Lock (ScrLk) και μετά μπορείτε χρησιμοποιώντας τα βελάκια να προχωρήσετε προς τα πίσω. Πιέστε και πάλι το ScrLk για να επανέλθετε στην αρχική κατάσταση. Εάν το πληκτρολόγιο του υπολογιστή σας δεν διαθέτει το πλήκτρο ScrLk ή δεν μπορεί να παραχθεί με συνδυασμό άλλων πλήκτρων, χρησιμοποιήστε το Soft Keyboard… από το μενού *Input→Keyboard* του εικονικού μηχανήματος.

2.9 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε στην κάρτα δικτύου em0 πακέτα της επικοινωνίας μεταξύ δύο μηχανημάτων με διευθύνσεις 10.0.0.1 και 10.0.0.2;

2.10 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε πακέτα IPv4 για το δίκτυο 1.1.0.0/16 και να εμφανίσετε στην οθόνη το περιεχόμενό τους;

2.11 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε πακέτα IPv4 που δεν ανήκουν (και δεν έπρεπε ποτέ να έχουν φτάσει) στο τοπικό σας δίκτυο, ας πούμε το 192.168.1.0/24, και να τυπώσετε στην οθόνη το περιεχόμενό τους περιλαμβανομένων των επικεφαλίδων Ethernet;

2.12 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε IPv4 πακέτα εκπομπής ή πολλαπλής διανομής;

2.13 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε πακέτα IPv4 μήκους μεγαλύτερου των 576 byte;

2.14 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε πακέτα IPv4 με τιμές TTL μικρότερες του 5;

2.15 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε πακέτα IPv4 με προαιρετικές επικεφαλίδες;

2.16 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε πακέτα ICMP με αποστολέα την IP διεύθυνση 10.0.0.1;

2.17 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε τεμάχια TCP με παραλήπτη την IP διεύθυνση 10.0.0.2;

2.18 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε δεδομενογράμματα UDP με θύρα προορισμού 53;

2.19 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε τεμάχια TCP με διεύθυνση αποστολέα ή παραλήπτη 10.0.0.10;

2.20 Τροποποιήστε την εντολή της παραπάνω ερώτησης, ώστε να εμφανίζονται μόνο όσα τεμάχια εξ αυτών περιλαμβάνουν την TCP θύρα 23 και τα αποτελέσματα να αποθηκεύονται στο αρχείο “sample_capture”.

2.21 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε τεμάχια TCP που περιέχουν **μόνο** τη σημαία SYN;

2.22 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε τα πρώτα δύο τεμάχια της τριμερούς χειραψίας TCP;

2.23 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε τα σχετικά με την απόλυση μιας σύνδεσης TCP τεμάχια;

2.24 Τι ακριβώς υπολογίζει η παράσταση ((tcp[12:1] & 0xf0) >> 2) χρησιμοποιούμενη ως στοιχείο φίλτρου για τη σύλληψη τεμαχίων TCP;

2.25 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε τεμάχια TCP που περιλαμβάνουν προαιρετικές επικεφαλίδες (options);

2.26 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε μηνύματα HTTP και να δείτε το περιεχόμενο ως χαρακτήρες ASCII;

2.27 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε μηνύματα telnet προς το edu-dy.cn.ntua.gr;

2.28 Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε πακέτα IPv6;

Άσκηση 3: Δικτύωση Host-only

Επαναλάβετε τη διαδικασία ξεκινήματος ενός νέου εικονικού μηχανήματος όπως στην προηγουμένη άσκηση, ορίστε το όνομα της συσκευής σε PC2 και μην ξεχάσετε να επιλέξετε τη ρύθμιση "Generate new MAC addresses for all network adapters". Το VirtualBox θα έχει τώρα δύο εικονικά μηχανήματα που θα φαίνονται με ονόματα PC1 και PC2. Ξεκινήστε το δεύτερο και κάντε login ως διαχειριστής "root" με συνθηματικό "ntua". Από τη διαδρομή *Machine → Settings → Network* ρυθμίστε την κάρτα δικτύου και στα δύο εικονικά μηχανήματα σε δικτύωση Host-only. Τα εικονικά μηχανήματα δεν έχουν λάβει αυτόματα κάποια διεύθυνση IP, οπότε θα πρέπει να το κάνετε χειροκίνητα.

