Αναλυτές πρωτοκόλλου δικτύου εν συντομία

Σύγκριση εργαλειών και χρήσης περιπτώσεων & μελέτη βιβλιογραφίας

ΜΙΧΑΗΛ ΜΑΡΚΟΥ

ΕΠΙΣΤΗΜΗ ΥΠΟΛΟΓΙΣΤΩΝ ΕΤΟΣ 3, ΥΠΟΛΟΓΙΣΤΕΣ ΚΑΙ ΑΣΦΑΛΕΙΑ ΔΙΚΤΩΝ



**SCHOOL OF ARCHITECTURE, COMPUTING & ENGINEERING**

*BSc in Computer Science*

**Michail Markou**

*CN6003 – COMPUTER AND NETWORK SECURITY*

**UEL NUMBER**

*2020732*

***Date***

11/11/2021

**Network Protocol Analyzers in short**

Michail Markou

University of East London

Contents

[1. Περίληψη 1](#_Toc89433107)

[2. Εισαγωγή 1](#_Toc89433108)

[2.1. Αρχή τεχνολογίας ανάλυσης πρωτοκόλλου δικτύου 1](#_Toc89433109)

[3. Εργαλεία ασφαλείας 4](#_Toc89433110)

[3.1. Wireshark 4](#_Toc89433111)

[3.1.1. Ιστορία 4](#_Toc89433112)

[3.1.2. Περιπτώσεις χρήσεις & Μειονεκτήματα 4](#_Toc89433113)

[3.2. TCPdump 6](#_Toc89433114)

[3.2.1. Ιστορία 6](#_Toc89433115)

[3.2.2. Περιπτώσεις χρήσεις & Μειονεκτήματα 6](#_Toc89433116)

[3.3. Συγκρίτικά αποτελέσματα 7](#_Toc89433117)

[4. Ανασκόπηση βιβλιογραφίας ανάλυσης πραγματικής περίπτωσης 9](#_Toc89433118)

[4.1. Η μελέτη περίπτωσης 9](#_Toc89433119)

[4.1.1. Η τεχνική προσέγγισης προβλήματος 9](#_Toc89433120)

[4.1.2. Πρώτος γυρος 9](#_Toc89433121)

[4.1.3. Δεύτερος γύρος 11](#_Toc89433122)

[4.1.4. Περιορίζοντας το πεδίο εφαρμογής 13](#_Toc89433123)

[4.1.5. Μαθήματα & Απαντήσεις 16](#_Toc89433124)

[Αναφορές 17](#_Toc89433125)

[Παράρτημα 19](#_Toc89433126)

[Γλωσσάριο 19](#_Toc89433127)

[Διαμόρφωση συσκευής 19](#_Toc89433128)

[R1 19](#_Toc89433129)

[L3Switch 24](#_Toc89433130)

[ciscoasa 28](#_Toc89433131)

[Figure 1 https://en.wikipedia.org/wiki/Ethernet\_frame 2](#_Toc89362793)

[Figure 2 https://en.wikipedia.org/wiki/IPv4#Packet\_structure 3](#_Toc89362794)

[Figure 3 https://el.wikipedia.org/wiki/Wireshark 4](#_Toc89362795)

[Figure 4 https://en.wikipedia.org/wiki/Tcpdump 5](#_Toc89362796)

[Figure 5 Simulation of the example in GNS3 8](#_Toc89362797)

[Figure 6 Step 1) Client's PC unable to get DHCP offer 9](#_Toc89362798)

[Figure 7 Step 2) Server Logs shows that communication is ok up to a point 10](#_Toc89362799)

[Figure 8 Step 3) port forwarding the traffic and capture with Wireshark on top of WAN backhaul 10](#_Toc89362800)

[Figure 9 Steps 4) Wireshark DORA process. The Server in WAN sends the offer back 11](#_Toc89362801)

[Figure 10 Step 5) Inside Intranet (Figure 11) business there is no offer seen so the error is before that 11](#_Toc89362802)

[Figure 11 Steps 6) In the Intranet there is no Offer seen so the error/misconfiguration must be on the Firewall Concentrator 12](#_Toc89362803)

[Figure 12 ASA firewall receives correct clients discover but still no offer 13](#_Toc89362804)

[Figure 13 Firewall can reach the DHCP server 13](#_Toc89362805)

[Figure 14 Successful DORA 14](#_Toc89362806)

[Figure 15 The problem was the DHCP server IP address as not adjacent 14](#_Toc89362807)

[Figure 16 Client DORA succeed 15](#_Toc89362808)

[Figure 17 Logs on DHCP server 15](#_Toc89362809)

[Figure 18 https://www.ciscopress.com/articles/article.asp?p=2273070&seqNum=2 16](#_Toc89362810)

# Περίληψη

Η ανάλυση πρωτοκόλλου δικτύου είναι μια τεχνική που παρέχει στους αρχιτέκτονες, τους μηχανικούς, τους κατασκευαστές και τους ιδιοκτήτες-χειριστές να συλλαμβάνουν δυαδικά ακατέργαστα δεδομένα για περαιτέρω ανάλυση, υποκλοπώντας, μυρίζοντας τη δραστηριότητα διεπαφής μιας κάρτας δικτύου για τη διατήρηση υποδομών. Θα καταγράψουμε και θα αναλύσουμε την κυκλοφορία δικτύου με 2 διαφορετικές λύσεις λογισμικού, π.χ. εργαλεία (Wireshark, tcpdump) και θα δούμε τις περιπτώσεις χρήσης και τα μειονεκτήματα του καθενός.

*Keywords*: Αναλυτές πρωτοκόλλου δικτύου; Πακέτο λογισμικού; Εργαλεία ασφάλειας δικτύου; Ανίχνευση δικτύου;

# Εισαγωγή

Το sniffing δικτύου παρεμποδίζεται από τη δυαδική μορφή συναρμολόγησης πακέτων του αρχικού περιεχομένου μηνύματος σε δίκτυα μεταγωγής και μη μεταγωγής[[1]](#footnote-1). Μετά τη λήψη, το ληφθέν πακέτο κατασκευάζεται για την κατασκευή της αρχικής μορφής από την οπτική γωνία του αποστολέα. Τεχνικά, εάν κάποιος λαμβάνει δεδομένα με αυτόν τον τρόπο, θεωρείται παραβίαση ασφαλείας του επιπέδου 2[[2]](#footnote-2) μεταγωγής δικτύου [1] [2].

Κάθε εργαλείο μπορεί να χρησιμοποιηθεί είτε ηθικά είτε αντιδεοντολογικά. Η καταγραφή της κίνησης του δικτύου μπορεί να αποδειχθεί πολύ χρήσιμη για την αντιμετώπιση προβλημάτων ασφάλειας, απόδοσης, δραστηριότητας και σχεδίασης δικτύου συνολικά ή ως μεμονωμένα[[3]](#footnote-3). Επιπλέον, τα στατιστικά στοιχεία μπορούν να σχεδιαστούν και να παρουσιαστούν μέσω αυτοματοποίησης σε ένα εργαλείο οπτικοποίησης και παρακολούθησης (π.χ. Nagios)[[4]](#footnote-4).

## Αρχή τεχνολογίας ανάλυσης πρωτοκόλλου δικτύου

**Πώς λειτουργεί το επίπεδο OSI?**

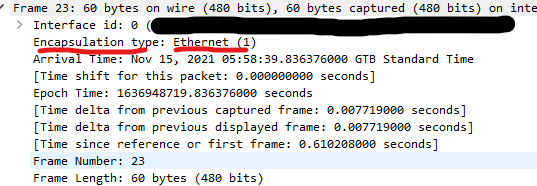
Η δια-επικοινωνία υπολογιστών γίνεται μέσω διεπαφών δικτύου. Από την άποψη του επιπέδου εφαρμογής, όταν θέλει να επικοινωνήσει με μια υπηρεσία μέσω του δικτύου, ξεκινά μια διαδικασία ενθυλάκωσης πακέτων [3] [4], πριν μεταφερθούν δεδομένα στο επίπεδο εφαρμογής αντίστοιχα, ενθυλάκωση κεφαλίδας πρωτοκόλλου TCP ή UDP, κεφαλίδα πρωτοκόλλου IP και κεφαλίδα πρωτοκόλλου επιπέδου σύνδεσης π.χ. , Ethernet, wi-fi (802.11 xx) κλπ, δεσμευτείτε στο αρχικό ωφέλιμο φορτίο δεδομένων, εάν τα δεδομένα του επιπέδου εφαρμογής υπερβαίνουν το μέγιστο μήκος των πακέτων IP και του επιπέδου σύνδεσης, στη συνέχεια αναλύονται μέσω της πολιτικής και τα χωρίζουν σε πολλά πακέτα και στη συνέχεια μεταδίδονται μέσω μιας σύνδεσης δικτύου. Όταν το δίκτυο εκπέμπει σε κάθε κόμβο, η αντίστροφη λειτουργία της διαδικασίας αποσυσκευασίας πακέτων θα συμβεί ανάλογα με τις πληροφορίες πακέτων σε κάθε επίπεδο και επίπεδο ικανότητας πρόσβασης κόμβου (π.χ. διακόπτει την επιθεώρηση/ανάγνωση μέχρι το επίπεδο 2) Επίπεδο μόνο του τελικού στόχου. θα ξετυλίξει, θα ξαναχτίσει το πακέτο πλήρως μέχρι το Επίπεδο 7/Εφαρμογή και θα υποβάλει τα δεδομένα του επιπέδου εφαρμογής στην υπηρεσία δικτύου ή στην εφαρμογή για επεξεργασία.

