Διαχείριση Δικτύων Ι

Επιμέλεια: Δημήτρης Μπότος

ARP

- Το ακρωνύμιο ARP σημαίνει Address Resolution Protocol (Πρωτόκολλο Ανάλυσης Διεύθυνσης), το οποίο είναι ένα από τα πιο σημαντικά πρωτόκολλα του επιπέδου δικτύου.
- Σημείωση: Το ARP βρίσκει τη διεύθυνση υλικού, γνωστή και ως διεύθυνση MAC, ενός κεντρικού υπολογιστή από τη γνωστή διεύθυνση IP του.

ARP II

- Τα περισσότερα από τα προγράμματα/εφαρμογές υπολογιστών χρησιμοποιούν λογική διεύθυνση (διεύθυνση IP) για την αποστολή/λήψη μηνυμάτων, αλλά η πραγματική επικοινωνία γίνεται μέσω της φυσικής διεύθυνσης (διεύθυνση MAC).
- Πρέπει λοιπόν να βρούμε τη διεύθυνση MAC προορισμού που βοηθά στην επικοινωνία με άλλες συσκευές. Αυτό είναι όπου το ARP εμφανίζεται στην εικόνα, η λειτουργικότητά του είναι να μεταφράζει τη διεύθυνση IP σε φυσικές διευθύνσεις.

ARP III

- Φανταστείτε μια συσκευή που θέλει να επικοινωνήσει με τον άλλον μέσω Διαδικτύου. Τι κάνει το ARP; Εκπέμπει ένα πακέτο σε όλες τις συσκευές του δικτύου πηγής.
- Οι συσκευές του δικτύου μεταφέρουν το πακέτο στο επίπεδο δικτύου όπου το αναγνωριστικό δικτύου του πακέτου επικυρώνεται με την IP του προορισμού και αν είναι ίσο, τότε αποκρίνεται στην πηγή με τη διεύθυνση MAC του προορισμού.

ARP IV

- ARP Cache: Μετά την επίλυση της διεύθυνσης MAC, το ARP τη στέλνει στην πηγή όπου είναι αποθηκευμένη σε έναν πίνακα για μελλοντική αναφορά. Οι επόμενες επικοινωνίες μπορούν να χρησιμοποιήσουν τη διεύθυνση MAC από τον πίνακα.
- ARP Cache Timeout: Υποδεικνύει το χρόνο για τον οποίο μπορεί να παραμείνει η διεύθυνση MAC στη μνήμη cache ARP.

ARP V

- Αίτημα ARP: Αυτό δεν είναι τίποτα άλλο από τη μετάδοση ενός πακέτου μέσω του δικτύου για να επικυρωθεί εάν συναντήσαμε τη διεύθυνση MAC προορισμού ή όχι. Συμβαίνει όταν δεν μπορεί η συσκευή να εντοπίσει τα απαραίτητα δεδομένα απο τον πίνακα της ARP cache.
- Απόκριση/απάντηση ARP: Είναι η απόκριση διεύθυνσης MAC που λαμβάνει η πηγή από τον προορισμό που βοηθά στην περαιτέρω επικοινωνία των δεδομένων.

ARP VI

- Χρησιμοποιούμε την εντολή ARP μέσω cmd. Δοκιμάζουμε το arp -a. Με αυτό τον τρόπο παίρνουμε τον πίνακα της ARP cache.
- Χρησιμοποιούμε την εντολή arp -d μπορούμε να σβήσουμε την arp cache. Αυτό είναι χρήσιμο όταν έχει διαφθαρεί και θέλουμε να την ξαναδημιουργήσουμε.
- Για να σβήσουμε μια συγκεκριμένη ip address γράφουμε την εντολή: arp -d <ip-address>

Πρωτόκολλο SNMP

- Με την τρομερή αύξηση των συστημάτων που είναι συνδεδεμένα στο Internet και την ανάλογη αύξηση του αριθμού των υποδικτύων δημιουργήθηκε η ανάγκη της ανάπτυξης ενός αποδοτικού λογισμικού με δυνατότητες διαχείρισης.
- Το πρωτόκολλο SNMP (Simple Network Management Protocol - 1988) αποτελεί επέκταση ενός άλλου παλαιότερου πρωτοκόλλου διαχείρισης δικτύου ονομαζόμενου SGMP (Simple Gateway Monitoring Protocol - 1987), το οποίο είχε σχεδιασθεί για τον έλεγχο των πυλών.
- Το SNMP έγινε γρήγορα ευρέως διαθέσιμο σε μηχανήματα διαφόρων κατασκευαστών και υπερίσχυσε στο Internet κάνοντας το SNMP την πρώτη επιλογή σε πρωτόκολλα διαχείρισης.