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

3.1 Από το μενού του VirtualBox βρείτε τη διεύθυνση IPv4 του Host-only Ethernet adapter.
3.2 Παρομοίως βρείτε τη διεύθυνση IPv4 του εξυπηρετητή DHCP για το δίκτυο Host-only καθώς και την περιοχή διευθύνσεων IPv4 που αυτός μπορεί να εκχωρήσει.
3.3 Αποδώστε μέσω DHCP διευθύνσεις IPv4 στα εικονικά μηχανήματα.
3.4 Ποιες είναι οι διευθύνσεις IPv4 που έχει αποδώσει το VirtualBox στα μηχανήματα;
3.5 Πώς θα καταλάβετε αν τα δύο μηχανήματα επικοινωνούν μεταξύ τους;
3.6 Πώς θα καταλάβετε αν το φιλοξενούν μηχάνημα επικοινωνεί με τα δύο μηχανήματα;
3.7 Ποια είναι η σύνταξη της εντολής που θα σας δείξει την προεπιλεγμένη πύλη; *[Υπόδ.: man netstat]*.
3.8 Υπάρχει προεπιλεγμένη πύλη στη συγκεκριμένη κατάσταση δικτύωσης; Τεκμηριώστε την απάντησή σας.
3.9 Από τα εικονικά μηχανήματα μπορείτε να κάνετε ping στην IPv4 διεύθυνση της φυσικής κάρτας δικτύου του φιλοξενούντος μηχανήματος; Τεκμηριώστε την απάντησή σας.
3.10 Ποιο είναι το όνομα των μηχανημάτων όπως το αντιλαμβάνεται το λειτουργικό τους σύστημα; Ποια εντολή φλοιού χρησιμοποιήσατε;
3.11 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. [Σημ. το FreeBSD αναμένει ονόματα FQDN (fully qualified domain name) άσχετα από το εάν αυτά επιλύονται στο τοπικό δίκτυο].

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

3.12 Χωρίς χρήση κάποιας εντολής, επιβεβαιώστε ότι το όνομα άλλαξε. Που εμφανίζεται αυτό στον φλοιό;
3.13 Περιέχει το αρχείο παραμετροποίησης /etc/rc.conf στο PC1 το νέο όνομα; Σε ενδεχόμενη επανεκκίνηση του PC1 ποιο θα είναι το όνομά του;
3.14 Διορθώστε, ώστε στην επόμενη επανεκκίνηση τα μηχανήματα να έχουν τα νέα ονόματα;

Προτού υπάρξει το DNS, υπήρχε το αρχείο hosts για την αντιστοίχιση του ονόματος σε διεύθυνση IP. Οι υπολογιστές το κατέβαζαν από ένα κεντρικό εξυπηρετητή μέσω FTP. Το αρχείο υπάρχει ακόμη στα περισσότερα λειτουργικά συστήματα. Στο FreeBSD θα το βρείτε στο /etc/hosts.

3.15 Τι πρέπει να προσθέσετε στο /etc/hosts για να χρησιμοποιείτε σε αμφότερα τα μηχανήματα τα ονόματά τους αντί των IPv4 διευθύνσεων στις διάφορες δικτυακές εντολές;
3.16 Γράψτε ένα παράδειγμα σύνταξης κάποιας εντολής, στην οποία χρησιμοποιείται η λειτουργία που προσφέρει το αρχείο hosts, ώστε να μη χρειάζεται να ορίσουμε διεύθυνση IPv4.

3.17 Από το PC1 κάντε ping κατά σειρά στο ίδιο, στο PC2, στη διεύθυνση IPv4 της εικονικής κάρτας (Host-only) του φιλοξενούντος μηχανήματος[3] και στη διεύθυνση IPv4 του εξυπηρετητή DHCP. Καταγράψτε το μήκος και την τιμή του πεδίου TTL των απαντήσεων;

Θα χρησιμοποιήσετε τώρα το tcpdump για να δείτε την κίνηση που παράγεται όταν εκτελείτε την εντολή ping. Στο PC2 ξεκινήστε το tcpdump με κατάλληλο φίλτρο ώστε να συλλαμβάνει μόνο πακέτα που περιέχουν τη διεύθυνση IPv4 του PC1 με εμφάνιση λεπτομερειών και χωρίς επίλυση διευθύνσεων IPv4 σε ονόματα.