Η ανάλυση πρωτοκόλλου δικτύου ακολουθεί τις ίδιες αρχές με τη διαδικασία αποσυσκευασίας (που περιγράφεται παραπάνω) η οποία πρέπει να επιλυθεί από κάτω προς τα πάνω στο μοντέλο OSI. Ο αρχικός κεντρικός υπολογιστής προορισμού όταν λαμβάνει το πακέτο ενδιαφέρεται μόνο για το επίπεδο εφαρμογής[[5]](#footnote-5) τα δεδομένα που περιέχει, τα τμήματα μεταφοράς, τα πακέτα δικτύου και το περιεχόμενο πληροφοριών πλαισίων σύνδεσης ελέγχονται αλλά στη συνέχεια απορρίπτονται, ο κεντρικός υπολογιστής δεν χρειάζεται να διατηρεί προσωρινή μνήμη για αυτά, ενώ το λογισμικό/υλισμικό ανάλυσης πρωτοκόλλου δικτύου πρέπει να αποθηκεύσει όλα τα πεδία κεφαλίδας του πληροφορίες για τα διάφορα επίπεδα δικτύου, καθώς και το υψηλότερο επίπεδο περιεχομένου δεδομένων επιπέδου εφαρμογής, προκειμένου οι μηχανικοί να κατανοήσουν το πλήρες εύρος των πληροφοριών πακέτων δικτύου.

Για να λειτουργήσει ένας sniffer πρώτα πρέπει να προσδιορίσει τον τύπο του πρωτοκόλλου δικτύου και την αντίστοιχη τυπική προδιαγραφή πρωτοκόλλου, ανάλυση πακέτων.

Γενικά, περιλαμβάνει τα ακόλουθα βήματα:

1. Πρώτον, ο ανιχνευτής δικτύου έλαβε ακατέργαστα δεδομένα είναι σε δυαδική μετάδοση επιπέδου σύνδεσης πακέτων, οι περισσότερες περιπτώσεις είναι πλαίσιο δεδομένων Ethernet;



1. Ανάλυση δομής του πλαισίου δεδομένων Ethernet που περιέχει πάντα πληροφορίες για το επόμενο επίπεδο OSI e.g., 0x0800 equals IPv4

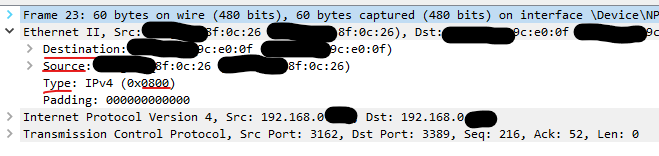


Figure 1 https://en.wikipedia.org/wiki/Ethernet\_frame

1. Περαιτέρω για την ανάλυση του πακέτου IP, εάν το κομμάτι bit έχει οριστεί, τότε μια αναδιάρθρωση θραύσματος IP, κάτω από το Πρωτόκολλο IP στο πεδίο κεφαλίδας πρωτοκόλλου, καθορίζει τον τύπο πρωτοκόλλου του επιπέδου μεταφοράς, συνήθως TCP (6) ή UDP (17) και εξάγει τα δεδομένα του επιπέδου μεταφοράς IP στα περιεχόμενα του πακέτου.

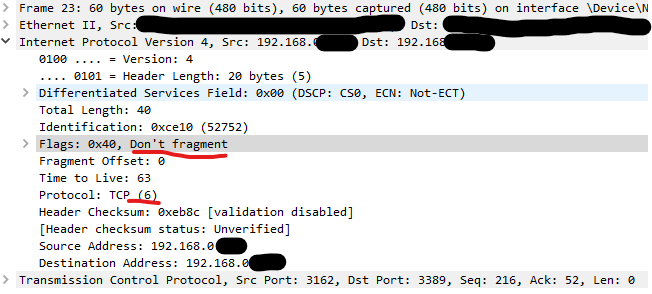


Figure 2 https://en.wikipedia.org/wiki/IPv4#Packet\_structure

1. Συνεχίστε να αναγνωρίζετε συγκεκριμένες θύρες προορισμού TCP ή UDP πρωτοκόλλων επιπέδου εφαρμογής, όπως DNS, BGP, HTTPS, Telnet, DHCP και άλλα πακέτα πρωτοκόλλου στην περίπτωσή μας 3389/TCP/UDP που είναι μια περίοδος λειτουργίας RDP, και συνδέοντας το TCP ή Τα πακέτα UDP του ανασυνδυασμένου, έχουν την εφαρμογή διαδραστικού περιεχομένου για το πρωτόκολλο του επιπέδου εφαρμογής;
2. Σύμφωνα με το αντίστοιχο πρωτόκολλο επιπέδου εφαρμογής που ενοποιεί την ανάκτηση δεδομένων, είναι η πραγματική μεταφορά δεδομένων

Για πρωτόκολλα άγνωστου δικτύου, όπως τα προσαρμοσμένα πρωτόκολλα που χρησιμοποιούνται από έναν αριθμό νέων κακόβουλων κωδικών, ή ορισμένα πρωτόκολλα χρησιμοποιούν κρυπτογράφηση για την προστασία, για παράδειγμα, πολύ δύσκολο για ανάλυση πρωτοκόλλου, η δυαδική αντίστροφη μηχανική απαιτεί αναλυτές με υψηλή τεχνική ικανότητα να προσδιορίσουν το μορφή αυτών των συμφωνιών [2].

# Εργαλεία ασφαλείας

## Wireshark

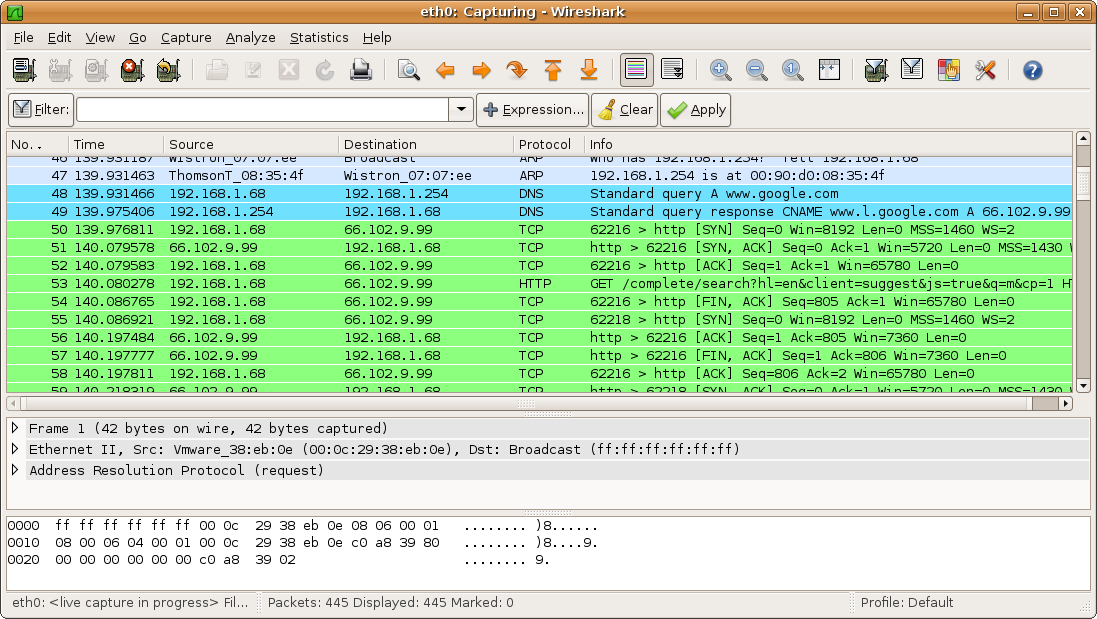


Figure 3 https://el.wikipedia.org/wiki/Wireshark

### Ιστορία

Ένας βιομηχανικός αναλυτής δικτύου ανοιχτού κώδικα [5], είτε εκτός σύνδεσης είτε σε απευθείας σύνδεση αποθήκευση και διαδικασία για την αντιμετώπιση προβλημάτων δικτύου, την ανάλυση, την ανάπτυξη λογισμικού και πρωτοκόλλων επικοινωνιών και την εκπαίδευση γραμμένο σε C++ με άδεια GPL-2.0+. Αναπτύχθηκε αρχικά το 1998, είναι γνωστό για την ευελιξία και την ωραία προσέγγιση UI/UX εμπειρίας GUI, διαθέσιμη στις περισσότερες τυπικές πλατφόρμες συστημάτων, π.χ. Windows, Linux, macOS κλπ [6].

Επιπλέον, είναι επίσης διαθέσιμο στη γραμμή εντολών γνωστό tshark.

### Περιπτώσεις χρήσεις & Μειονεκτήματα

#### Θετικά [7] [8]

* Ανοιχτή πηγαίου κώδικα
* Επίπεδη καμπύλη μάθησης
* GUI εργαλείο – Ευκολία
* Ανάλυση πακέτων και αναγνώριση και αποκωδικοποίηση ωφέλιμων φορτίων δεδομένων εάν είναι γνωστά τα κλειδιά κρυπτογράφησης
* Προηγμένες διεπαφές δικτύου
* Σύνθετα φίλτρα (εμφάνιση & λήψη)[[6]](#footnote-6)
* Μπορεί να εισάγει/διαβάσει αρχεία tcpdump (διασταυρούμενη συμβατότητα)
* Παρέχει αποκωδικοποίηση της σύλληψης πακέτων που βασίζεται σε πρωτόκολλο.
* API testing/troubleshooting

#### Αρνητικά

* Τα φίλτρα είναι δύσκολο να θυμηθούν και να διαμορφωθούν;
* ~ Εκφοβιστικό για τους νέους χρήστες λόγω των χρωμάτων και των στηλών του;

#### Χρήση

Το Wireshark χρησιμοποιείται για την αντιμετώπιση προβλημάτων του Δικτύου είτε για Δίκτυο [[7]](#footnote-7) σφάλματα λογισμικού/υλισμικού μέχρι την ανίχνευση εισβολών ασφαλείας [9] ως βοηθητικό στοιχείο. Με αυτό, μπορείτε να συλλέξετε και να ξαναχτίσετε πακέτα, να ακούσετε κίνηση VoIP με έξοδο ήχου, να αποκρυπτογραφήσετε δομές πακέτων που συλλέξατε[[8]](#footnote-8), και στο μέλλον να τα αποκρυπτογραφήσει με εισαγωγή μυστικού κλειδιού. Από ένα οικιακό δίκτυο, μια μικρή επιχείρηση σε επίπεδο επιχείρησης ή εκπαιδευτικό σκοπό για να κατανοήσετε πώς η κυκλοφορία των πρωτοκόλλων αλληλεπιδρά με εσάς και το Διαδίκτυο.