Πρωτόκολλο SNMP (II)

- Έτσι τον Αύγουστο του 1988 παρουσιάστηκαν οι προδιαγραφές του και δεν άργησε να καθιερωθεί ως το κυρίαρχο πρωτόκολλο διαχείρισης δικτύων. Όπως φαίνεται και από το όνομα του (Simple Network Management Protocol) πρόκειται για ένα απλό πρωτόκολλο διαχείρισης δικτύων, το οποίο χρησιμοποιείται για τη διαχείριση μικρών αλλά και μεγαλύτερου μεγέθους δικτύων, σχεδιασμένο για το επίπεδο εφαρμογής.
- Χρησιμοποιεί UDP (User Datagram Protocol) πακέτα για την ανταλλαγή πληροφοριών μεταξύ των συσκευών που διαχειρίζεται. Οι πληροφορίες αυτές αναφέρονται σε διάφορα στοιχεία των συσκευών, όπως: κατάσταση στοιχείων συσκευής, υπερφόρτωση συσκευής, σφάλματα κ.α.

Πρωτόκολλο SNMP (III)

- Σε γενικές γραμμές μπορούμε να πούμε ότι ορίζει μια περιορισμένη και εύκολα πραγματοποιήσιμη βάση δεδομένων (MIB), βαθμωτών μεταβλητών και διδιάστατων πινάκων, ενώ ορίζει και ένα πρωτόκολλο ώστε να επιτρέπει στο διαχειριστή να καθορίζει την τιμή των μεταβλητών της MIB και σε ένα πράκτορα να εκδίδει αυτόνομα ειδοποιήσεις που λέγονται παγίδες (traps).
- Η απλότητα που το διακρίνει είναι και ο λόγος για τον οποίο το συγκεκριμένο πρωτόκολλο έχει επικρατήσει, καταναλώνοντας μικρή υπολογιστική ισχύ και δικτυακούς πόρους. Το SNMP καταφέρνει και συγκεντρώνει τις πληροφορίες που χρειάζεται με ένα μικρό αριθμό εντολών και αυτό ισχύει για όλες τις συσκευές του δικτύου.
- Πάντως με τη μεγάλη δημοσιότητα του SNMP, άρχισαν να φαίνονται και τα μειονεκτήματα του τα οποία είχαν να κάνουν κυρίως με θέματα ασφάλειας. Έτσι το 1993 παρουσιάστηκε η δεύτερη έκδοση (SNMPv2), η οποία ήταν σαφώς βελτιωμένη σε σχέση με την πρώτη έκδοση και αργότερα η τρίτη έκδοση (SNMPv3).

Σταθμός διαχείρισης δικτύου (NMS)

- Πρόκειται για τον κεντρικό σταθμό από τον οποίο γίνεται και η κυρίως διαχείριση. Μπορεί να είναι ένα μεμονωμένο σύστημα, αλλά μπορούν να υπάρχουν και περισσότερα από ένα τέτοια συστήματα (κατανεμημένο σύστημα) για τον καταμερισμό των εργασιών σε ένα μεγάλο δίκτυο ή για εφεδρικούς λόγους.
- Στις παραπάνω περιπτώσεις, το διαλογικό περιβάλλον που παρουσιάζεται στο χρήστη του συνολικού συστήματος διαχείρισης, είναι γνωστό ως κονσόλα. Τις θέσεις αυτών των σταθμών κατέχουν, συνήθως, μεγάλοι σε δυνατότητες σταθμοί εργασίας, με μεγάλες οθόνες και αρκετή χωρητικότητα σε μνήμη.

Σταθμός διαχείρισης δικτύου (NMS) (II)

- Ο σταθμός διαχείρισης πρέπει κατ' ελάχιστον να αποτελείται από:

- Ένα σύνολο από εφαρμογές διαχείρισης για την ανάλυση δεδομένων και ανίχνευση σφαλμάτων/βλαβών, αφού τα ακατέργαστα δεδομένα δεν προσφέρουν καμιά ουσιαστική πληροφορία στο διαχειριστή για την κατάσταση και τη λειτουργικότητα του συστήματος.