3.18 Ποια είναι η σύνταξη της εντολής tcpdump που χρησιμοποιήσατε;

3.19 Στο PC1 εκτελέστε την εντολή `ping -c 4 PC2`. Ποιο είναι το μήκος των μηνυμάτων ICMP echo request που λαμβάνει το PC2, ποιο το μήκος και ποια είναι η τιμή του πεδίου TTL των αντίστοιχων πακέτων IPv4;

Ξεκινήστε τώρα μια νέα καταγραφή στο PC2 ώστε να συλλαμβάνετε μόνο μηνύματα ICMP και να τα εμφανίζετε με όσο πιο πολλές λεπτομέρειες. Στη συνέχεια ανοίξτε ένα παράθυρο εντολών στο φιλοξενούν μηχάνημα και κάντε ping στη διεύθυνση IPv4 του PC2.

3.20 Ποια είναι η σύνταξη της εντολής tcpdump που χρησιμοποιήσατε;

3.21 Ποιο είναι το μήκος των μηνυμάτων ICMP echo request που παράγει το φιλοξενούν μηχάνημα; Γιατί διαφέρει από το μήκος που παρατηρήσατε πριν;

3.22 Ποια είναι η τιμή του πεδίου TTL των πακέτων IPv4 που ανταλλάσσουν τα δύο μηχανήματα; Συμφωνεί με τις τιμές που βρήκατε προηγουμένως;

3.23 Υποδείξτε 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]*.

3.24 Στο PC1 ξεκινήστε νέα καταγραφή όπως πριν και από το παράθυρο εντολών στο φιλοξενούν μηχάνημα κάντε πάλι ping στη διεύθυνση IP του PC2 και αφήστε το να τρέχει. Παρατηρείτε στην καταγραφή στο PC1 κάποια σχετική με το ping κίνηση.

3.25 Παρατηρείτε κάποιου άλλου είδους κίνηση; Εάν ναι, τι αφορά;

3.26 Αφού σταματήσετε την καταγραφή, από το μενού Advanced στις ρυθμίσεις της κάρτας δικτύου του PC1 αλλάξτε το promiscuous mode σε Allow VMs και επαναλάβετε την καταγραφή. Τι διαφορετικό παρατηρείτε τώρα;

Άσκηση 4: Δικτύωση Internal

Στο PC2 από τη διαδρομή *Machine → Settings → Network* αλλάξτε τις ρυθμίσεις δικτύου από “Host-only Adapter” σε “Internal Network” δηλώνοντας ως όνομα εσωτερικού δικτύου το LAN. Κατόπιν, χρησιμοποιώντας την εντολή φλοιού ifconfig ορίστε στα PC1 και PC2 στατικές διευθύνσεις IPv4 ίδιες με τις δυναμικές που είχαν αποδοθεί προηγουμένως.

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

4.1 Ποια είναι η σύνταξη της εντολής που χρησιμοποιήσατε για να ορίσετε τις στατικές διευθύνσεις IPv4 στα δύο μηχανήματα;

4.2 Τι σημαίνει το μήνυμα λάθους που εμφανίσθηκε όταν ορίσατε στατικές διευθύνσεις;

4.3 Ξεκινήστε καταγραφή με εμφάνιση λεπτομερειών στο PC1 και αφήστε την να τρέχει.

[3] Στον προσωπικό σας υπολογιστή, ενδέχεται να πρέπει να ρυθμίσετε το τείχος προστασίας (firewall) ώστε να επιτρέπει την αποδοχή πακέτων ICMP.