Μια σημαντική σημείωση είναι ότι το Wireshark καταγράφει μόνο τη δραστηριότητα διεπαφών του κεντρικού υπολογιστή (είτε καταγράφοντας πακέτα εκπομπής κ.λπ. σε ακατάλληλη λειτουργία είτε μόνο για τον κεντρικό υπολογιστή, εάν προορίζεται) που σημαίνει ότι δεν μπορείτε να μυρίσετε τον "ολόκληρο" τομέα εκπομπής/(V)LAN ή Δίκτυο αλλά μόνο ό,τι σας έρχεται, μια λύση για να επιτευχθεί αυτό είναι να ενεργοποιήσετε το πρωτόκολλο κατοπτρισμού θύρας γνωστό και ως (x)SPAN στη συσκευή δικτύου [10].

## TCPdump

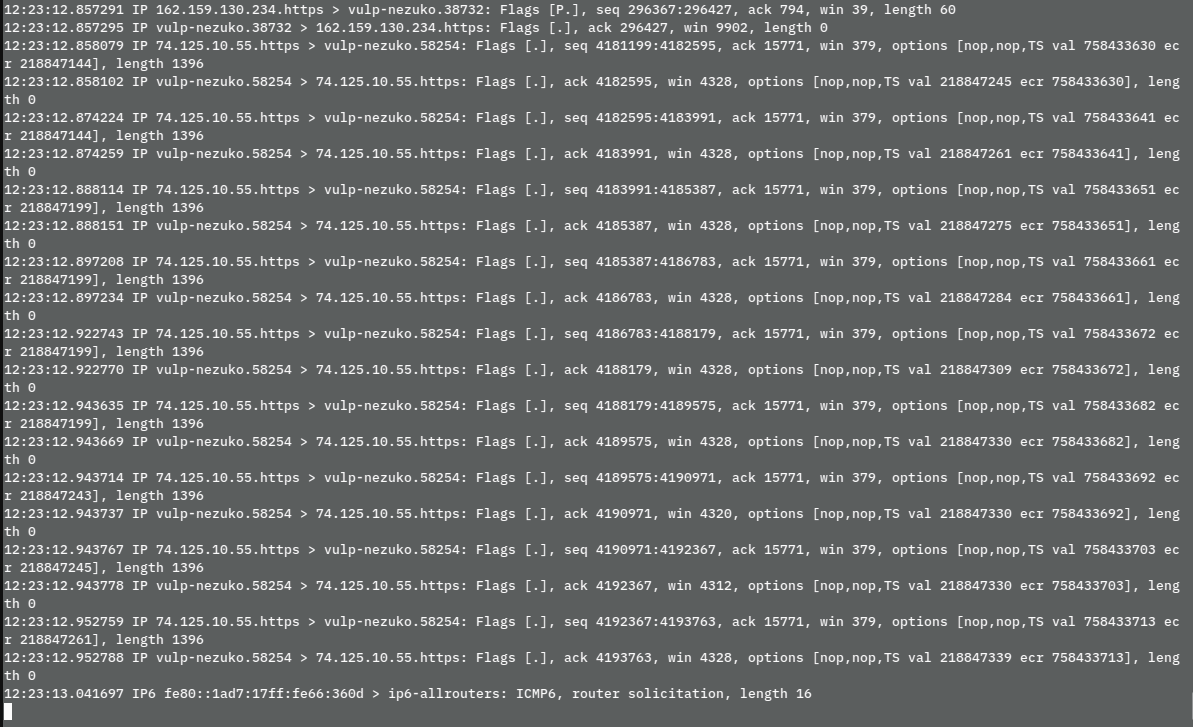


Figure 4 https://en.wikipedia.org/wiki/Tcpdump

### Ιστορία

Ένας βιομηχανικός αναλυτής δικτύου ανοιχτού κώδικα, είτε εκτός σύνδεσης είτε σε απευθείας σύνδεση αποθήκευση και διαδικασία για την αντιμετώπιση προβλημάτων δικτύου, την ανάλυση, την ανάπτυξη λογισμικού και πρωτοκόλλων επικοινωνιών και την εκπαίδευση. Προορίζεται για πιο προχωρημένους επαγγελματίες χρήστες λόγω της πολυπλοκότητάς του χωρίς GUI, γραμμένο σε C με την άδεια BSD. Αναπτύχθηκε αρχικά το 1988 και χρησιμοποιεί μια τεχνική διεπαφή γραμμής εντολών για την έξοδο δεδομένων, διαθέσιμη στις περισσότερες τυπικές πλατφόρμες συστήματος, π.χ. Windows, Linux, macOS κ.ά. [11].

### Περιπτώσεις χρήσεις & Μειονεκτήματα

#### Θετικά [8]

* Ανοιχτή πηγαίου κώδικα
* φίλτρα
* Ρύθμιση λόγω CLI (δεν χρειάζεται GUI για εκτέλεση σε διακομιστή)
* Ανάλυση πακέτων & απλή αναγνώριση και αποκωδικοποίηση [[9]](#footnote-9)
* Προεγκατεστημένο στα περισσότερα repos Linux από προεπιλογή

#### Αρνητικά

* Απότομη καμπύλη εκμάθησης
* Εκφοβιστική εμπειρία CLI
* Απλή ανάλυση συγκεκριμένων τύπων, π.χ., ερωτήματα DNS
* Απλές συμβατικές διεπαφές που βασίζονται σε σύστημα

#### Χρήση

Όπως κάνει η χρήση του Wireshark με την αντίθεση, δεν μπορεί να χρησιμοποιηθεί για "ζωντανή" αναπαραγωγή VoIP ή μηχανισμούς αποκρυπτογράφησης wi-fi.

## Συγκρίτικά αποτελέσματα

**Wireshark vs TCPdump**

|  |  |  |
| --- | --- | --- |
| **Criteria** | **Wireshark** | **tcpdump** |
| Ανοιχτή πηγή | **+** | **+** |
| Εύχρηστος | **+** | **-** |
| Εύκολο στην εκμάθηση | **+** | **-** |
| Ανάλυση & αποκωδικοποίηση αναγνώρισης πακέτων | **+** | **-** |
| Αποκωδικοποίηση αποτελεσματικότητας | **+** | **-** |
| Γρήγορη εγκατάσταση στον κεντρικό υπολογιστή | **+** | **+** |
| Φίλτρα | **+** | **-** |
| Διεπαφές δικτύου | **+** | **-** |
| Διασταυρούμενη συμβατότητα | **+** | **-** |
| Ευελιξία στη χρήση ζωντανών | **+** | **+** |
| Αντιμετώπιση προβλημάτων | **+** | **+** |
| Δυνατότητες λήψης δεδομένων | **+** | **+** |
| Πρότυπο της βιομηχανίας | **+** | **+** |
| Υποστήριξη προϊόντος και κοινότητας | **+** | **+** |

#### **Σημειώσεις προς λήψη & Επεξήγηση επιλεγμένων κριτηρίων**

Όταν συγκρίνουμε προϊόντα, πρέπει να έχουμε κατά νου ορισμένα βασικά πράγματα.

Εάν είναι αρκετά μεγάλο εκεί έξω, ώστε να μπορούμε να βασιστούμε σε αυτήν ως επιχείρηση και να το προσαρμόσουμε κάτω από τον γενικό όρο «βιομηχανικό πρότυπο» από τα χαρακτηριστικά του, την καμπύλη εκμάθησης, την υποστήριξη προϊόντων και τη διαθεσιμότητα του προϊόντος σε πολλές μορφές.

• **Ανοιχτού κώδικα:** Για μάθηση και ανάπτυξη και κατανόηση. Μοιραστείτε == φροντίδα

• **Εύκολο στη χρήση**: Αφαίρεση πολύπλοκου υποκείμενου συστήματος

• **Εύκολη εκμάθηση:** Εύκολο στη χρήση + περισσότεροι πελάτες

• **Ανάλυση & αποκωδικοποίηση αναγνώρισης πακέτων:** Λεπτομερής κατανόηση ενός προβλήματος δικτύου και παρακολούθησης

• **Αποκωδικοποίηση αποδοτικότητας:** Καμία σπατάλη πόρων για επιπλέον βήματα εντός αλγορίθμων. Κατευθείαν στον προβληματικό στόχο

• **Γρήγορη εγκατάσταση στον κεντρικό υπολογιστή:** Εύκολο στη χρήση + χωρίς προβλήματα δοκιμής ή δίκτυα παραγωγής

• **Φίλτρα:** Λεπτομερής ανάλυση κατ' απαίτηση πακέτων για προβολή διατηρώντας παράλληλα μικρό μέγεθος αρχείου + Διαχείριση μνήμης προγραμμάτων. Απλώς πηγαίνει βαθιά.

• **Διεπαφές δικτύου:** Κάθε θύρα εισόδου/εξόδου από ένα κεντρικό σύστημα

• **Cross-Compatibility:** Εύκολη μεταφορά σε οποιαδήποτε πλατφόρμα και πρόγραμμα

• **Ευελιξία στη χρήση live:** Τροποποίηση φίλτρου κατά παραγγελία

• Αντιμετώπιση προβλημάτων: Λεπτομερής ανάλυση OSI με GUI για να γίνει ακόμα πιο απλή

• **Ικανότητες σύλληψης δεδομένων:** Χρησιμοποιεί κάθε τεχνική/πρωτόκολλη ικανότητα στο μέγιστο που εφαρμόζεται σε επίπεδο λογισμικού και υλικού για να συλλάβει και να αποκαλύψει τα δεδομένα που ρέουν στο καλώδιο/αέρα

• **Industry Standard:** Απλώς λειτουργεί για τα πάντα, επομένως η προσαρμογή για όλους είναι ευπρόσδεκτη. Το οικοσύστημα επεκτείνεται.

• **Υποστήριξη προϊόντος και κοινότητας:** Βελτίωση και βελτίωση (λογισμικό) και υποστήριξη πελατών με λύσεις και πρόσθετα/εργαλεία για ένα ισχυρό οικοσύστημα.

#### **Αποτελέσματα**

Από τα παραπάνω αποτελέσματα, μπορούμε να δούμε ξεκάθαρα ότι το Wireshark είναι ο νικητής, ωστόσο, το tcpdump είναι το προεπιλεγμένο πακέτο πακέτου λογισμικού που διατίθεται στις περισσότερες διανομές Linux προεγκατεστημένο και είναι πολύ εύκολο να το ρυθμίσετε σε έναν κεντρικό υπολογιστή, να καταγράψετε τα δεδομένα αποθηκεύστε τα και προωθήστε τα σε έναν άλλο κεντρικό υπολογιστή που φιλοξενεί την εφαρμογή Wireshark όλα αυτά χρησιμοποιώντας απλώς το CLI/διεπαφή γραμμής εντολών. Σε αντίθεση, το tshark που είναι μια έκδοση CLI του Wireshark δεν είναι προεγκατεστημένο.

Το θέμα δεν είναι ποιο είναι καλύτερο αλλά ποια προσέγγιση σχεδιασμού έχουμε κατά νου για τη λήψη και την ανάλυση των Δεδομένων. Μια κοινή ροή εργασίας/αγωγός στο sniffing δικτύου είναι tcpdump -> Wireshark ή tshark -> Wireshark επειδή το περιβάλλον διακομιστή GUI συνήθως δεν αποτελεί επιλογή και μπορεί να εισαγάγει ευπάθειες ασφαλείας και εύρος ζώνης κατανάλωσης δικτύου σε υψηλότερους ρυθμούς, αλλά αν δεν ξέρετε τι ψάχνετε γιατί το γραφικό περιβάλλον εργασίας του Wireshark είναι πιο γρήγορο και πιο συνεπές οπτικά στην ανάλυση μοτίβων εν κινήσει, επειδή ως άνθρωποι, μπορούμε να αντιληφθούμε πληροφορίες και να τις αναλύσουμε πιο γρήγορα όταν οπτικά βλέπουμε κάτι πιο κατανοητό.

# Ανασκόπηση βιβλιογραφίας ανάλυσης πραγματικής περίπτωσης

## Η μελέτη περίπτωσης [12]

### Η τεχνική προσέγγισης προβλήματος

Ένας μεγάλος πάροχος υπηρεσιών Διαδικτύου που βλέπει τυχαίες αποτυχίες ενός πελάτη/ών να λάβει IP/εγγραφή στην υπηρεσία πλατφόρμας IPTV του. Υπάρχουν πολλές πηγές δεδομένων και δεν έχουν όλα πρόβλημα.

Η πλειοψηφία των πελατών της ίδιας ομάδας που σημαίνει ότι είναι συνδεδεμένοι στο ίδιο δίκτυο μεταγωγής LAN L2 μπορούν να εγγραφούν στην υπηρεσία τους, αλλά ορισμένοι για περίεργους λόγους δεν μπορούν.

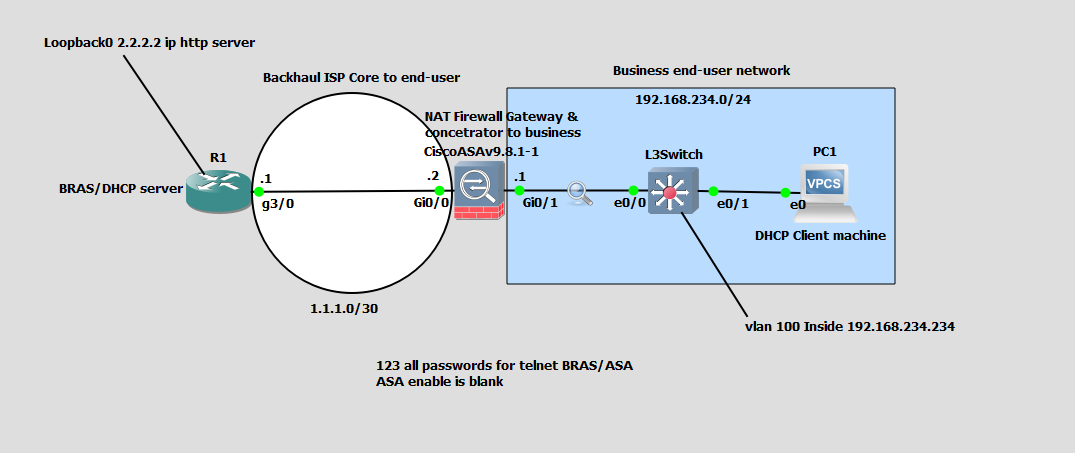


Figure 5 Simulation of the example in GNS3

### Πρώτος γυρος

Το πρώτο βήμα ήταν να κοιτάξουμε τον διακομιστή μητρώου για την παροχή της υπηρεσίας σε IP/καταχωρητές (BRAS). Ο διακομιστής της εφαρμογής βλέπει το DHCP Discover αυτού του μεμονωμένου πελάτη, μπορούμε τώρα να γνωρίζουμε ότι πράγματι στάλθηκε το DHCP Discover και μετά κοιτάμε τον πελάτη/ s logs επιτυγχάνοντας αυτό υπάρχουν 2 διαδικασίες.

1) Στείλτε έναν απομακρυσμένο μηχανικό στον ιστότοπο

2) Θύρα Αντικατοπτρίστε τη θύρα μεταγωγής για να δείτε την κίνηση της υπηρεσίας IPTV.

Ακολουθούμε πάντα την επιχειρηματική ροή για την επίλυση ενός ζητήματος. Ο Μηχανικός στην τοποθεσία λαμβάνει τα αρχεία καταγραφής και διασφαλίζει ότι ο κατάλληλος τελικός καταναλωτής L1 είναι σε καλή κατάσταση ακεραιότητας και δομή Σχεδίασης Δικτύου για τυχόν περίεργες διαμορφώσεις μεταξύ αυτών, διασφαλίζει ότι η διαδικασία DHCP DORA θα είναι συνεχώς ενεργή ότι λόγω της φύσης της εφαρμογής DHCP κάθε αποτυχία ο πελάτης στέλνει το επόμενο Request Discover με μια πρόσθετη μεγάλη καθυστέρηση στην παραγωγή αυτού του πακέτου.

Στα αρχεία καταγραφής, διαπιστώσαμε ότι η σύνδεση «κολλούσε» στη φάση της χειραψίας της εφαρμογής και στη συνέχεια έβγαινε σφάλμα. Δεν μπορούσε να επικοινωνήσει ή να λάβει πληροφορίες σε όλο το δίκτυο.

Κάνουμε telnet πάνω από το SSH και συνδέουμε στον πλησιέστερο κόμβο Edge από την πλευρά του ISP[[10]](#footnote-10) στην περίπτωσή μας, το L3 Switch (όχι στον ίδιο τον τελικό χρήστη/πελάτη, επειδή οι μηχανικοί λειτουργίας δεν έχουν το δικαίωμα για λόγους νόμου) και μεταφέρουμε τον αντικατοπτρισμό της κυκλοφορίας χρησιμοποιώντας RSPAN σε έναν σχεδιασμένο συγκεκριμένο κόμβο στο δίκτυο που χρησιμοποιείται για τη λήψη και αναλύστε την επισκεψιμότητα χρησιμοποιώντας το Wireshark χωρίς να προκαλείτε προβλήματα εύρους ζώνης.

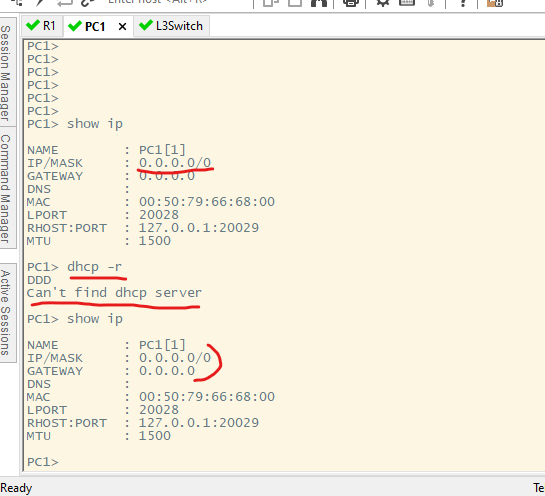


Figure 6 Step 1) Client's PC unable to get DHCP offer

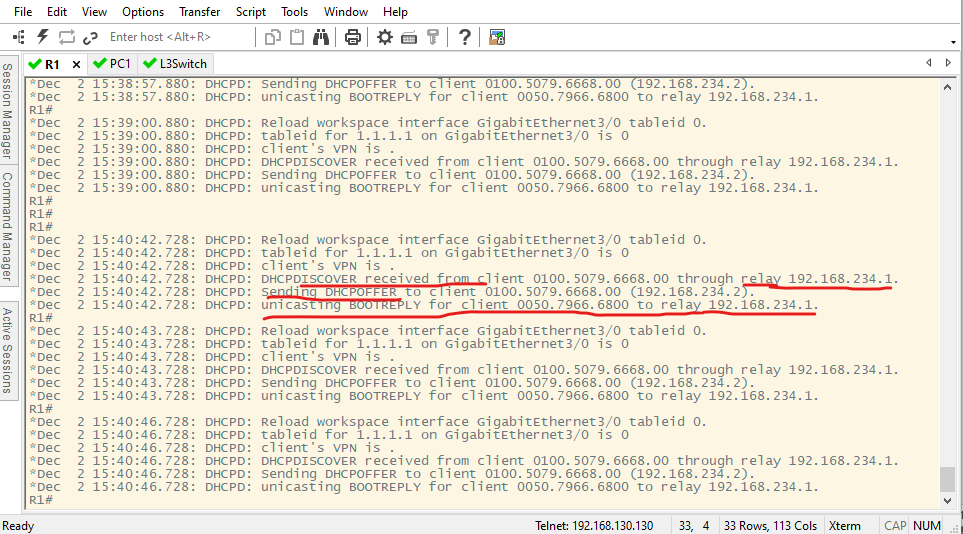


Figure 7 Step 2) Server Logs shows that communication is ok up to a point

### Δεύτερος γύρος

Επιβεβαιώνουμε ότι το DHCP Discover στάλθηκε πράγματι. Αλλά καμία προσφορά δεν εμφανίστηκε παρά το γεγονός ότι ο διακομιστής έστειλε αυτό το μήνυμα.