4.4 Από το φιλοξενούν μηχάνημα μπορείτε να κάνετε ping στο PC2;
4.5 Παρατηρείτε στην καταγραφή κίνηση σχετική με το ping προς το PC2;
4.6 Από το PC2 μπορείτε να κάνετε ping στο PC1;
4.7 Παρατηρείτε στην καταγραφή κίνηση σχετική με το ping προς το PC1;
4.8 Αφού σταματήσετε την καταγραφή, αλλάξτε τις ρυθμίσεις δικτύου του PC1 σε Internal Network όπως στο PC2. Επικοινωνούν τώρα τα δύο εικονικά μηχανήματα;
4.9 Από το φιλοξενούν μηχάνημα μπορείτε να επικοινωνήσετε με κάποιο από τα δύο εικονικά μηχανήματα; Τεκμηριώστε την απάντησή σας.
4.10 Αφού επαναφέρετε το promiscuous mode στην προκαθορισμένη τιμή Deny ξεκινήστε μια νέα καταγραφή στο PC1 χωρίς επίλυση διευθύνσεων IPv4 σε ονόματα.
4.11 Στη συνέχεια στο PC2, αφού αδειάσετε τον πίνακα arp (δείτε σχετική σελίδα man), κάντε ping στη διεύθυνση IPv4 της εικονικής κάρτας (Host-only) του φιλοξενούντος μηχανήματος. Στην καταγραφή στο PC1, τι είδους μηνύματα παρατηρείτε ότι παράγει το PC2;
4.12 Πώς εξηγείτε το μήνυμα host is down που επιστρέφει το ping;
4.13 Αλλάξτε τη διεύθυνση IPv4 των δύο συστημάτων χρησιμοποιώντας τις τελευταίες 2 διαθέσιμες διευθύνσεις IP από το υποδίκτυο 10.11.12.0/26.
4.14 Επικοινωνούν τώρα τα δύο εικονικά μηχανήματα μεταξύ τους χρησιμοποιώντας τις διευθύνσεις IPv4 που ορίσατε προηγουμένως;

Άσκηση 5: Δικτύωση NAT

Δημιουργήστε ένα τρίτο εικονικό σύστημα επιλέγοντας πάλι το αρχείο FreeBSD13.4.ova. Επαναλάβετε τη διαδικασία Import Appliance, αλλάζοντας το όνομα σε PC3 και επιλέξτε τη ρύθμιση “Generate new MAC addresses for all network adapters” όπως και πριν. Στις ρυθμίσεις δικτύου του συστήματος θέστε, εάν δεν είναι ήδη, τον Adapter 1 σε NAT. Ξεκινήστε το νέο μηχάνημα και κάντε login ως διαχειριστής “root”. Κατόπιν, στα εικονικά μηχανήματα PC1 και PC2, από το εικονίδιο δικτύου στη γραμμή κατάστασης των εικονικών μηχανημάτων, αλλάξτε τις ρυθμίσεις δικτύου των από “Internal Network” σε “NAT”

5.1 Αποδώστε με DHCP διεύθυνση IPv4 στη διεπαφή em0 των εικονικών μηχανημάτων.
5.2 Ποια διεύθυνση IPv4 έχουν λάβει και από πού (διεύθυνση IP) αποδόθηκε;
5.3 Ποια είναι η προεπιλεγμένη πύλη στον πίνακα δρομολόγησης;
5.4 Ποιο είναι το περιεχόμενο του αρχείου /etc/resolv.conf;
5.5 Σε ποιο αρχείο του εικονικού μηχανήματος έχει καταγραφεί η διεύθυνση IPv4 που αποδόθηκε προηγουμένως μέσω DHCP καθώς και οι πληροφορίες που περιέχει το resolv.conf;
5.6 Από τα εικονικά μηχανήματα μπορείτε να κάνετε ping στη διεύθυνση IPv4 της προεπιλεγμένης πύλης;
5.7 Επικοινωνεί το νέο εικονικό μηχάνημα με το Internet; Τεκμηριώστε την απάντησή σας.
5.8 Σε ποιες από τις διευθύνσεις 10.0.2.1 έως 10.0.2.4 λαμβάνετε απάντηση εάν κάνετε ping; Τι παριστάνουν αυτές; *[Υποδ. Δείτε https://www.virtualbox.org/manual/ch09.html#changenat.]*
5.9 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 μια καταγραφή της κίνησης ICMP στην φυσική του κάρτα. Στο εικονικό μηχάνημα PC3, κάνοντας χρήση του `tcpdump -n` με κατάλληλο φίλτρο σύλληψης ξεκινήστε μια άλλη καταγραφή της κίνησης ICMP στην διεπαφή em0 αποθηκεύοντάς την στο αρχείο “data”. Στη συνέχεια πατήστε

ALT+F2 για να ανοίξει μια δεύτερη κονσόλα[4] και εκτελέστε την εντολή ping -n -c 3 -m 64 9.9.9.9. Αφού σταματήσετε τις καταγραφές, επιστρέψτε με ALT+F1 στην αρχική κονσόλα του εικονικού μηχανήματος και ανοίξτε το αρχείο "data".