Κάπου στη μέση έχουν πέσει τα πακέτα. Το σημαντικό σημείο είναι ότι ο διακομιστής στέλνει μια απάντηση στο αίτημα του πελάτη/ων χωρίς επιτυχία να το λάβει, αλλά γιατί;

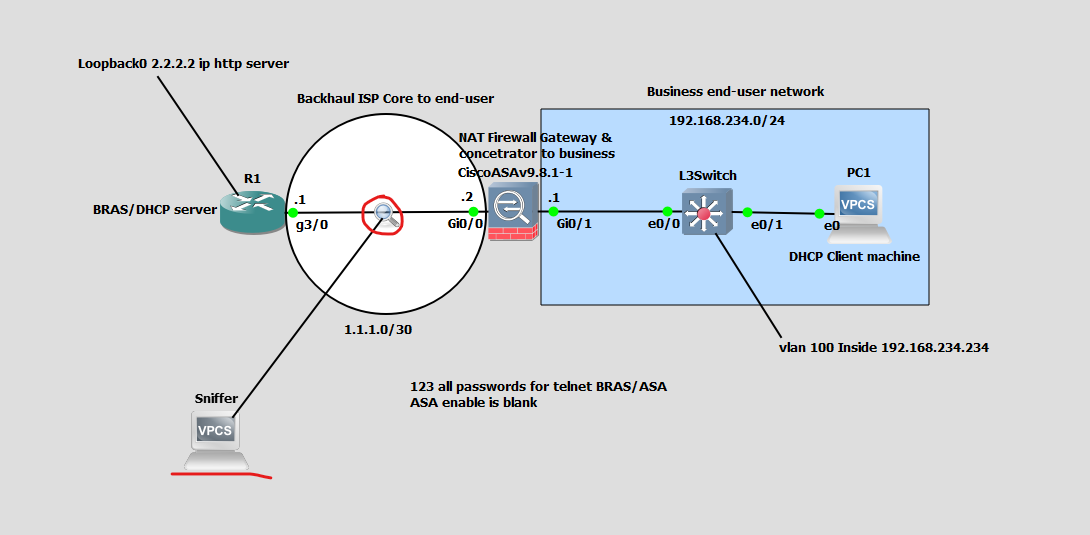


Figure 8 Step 3) port forwarding the traffic and capture with Wireshark on top of WAN backhaul

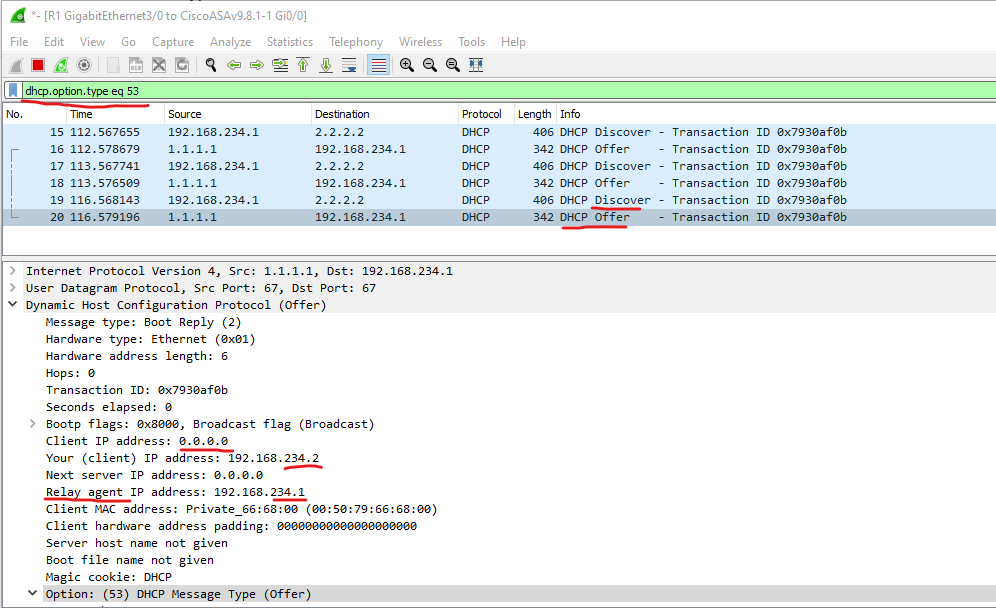


Figure 9 Steps 4) Wireshark DORA process. The Server in WAN sends the offer back

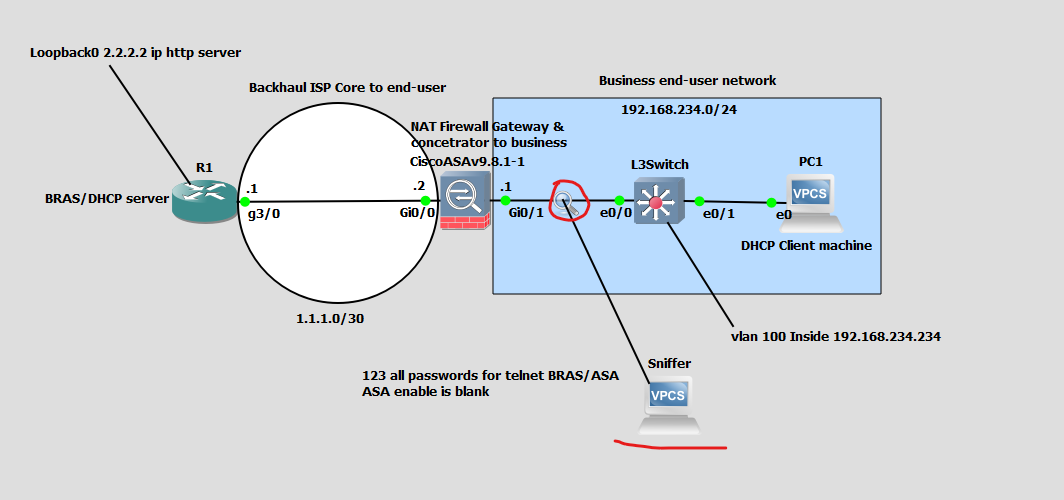


Figure 10 Step 5) Inside Intranet (Figure 11) business there is no offer seen so the error is before that

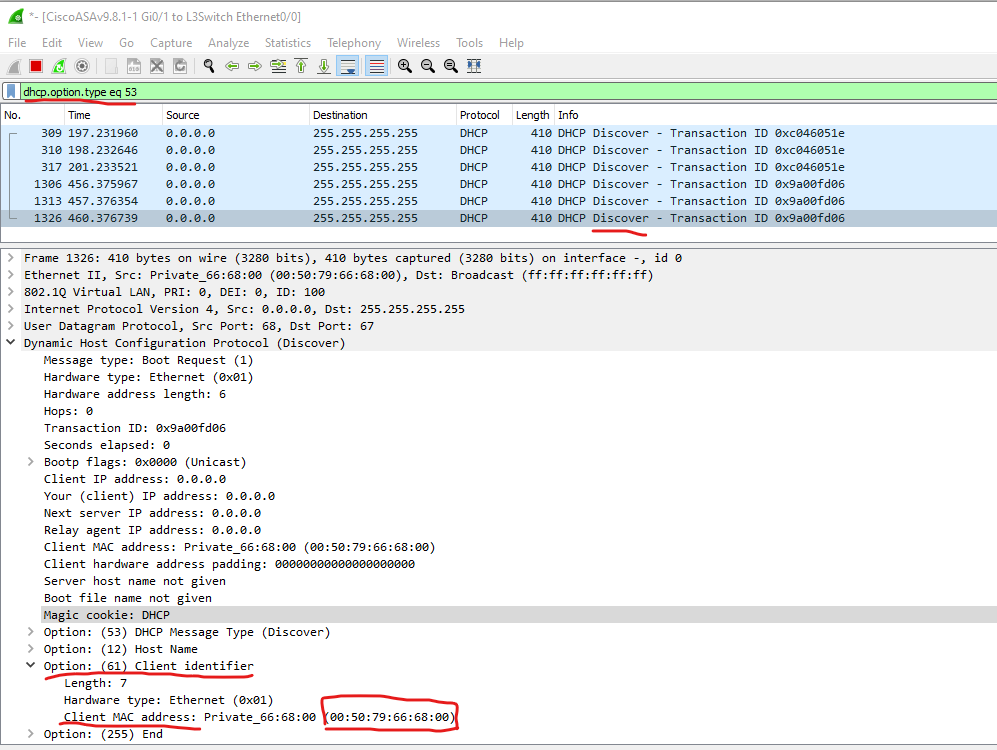


Figure 11 Steps 6) In the Intranet there is no Offer seen so the error/misconfiguration must be on the Firewall Concentrator

### Περιορίζοντας το πεδίο εφαρμογής

Το αίτημα πελάτη μπορεί να σταλεί μέχρι το τέλος στον διακομιστή μέσω του WAN.

Ο διακομιστής ανταποκρίνεται, αλλά λίγο πριν το δίκτυο Metro Ethernet, το πακέτο εξαφανίζεται.

Έτσι, το επόμενο βήμα είναι να μεταφέρετε το Mirror/κλωνοποιήστε την κυκλοφορία από κάθε κατεύθυνση «παιδιού» σε αυτό το γράφημα[[11]](#footnote-11) απευθείας συνδεδεμένο ή λογικά συνδεδεμένο με την τελευταία γνωστή διεπαφή δρομολογητή που λαμβάνει τα πακέτα με επιτυχία.

Ακολουθώντας το μονοπάτι σταδιακά μπορούμε να φτάσουμε στην αιτία της αποτυχίας του δικτύου και της δυσαρέσκειας του πελάτη. Θα μπορούσε να είναι ένα ζήτημα κατεύθυνσης διασύνδεσης τείχους προστασίας το γεγονός ότι μια περικοπή πολιτικής είναι απενεργοποιημένη ή ακόμα και μια εσφαλμένη διαμόρφωση δικτύου με οποιοδήποτε είδος υπηρεσιών σύγκρουσης, ειδικά όταν ένας ISP αποτελείται από 3+ κύρια δίκτυα που ανταλλάσσουν επικοινωνία στη διαδικασία, σταθεροί πελάτες, πελάτες κινητής τηλεφωνίας (CPN), δίκτυο παράδοσης περιεχομένου (CDN), IMS, κ.ά.

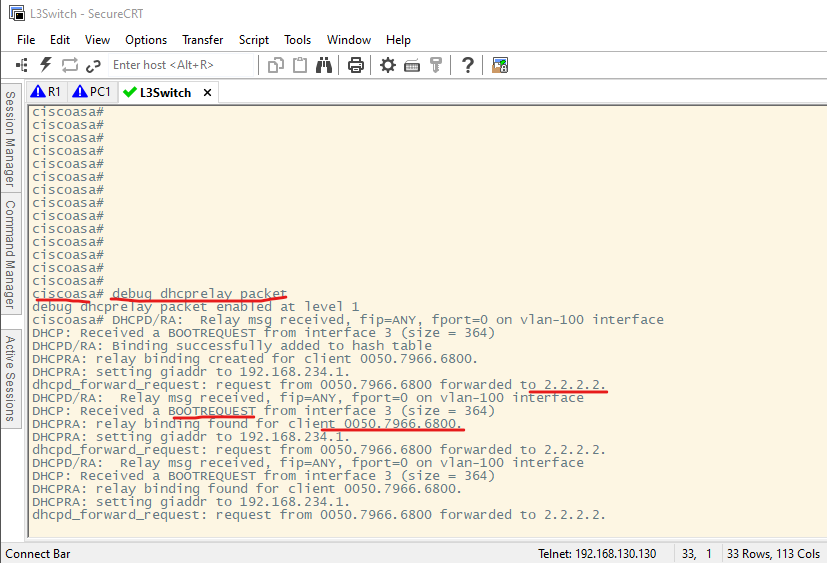


Figure 12 ASA firewall receives correct clients discover but still no offer

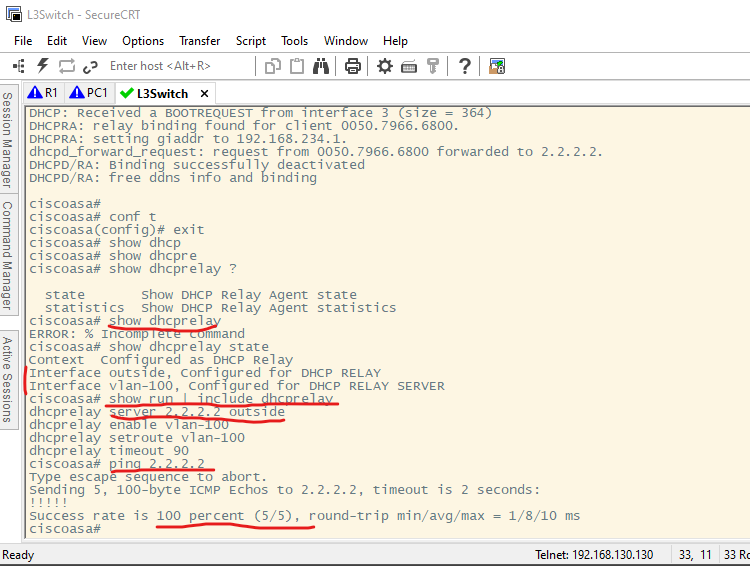


Figure 13 Firewall can reach the DHCP server

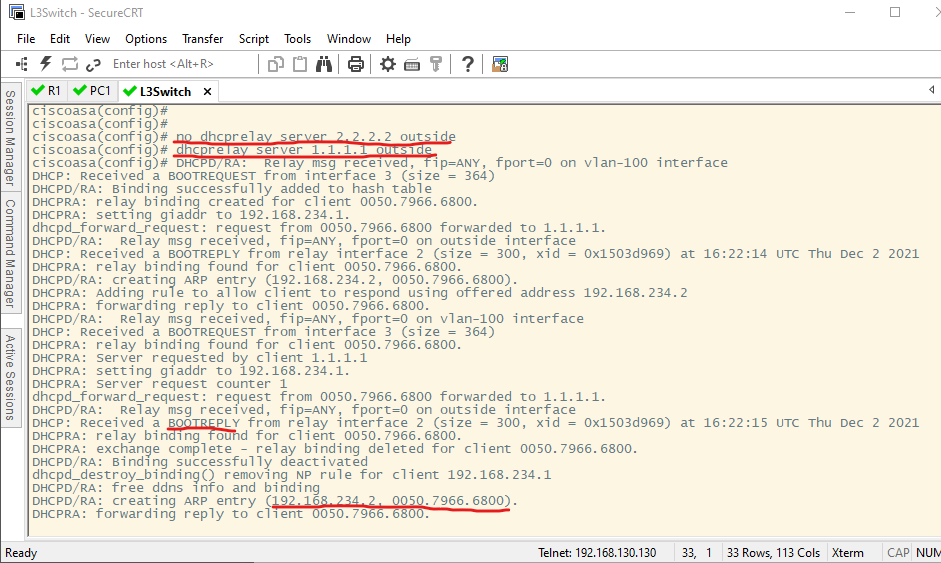


Figure 14 The problem was the DHCP server IP address as not adjacent

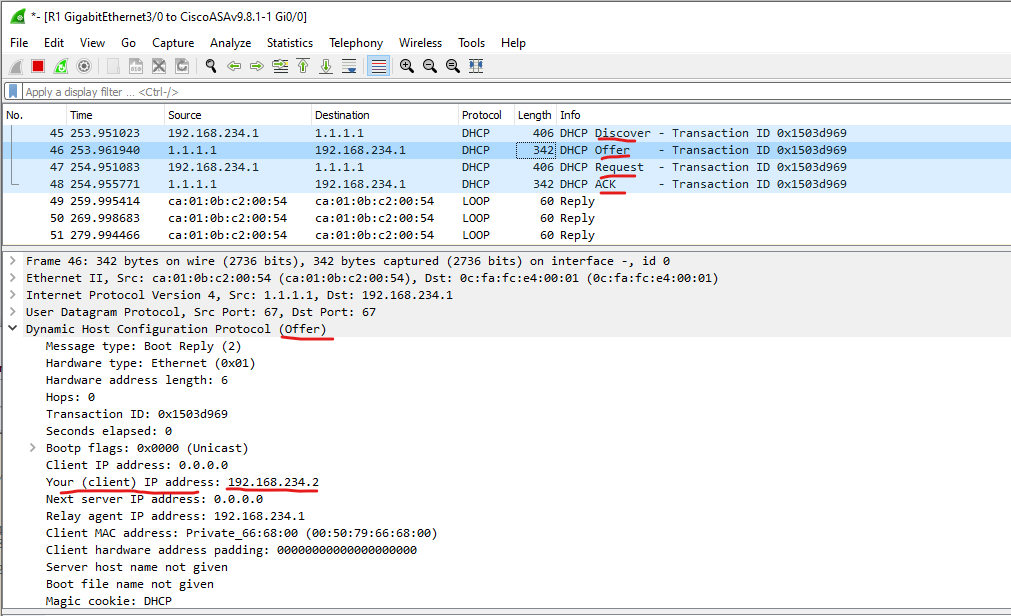


Figure 15 Successful DORA

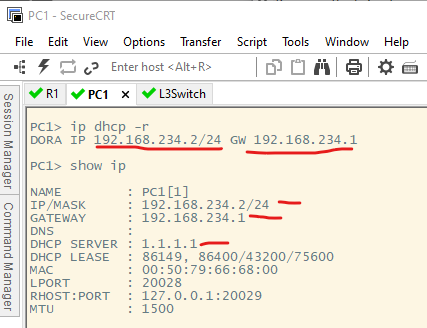


Figure 16 Client DORA succeed

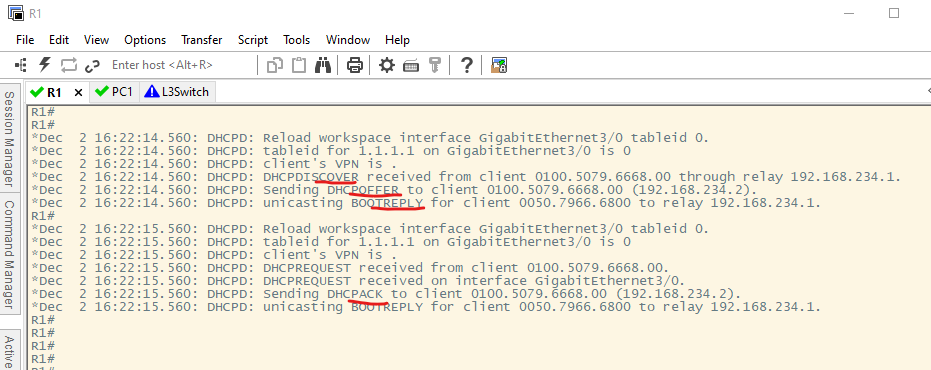
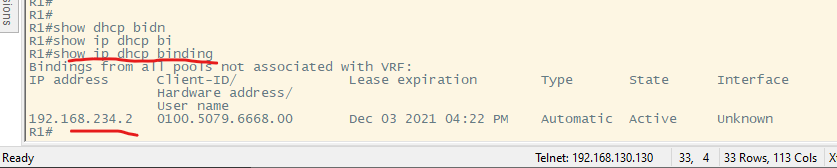


Figure 17 Logs on DHCP server



### Μαθήματα & Απαντήσεις

• Για να κατανοήσουμε ένα πρόβλημα πρώτα κατανοούμε το σφάλμα επιπέδου εφαρμογής και μετά το δίκτυο.