5.10 Ποια η σημασία των παραμέτρων στην εντολή ping;

5.11 Ποια είναι η διεύθυνση IPv4 πηγής και το TTL των μηνυμάτων ICMP request που παράγονται από το ping όπως αυτά εμφανίζονται στην καταγραφή του tcpdump;

5.12 Ποια είναι η διεύθυνση IPv4 πηγής και το TTL των αντίστοιχων μηνυμάτων ICMP request όπως αυτά εμφανίζονται στην καταγραφή του Wireshark;

5.13 Ποια είναι η διεύθυνση IPv4 προορισμού και το TTL των μηνυμάτων ICMP reply στην καταγραφή του Wireshark;

5.14 Ποια είναι η διεύθυνση IPv4 προορισμού και το TTL των μηνυμάτων ICMP reply στην καταγραφή του tcpdump;

5.15 Αν εκτελέσετε την εντολή tracert -d 9.9.9.9 στο φιλοξενούν μηχάνημα, ποιο είναι το πλήθος των αναπηδήσεων (hops) που προκύπτει;

5.16 Συμφωνεί αυτό με την τιμή του TTL της ερώτησης 5.13; Αιτιολογήστε.

5.17 Εκτελέστε τώρα την εντολή traceroute -I -n -q 1 9.9.9.9 στο εικονικό μηχάνημα PC3. Ποια η σημασία των παραμέτρων στην εντολή traceroute;

5.18 Σύμφωνα με την έξοδο της εντολής traceroute, πόσα βήματα μακριά από το εικονικό μηχάνημα βρίσκεται το 9.9.9.9; Συμφωνεί αυτό με την τιμή του TTL της ερώτησης 5.14 και το αποτέλεσμα της ερώτησης 5.15;

Άσκηση 6: Δικτύωση NAT Network

Από τη διαδρομή *File* → *Tools* → *Network Manager* του VirtualBox επιλέξτε NAT Networks και εάν δεν υπάρχει ορισμένο κάποιο δίκτυο, προσθέστε και ενεργοποιήστε ένα δίκτυο NAT (NAT network) με όνομα NatNetwork που να διαθέτει εξυπηρετητή DHCP. Κατόπιν, στα εικονικά μηχανήματα PC1 και PC2, από το εικονίδιο δικτύου στη γραμμή κατάστασης των εικονικών μηχανημάτων, αλλάξτε τις ρυθμίσεις δικτύου των από "NAT" σε "NAT Network".

6.1 Ποια είναι η διεύθυνση του δικτύου NAT που έχει οριστεί στο VirtualBox;

6.2 Στα PC1, PC2 διαγράψτε τη διεύθυνση IPv4 από την κάρτα δικτύου καθώς και το αρχείο /var/db/dhclient.leases.em0 με τα δάνεια που έχουν εκχωρηθεί.

6.3 Αποδώστε μέσω DHCP διευθύνσεις IPv4 στα εικονικά μηχανήματα PC1, PC2.

6.4 Ποιες διευθύνσεις αποδόθηκαν; Διαφέρουν από αυτές που είχαν τα PC1, PC2 προηγουμένως;

6.5 Ποια η διεύθυνση IPv4 του εξυπηρετητή DHCP;

6.6 Ποιο είναι το περιεχόμενο του αρχείου /etc/resolv.conf;

6.7 Ποια είναι η προεπιλεγμένη πύλη στον πίνακα δρομολόγησης;

6.8 Από τα εικονικά μηχανήματα PC1, PC2 μπορείτε να κάνετε ping στην IPv4 διεύθυνση της προεπιλεγμένης πύλης;

6.9 Από τα PC1, PC2 μπορείτε να κάνετε ping στην IPv4 διεύθυνση του εξυπηρετητή DHCP;

6.10 Από τα PC1, PC2 μπορείτε να κάνετε ping στη διεύθυνση 10.0.2.2; Ποιο μηχάνημα απαντά; *[Δείτε πίνακα arp.]*

[4] 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).

6.11 Επικοινωνούν τα εικονικά μηχάνημα με το Internet; Τεκμηριώστε την απάντησή σας.
6.12 Επικοινωνούν τα PC1, PC2 μεταξύ τους;
6.13 Μπορείτε από το PC3 να κάνετε ping στα PC1, PC2;
6.14 Εάν σε κάποιο από τα προηγούμενα ping λάβετε απάντηση είναι το αντίστοιχο PC που απαντά; Γιατί; Πώς μπορείτε να το διαπιστώσετε;

Στο φιλοξενούν μηχάνημα και στο εικονικό μηχάνημα PC1 ξεκινήστε καταγραφές της κίνησης ICMP όπως κάνατε προηγουμένως στην Άσκηση 5. Σε νέα κονσόλα[5] στο εικονικό μηχάνημα PC1 εκτελέστε την εντολή traceroute -I -n -q 1 9.9.9.9. Όταν ολοκληρωθεί η εκτέλεση της εντολής σταματήστε τις καταγραφές.