• Ανεξάρτητα από το πόσο μεγάλο είναι το δίκτυο, κόψτε το σε κομμάτια μέχρι να κλείσετε το ζήτημα, είναι σαν μια λογική αλγορίθμου διαδρομής συντομότερης διαδρομής, στην πραγματικότητα, αυτός είναι ακριβώς ο τρόπος με τον οποίο θα λειτουργήσει ένας αλγόριθμος στη λύση π.χ., κάνουμε γείτονες, πολλές φορές με τον ίδιο τρόπο που χρησιμοποιούμε για να λύσουμε αγνωστικά προβλήματα[[12]](#footnote-12).

• Ανιχνεύστε το πρόβλημα με την κατάλληλη μεθοδολογία που εφαρμόζεται, π.χ. από κάτω επάνω στο επίπεδο OSI/TCP-IP [13].

• Καταγράψτε το πρώτο σημείο αστοχίας

• Καταγράψτε το τελευταίο σημείο αποτυχίας

• Επαναλαμβάνω

• Το Wireshark είναι φίλος σας

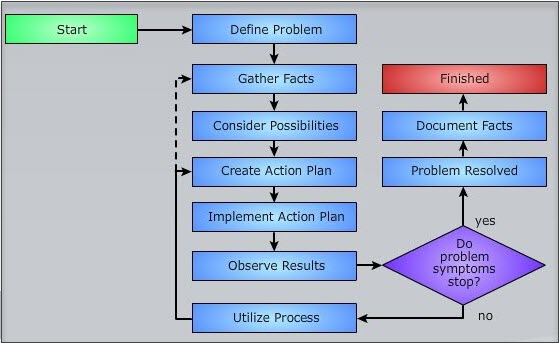


Figure 18 <https://www.ciscopress.com/articles/article.asp?p=2273070&seqNum=2>

# Αναφορές

|  |  |
| --- | --- |
| [1] | R. Spangler, "Packet Sniffing on Layer 2 Switched Local Area Networks," 15 December 2003. [Online]. Available: https://www.helpnetsecurity.com/2003/12/15/packet-sniffing-on-layer-2-switched-local-area-networks/. |
| [2] | Q.-X. Wu, "The Network Protocol Analysis Technique in Snort," *Physics Procedia,* vol. 25, pp. 1226-1230, 2012. |
| [3] | "Data Encapsulation," [Online]. Available: https://www.learncisco.net/courses/ccna/part-1-internetworking/data-encapsulation.html . [Accessed 11 11 2021]. |
| [4] | "Encapsulation," [Online]. Available: https://study-ccna.com/encapsulation/. [Accessed 11 11 2021]. |
| [5] | "1.1.7 what Wireshark is not," [Online]. Available: https://www.wireshark.org/docs/wsug\_html\_chunked/ChapterIntroduction.html. [Accessed 11 11 2021]. |
| [6] | "Wireshark - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Wireshark. [Accessed 11 11 2021]. |
| [7] | "Pros and Cons of Wireshark 2021," [Online]. Available: https://www.trustradius.com/products/wireshark/reviews?qs=pros-and-cons. [Accessed 11 11 2021]. |
| [8] | "Tcpdump vs Wireshark," [Online]. Available: https://www.educba.com/tcpdump-vs-wireshark/. [Accessed 11 11 2021]. |
| [9] | "1.1.8 what Wireshark is not," [Online]. Available: https://www.wireshark.org/docs/wsug\_html\_chunked/ChapterIntroduction.html. [Accessed 11 11 2021]. |
| [10] | ashirkar, "Understanding SPAN,RSPAN,and ERSPAN," cisco, [Online]. Available: https://community.cisco.com/t5/networking-documents/understanding-span-rspan-and-erspan/ta-p/3144951. [Accessed 11 11 2021]. |
| [11] | "tcpdump - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Tcpdump. [Accessed 11 11 2021]. |
| [12] | T. Poth, "SHARKFEST '12," [Online]. Available: https://sharkfestus.wireshark.org/sharkfest.12/presentations/BI-8b\_Wireshark\_Software\_Case\_Studies-Tim\_Poth.pdf. [Accessed 11 11 2021]. |
| [13] | C. Press, " Structured Troubleshooting Approaches > Troubleshooting Methods for Cisco IP Networks," [Online]. Available: https://www.ciscopress.com/articles/article.asp?p=2273070&seqNum=2. [Accessed 2021 11 11]. |
| [14] | nayarasi, "Decrypt WPA2-PSK using Wireshark," [Online]. Available: https://mrncciew.com/2014/08/16/decrypt-wpa2-psk-using-wireshark/ . [Accessed 11 11 2021]. |
| [15] | "HowToDecrypt802.11 - The Wireshark Wiki," [Online]. Available: https://wiki.wireshark.org/HowToDecrypt802.11 . [Accessed 11 11 2021]. |
| [16] | "Cisco three-layer hierarchical model," [Online]. Available: https://study-ccna.com/cisco-three-layer-hierarchical-model/ . [Accessed 11 11 2021]. |
| [17] | "Hierarchical internetworking model - Wikipedia," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Hierarchical\_internetworking\_model. |
| [18] | C. Press, "Hierarchical Network Design Overview (1.1) > Cisco Networking," [Online]. Available: https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4. [Accessed 11 11 2021]. |

# Παράρτημα

## Γλωσσάριο

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Αγνωστικισμου/agnostic | Δεν εξαρτάται από το περιεχόμενο, π.χ., χωρίς έντυπη κωδικοποίηση |
| Αφαίρεση/abstraction | Μια άποψη υψηλού επιπέδου των πραγμάτων από την οπτική γωνία του τελικού καταναλωτή χωρίς να γνωρίζει πάρα πολλά για τους υποκείμενους μηχανισμούς του, αλλά εξακολουθεί να μπορεί να το χρησιμοποιήσει. |
| DORA | Η διαδικασία αίτησης DHCP, Discover, Offer, Request, Accept/Ack |
| DHCP | Ένας διακομιστής με μια δυναμική ομάδα διευθύνσεων Διαδικτύου για κεντρικούς υπολογιστές που υποβάλλουν αίτημα ανακάλυψης. Μπορεί επίσης να δώσει στατική διεύθυνση IP μέσω επιλογών DHCP (82) καταγράφοντας την αντίστοιχη κράτηση mac σε IP. |
| LAN | Ένα ιδιωτικό τοπικό δίκτυο συνήθως μικρό εύρος λογικής (επικάλυψης) όχι σε φυσικό απαραίτητο. |
| VLAN | Εικονικά πολλαπλά δίκτυα στον ίδιο διακόπτη. Δημιουργεί έναν τομέα μετάδοσης. Διαχωρισμός ομάδων περιοχών LAN. |
| By Design by Default | Εισήχθη στο Design και εφαρμόστηκε από την αρχή σε περιβάλλον προπαραγωγής (πριν από την κυκλοφορία) |
| Repos | Αποθετήριο λογισμικού |
| DMVPN | Πρωτόκολλο Cisco για δυναμική ρύθμιση πολλαπλών VPN |
| IMS | Περιέκτης διαδικτύου υποσυστήματος πολυμέσων IP όπως LTE, PSTN et al. |

## Διαμόρφωση συσκευής

### R1

R1#sh run

Building configuration...

Current configuration : 1380 bytes

!

! Last configuration change at 15:36:03 UTC Thu Dec 2 2021

!

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

!

hostname R1

!

boot-start-marker

boot-end-marker

!

!

!

no aaa new-model

no ip icmp rate-limit unreachable

!

!

!

!

ip dhcp pool LAB\_WIRESHARK1

network 192.168.234.0 255.255.255.0

default-router 1.1.1.2

!

!

!

no ip domain lookup

ip cef

no ipv6 cef

!

!

multilink bundle-name authenticated

!

!

!

!

!

!

!

!

!

!

!

!

ip tcp synwait-time 5

!

!

!

!

!

!

!

!

!

interface Loopback0

ip address 2.2.2.2 255.255.255.255

!

interface FastEthernet0/0

ip address 1.1.1.1 255.255.255.252

shutdown

duplex full

!

interface FastEthernet2/0

no ip address

shutdown

speed auto

duplex auto

!

interface FastEthernet2/1

no ip address

shutdown

speed auto

duplex auto

!

interface GigabitEthernet3/0

ip address 1.1.1.1 255.255.255.252

negotiation auto

!

ip forward-protocol nd

!

!

ip http server

no ip http secure-server

ip route 0.0.0.0 0.0.0.0 1.1.1.2

!

ip access-list extended blockdhcp

deny udp any any eq bootpc

deny udp any any eq bootps

!

!

!

!

control-plane

!

!

line con 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line aux 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line vty 0

exec-timeout 40 0

password 123

logging synchronous

login

line vty 1 4

login

!

!

end

### L3Switch

L3Switch#sh run

Building configuration...

Current configuration : 1779 bytes

!

! Last configuration change at 14:57:15 UTC Thu Dec 2 2021

!

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

service compress-config

!

hostname L3Switch

!

boot-start-marker

boot-end-marker

!

!

logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL

logging buffered 50000

logging console discriminator EXCESS

!

no aaa new-model

!

!

!

!

!

no ip icmp rate-limit unreachable

!

!

!

no ip domain-lookup

ip cef

no ipv6 cef

!

!

!

spanning-tree mode rapid-pvst

spanning-tree extend system-id

!

!

vlan access-map 100 10

action forward

!

vlan internal allocation policy ascending

!

ip tcp synwait-time 5

!

!

!

!

!

!

!

!

!

!

!

!

!

interface Ethernet0/0

switchport trunk encapsulation dot1q

switchport mode trunk

!

interface Ethernet0/1

switchport access vlan 100

switchport mode access

!

interface Ethernet0/2

!

interface Ethernet0/3

!

interface Ethernet1/0

!

interface Ethernet1/1

!

interface Ethernet1/2

!

interface Ethernet1/3

!

interface Ethernet2/0

!

interface Ethernet2/1

!

interface Ethernet2/2

!

interface Ethernet2/3

!

interface Ethernet3/0

!

interface Ethernet3/1

!

interface Ethernet3/2

!

interface Ethernet3/3

!

interface Vlan1

no ip address

shutdown

!

interface Vlan100

ip address 192.168.234.234 255.255.255.0

!

ip default-gateway 192.168.234.1

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

ip route 0.0.0.0 0.0.0.0 192.168.234.1

!

ip access-list extended blockdhcp

deny udp any any eq bootpc

deny udp any any eq bootps

remark block incoming traffic

!

!

!

!

control-plane

!

!

line con 0

exec-timeout 0 0

privilege level 15

logging synchronous

line aux 0

exec-timeout 0 0

privilege level 15

logging synchronous

line vty 0 4

login

!

!

end

### ciscoasa

ciscoasa# sh run

: Saved

:

: Serial Number: 9AX11EB75NG

: Hardware: ASAv, 2048 MB RAM, CPU Pentium II 3695 MHz

:

ASA Version 9.8(1)

!

hostname ciscoasa

enable password $sha512$5000$FaLmzK1Wz00qhoGzib61Gg==$r3mrJCn3lTopIUOWExQsGQ== pbkdf2

xlate per-session deny tcp any4 any4

xlate per-session deny tcp any4 any6

xlate per-session deny tcp any6 any4

xlate per-session deny tcp any6 any6

xlate per-session deny udp any4 any4 eq domain

xlate per-session deny udp any4 any6 eq domain

xlate per-session deny udp any6 any4 eq domain

xlate per-session deny udp any6 any6 eq domain

passwd PLBb27eKLE1o9FTB encrypted

names

!

interface GigabitEthernet0/0

nameif outside

security-level 0

ip address 1.1.1.2 255.255.255.252

!

interface GigabitEthernet0/1

description Trunk

no nameif

no security-level

no ip address

!

interface GigabitEthernet0/1.100

description VLAN INSIDE 100

vlan 100

nameif vlan-100

security-level 100

ip address 192.168.234.1 255.255.255.0

!

interface GigabitEthernet0/2

shutdown

no nameif

no security-level

no ip address

!

interface GigabitEthernet0/3

shutdown

no nameif

no security-level

no ip address

!

interface GigabitEthernet0/4

shutdown

no nameif

no security-level

no ip address

!

interface GigabitEthernet0/5

shutdown

no nameif

no security-level

no ip address

!

interface GigabitEthernet0/6

shutdown

no nameif

no security-level

no ip address

!

interface Management0/0

shutdown

no nameif

no security-level

no ip address

!

ftp mode passive

access-list OUTSIDE extended deny udp any4 any4 eq bootpc

access-list OUTSIDE extended deny udp any4 any4 eq bootps

access-list OUTSIDE extended deny tcp any4 any4 eq telnet

pager lines 23

mtu outside 1500

mtu vlan-100 1500

no failover

no monitor-interface service-module

icmp unreachable rate-limit 1 burst-size 1

no asdm history enable

arp timeout 14400

no arp permit-nonconnected

arp rate-limit 8192

access-group OUTSIDE global

route outside 0.0.0.0 0.0.0.0 1.1.1.1 1

timeout xlate 3:00:00

timeout pat-xlate 0:00:30

timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02

timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00

timeout sip 0:30:00 sip\_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00

timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute

timeout tcp-proxy-reassembly 0:01:00

timeout floating-conn 0:00:00

timeout conn-holddown 0:00:15

timeout igp stale-route 0:01:10

user-identity default-domain LOCAL

aaa authentication login-history

no snmp-server location

no snmp-server contact

crypto ipsec security-association pmtu-aging infinite

crypto ca trustpoint \_SmartCallHome\_ServerCA

no validation-usage

crl configure

crypto ca trustpool policy

auto-import

crypto ca certificate chain \_SmartCallHome\_ServerCA

telnet 0.0.0.0 0.0.0.0 vlan-100

telnet timeout 5

ssh stricthostkeycheck

ssh timeout 5

ssh key-exchange group dh-group1-sha1

console timeout 0

dhcprelay server 1.1.1.1 outside

dhcprelay enable vlan-100

dhcprelay setroute vlan-100

dhcprelay timeout 90

threat-detection basic-threat

threat-detection statistics access-list

no threat-detection statistics tcp-intercept

dynamic-access-policy-record DfltAccessPolicy

!

class-map inspection\_default

match default-inspection-traffic

!

!

policy-map type inspect dns migrated\_dns\_map\_1

parameters

message-length maximum client auto

message-length maximum 512

no tcp-inspection

policy-map global\_policy

class inspection\_default

inspect dns migrated\_dns\_map\_1

inspect ftp

inspect h323 h225

inspect h323 ras

inspect ip-options

inspect netbios

inspect rsh

inspect rtsp

inspect skinny

inspect esmtp

inspect sqlnet

inspect sunrpc

inspect tftp

inspect sip

inspect xdmcp

policy-map type inspect dns migrated\_dns\_map\_2

parameters

message-length maximum client auto

message-length maximum 512

no tcp-inspection

!

service-policy global\_policy global

prompt hostname context

no call-home reporting anonymous

call-home

profile CiscoTAC-1

no active

: end

1. Μη εναλλαγή σαν κόμβος που μεταδίδει τα καρέ σε όλους. Από την άλλη πλευρά, τα δίκτυα μεταγωγής έχουν πίνακες CAM που περιέχουν διευθύνσεις MAC, θύρες μεταγωγής και πληροφορίες VLAN και επιπλέον ελέγχουν τον πίνακα cache ARP στον κεντρικό υπολογιστή πριν από την αποστολή. [↑](#footnote-ref-1)
2. Παρά την παραβίαση ασφαλείας, τα δεδομένα δικτύου πιθανότατα έχουν από την προοπτική του επιπέδου εφαρμογής (τη δική τους) και του επιπέδου παρουσίασης (το δικό τους) κρυπτογράφηση πολλαπλών επιπέδων στις μέρες μας. [↑](#footnote-ref-2)
3. Πρέπει να σχεδιαστεί ένα σωστό δίκτυο και να υποστηρίζει (από το σχεδιασμό και από προεπιλογή) και τις δύο έννοιες «προληπτικές», «αντιδραστικές». [↑](#footnote-ref-3)
4. Χρησιμοποιείται ευρέως ως βιομηχανικό πρότυπο από το γραφείο στο σπίτι, τις μικρές επιχειρήσεις έως τις μεγάλες επιχειρήσεις και οργανισμούς όπως οι πάροχοι υπηρεσιών Διαδικτύου (ISP). Διασκεδαστικό γεγονός για τον ISP μια χώρα σε φυσικό επίπεδο (υπόστρωμα/underlay) δεν είναι λογικό (επικάλυψη/overlay) είναι το LAN του, ότι επειδή τα (DM)VPN μπορούν επίσης να δημιουργήσουν λογικό LAN. [↑](#footnote-ref-4)
5. Επίπεδο εφαρμογής που σημαίνει τη συνεδρία, την παρουσίαση, την εφαρμογή ως αναφορά OSI ή ως Εφαρμογή συγχωνευμένη τρία προς ένα στο μοντέλο TCP/IP. Αυτά διατηρούνται στην προσωρινή μνήμη σε πρωτόκολλα TCP suit. [↑](#footnote-ref-5)
6. Το φίλτρο οθόνης καταγράφει όλα τα δεδομένα ζωντανά και φιλτράρετε εν κινήσει πακέτα που δεν θέλετε να προβάλλονται προσωρινά (δεν αφήνετε κανένα πακέτο), το χρησιμοποιείτε όταν δεν ξέρετε τι ψάχνετε.

   Το φίλτρο λήψης περιορίζει τη συμπεριφορά του μεγέθους των δεδομένων με τον τρόπο που μειώνετε το μέγεθος του αρχείου των δεδομένων που συλλέγονται, αλλά πρέπει να γνωρίζετε ακριβώς τι ψάχνετε και ότι υπάρχουν διαφορετικά στη σύνταξη από αυτά στη λειτουργία προβολής. [↑](#footnote-ref-6)
7. Υποστηρίζει λειτουργία παρακολούθησης ραδιοσυχνοτήτων που καταγράφει όλη τη δραστηριότητα Wi-Fi. [↑](#footnote-ref-7)
8. π.χ., μπορεί ακόμη και να αποκρυπτογραφήσει τη χειραψία wi-fi, εάν έχετε τα πακέτα αποθηκευμένα μόνο από το σημείο της χειραψίας 4 κατευθύνσεων και στη συνέχεια, στο μέλλον παρέχετε το κλειδί για την αποκρυπτογράφηση της κίνησης wi-fi, χωρίς χειραψία ακόμη και με το κλειδί αριθ. Τα δεδομένα μπορούν να αποκρυπτογραφηθούν λόγω της φύσης του μηχανισμού κρυπτογράφησης [14] [15] [↑](#footnote-ref-8)
9. δεν υπάρχει υποστήριξη αποκρυπτογράφησης wi-fi [↑](#footnote-ref-9)
10. Ένα σωστό δίκτυο αποτελείται από 3 κύρια επίπεδα/επίπεδα σύμφωνα με το CISCO Front-mid-backhaul (->) Δίκτυο πρόσβασης -> Συνάθροιση/Διανομή -> Mobile/fixed et al Core Layer σε ένα κέντρο δεδομένων [16] [17] [18]. [↑](#footnote-ref-10)
11. Ένα Δίκτυο είναι ένα γράφημα αλλά λειτουργεί σαν δέντρο χωρίς βρόχους/κύκλους ενεργούς ταυτόχρονα. Οι σύνδεσμοι για βρόχους συνήθως παραμένουν ανενεργοί μέχρι να συμβεί κάτι όπως η μη αυτόματη παράκαμψη, ο εντοπισμός αίσθησης αποτυχίας σύνδεσης ή η ενσωμάτωση νέας εγκατάστασης συσκευής δικτύου για την κυκλοφορία που μετακινείται αργά σε αυτές τις νέες περιοχές. [↑](#footnote-ref-11)
12. Συμπεριφορά κοινής λογικής για την επίλυση προβλημάτων. [↑](#footnote-ref-12)