6.15 Ποιες είναι οι διευθύνσεις IPv4 πηγής των μηνυμάτων ICMP τύπου TTL exceeded in transit της καταγραφής στο Wireshark.
6.16 Ποια είναι η διεύθυνση IPv4 προορισμού των μηνυμάτων αυτών;
6.17 Ποιες είναι οι διευθύνσεις IPv4 πηγής των μηνυμάτων ICMP τύπου TTL exceeded in transit που εμφανίζονται στην καταγραφή του tcpdump;
6.18 Ποια είναι η διεύθυνση IPv4 προορισμού των μηνυμάτων αυτών;
6.19 Αντιστοιχούν ένα προς ένα τα μηνύματα TTL exceeded in transit των δύο καταγραφών;
6.20 Παρατηρήσατε κάποια διαφορά σε σχέση με ό,τι είδατε στην προηγούμενη Άσκηση 5; Εάν ναι, εξηγήστε τι συμβαίνει.

[5] Εναλλακτικά, μπορείτε να στείλετε στο παρασκήνιο (background) την εντολή tcpdump προσθέτοντας ένα “&” στο τέλος της με κενό ενδιάμεσα. Αυτή τότε ξεκινά να εκτελείται στο παρασκήνιο, αφήνοντας τον φλοιό ελεύθερο για να δώσετε την επόμενη εντολή. Με την εντολή jobs βλέπετε τις εργασίες που τρέχουν στο παρασκήνιο. Με την εντολή “fg %<n>” φέρνετε 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 τερματίζετε την εργασία που τρέχει στο προσκήνιο. Μπορείτε να τερματίσετε οποιαδήποτε διεργασία με την εντολή kill %<n>” ή kill <pid>, όπου <pid> το αναγνωριστικό διεργασίας (process id) όπως αυτό φαίνεται με την εντολή “ps -ax”.

Ονοματεπώνυμο:	**Όνομα PC:**
Ομάδα:	**Ημερομηνία:**

Εργαστηριακή Άσκηση 2
Δικτύωση συστημάτων στο VirtualBox

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

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 .....

2.15 .....

2.16 .....

2.17 .....

2.18 .....

2.19 .....

2.20 .....

2.21 .....

2.22 .....

2.23 .....

2.24 .....

2.25 .....

2.26 .....

2.27 .....

2.28 .....

3

3.1 .....
3.2 .....
3.3 .....
3.4 .....
3.5 .....
3.6 .....
3.7 .....
3.8 .....
3.9 .....
.....
3.10 .....
3.11 .....
3.12 .....
3.13 .....
3.14 .....
.....
3.15 .....
.....
3.16 .....
3.17 .....
.....
.....
3.18 .....
3.19 .....
3.20 .....
3.21 .....
.....
3.22 .....
.....
3.23 .....
.....
3.24 .....
.....
3.25 .....
.....
3.26 .....

4

4.1 .....

.....

4.2 .....

4.3 .....

4.4 .....

4.5 .....

4.6 .....

4.7 .....

4.8 .....

4.9 .....

.....

4.10 .....

4.11 .....

.....

4.12 .....

4.13 .....

.....

4.14 .....

5

5.1 .....

5.2 .....

5.3 .....

5.4 .....

.....

5.5 .....

5.6 .....

5.7 .....

.....

5.8 .....

.....

.....

5.9 .....

.....

5.10 .....

.....

5.11 .....

5.12 .....
5.13 .....
5.14 .....
5.15 .....
5.16 .....
.....
5.17 .....
.....
5.18 .....
.....

6

6.1 .....
6.2 .....
6.3 .....
6.4 .....
.....
6.5 .....
6.6 .....
.....
6.7 .....
6.8 .....
6.9 .....
6.10 .....
.....
6.11 .....
.....
6.12 .....
6.13 .....
6.14 .....
.....
6.15 .....
.....
.....
.....
.....
6.16 .....

6.17 .....
.....
.....
.....
.....
.....
6.18 .....
6.19 .....
.....
6.20 .....
.....
.....