- Ένα διαλογικό (συνήθως γραφικό) περιβάλλον για να επιβλέπει την κατάσταση του συστήματος αλλά και μεμονωμένων συσκευών, να μεταβάλλει τις παραμέτρους της κάθε συσκευής και να διαχειρίζεται καταστάσεις σφαλμάτων.

- Τη δυνατότητα εφαρμογής των απαιτήσεων του διαχειριστή σε πραγματική παρακολούθηση και έλεγχο των απομακρυσμένων στοιχείων του δικτύου.

- Μία βάση δεδομένων που θα είναι απόρροια όλων των MIBs των διαφόρων χαρακτηριστικών παραμέτρων των στοιχείων του δικτύου.

- Κύρια δουλειά του κεντρικού σταθμού είναι να συλλέγει όλες τις πληροφορίες που έχουν συλλεχθεί από τις υπόλοιπες συσκευές του δικτύου και να τις παρουσιάζει στην κεντρική κονσόλα.

Διαχειριζόμενοι Πράκτορες (agents)

- Μ’ αυτό τον όρο μπορούν να χαρακτηριστούν όλες οι συσκευές οι οποίες είναι συνδεδεμένες στο δίκτυο όπως π.χ. υπολογιστές, εκτυπωτές, επαναλήπτες (hub), δρομολογητές (router) κλπ.
- Αυτές οι συσκευές διαχειρίζονται από το σταθμό διαχείρισης δικτύου. Οι πράκτορες είναι εφοδιασμένοι με κατάλληλο λογισμικό.
- Σκοπός του κάθε πράκτορα είναι να αποκρίνεται σε διάφορες αιτήσεις του σταθμού διαχείρισης, ενώ μπορεί να ενημερώνει ασύγχρονα το σταθμό διαχείρισης για διάφορα γεγονότα.

Πρωτόκολλο SNMP (IV)

- Το πρωτόκολλο αυτό στην πρώτη του έκδοση περιλαμβάνει τις εξής δυνατότητες:

- GET: Με αυτή την εντολή ο κεντρικός σταθμός μπορεί να ανακτήσει μια τιμή ενός αντικειμένου, από έναν πράκτορα. Έτσι ανακτάται η τιμή των διάφορων μεταβλητών, οι οποίες περιγράφουν την κατάσταση της συγκεκριμένης συσκευής.

- SET: Ο κεντρικός σταθμός με αυτή την εντολή θέτει την τιμή σε μια μεταβλητή και έτσι καθορίζει μια χαρακτηριστική τιμή μιας διαχειριζόμενης συσκευής.

- TRAP: Αυτή η εντολή χρησιμοποιείται μόνο από τον πράκτορα και ενημερώνει το σταθμό διαχείρισης ασύγχρονα για την πραγματοποίηση ενός γεγονότος.

Πρωτόκολλο SNMP (V)

- Το SNMP είναι σχεδιασμένο σαν πρωτόκολλο επιπέδου εφαρμογής ως μέρος της TCP/IP στοίβας πρωτοκόλλων. Λειτουργεί πάνω από το πρωτόκολλο UDP -User Datagram Protocol.
- Για ένα μεμονωμένο σταθμό διαχείρισης, η διαδικασία διαχειριστή ελέγχει την πρόσβαση στην κεντρική MIB στο σταθμό διαχείρισης και παρέχει ένα φιλικό περιβάλλον διαχείρισης.
- Η διαδικασία διαχειριστή πετυχαίνει τη διαχείριση του δικτύου χρησιμοποιώντας το SNMP, που υλοποιείται πάνω από το UDP, IP και τα σχετικά πρωτόκολλα δικτύου (για παράδειγμα Ethernet, FDDI, X25 κλπ).
- Κάθε πράκτορας πρέπει επίσης να υλοποιήσει το SNMP, UDP, και IP. Επιπλέον, η διαδικασία πράκτορα μεταφράζει τα SNMP μηνύματα και ελέγχει την MIB του πράκτορα.

Πρωτόκολλο SNMP (VI)

- Από το σταθμό διαχείρισης εκδίδονται τρεις τύποι μηνυμάτων από τις εφαρμογές διαχείρισης: GetRequest, GetNextRequest και SetRequest. Οι πρώτες δύο είναι παραλλαγές της λειτουργίας Get.
- Για όλα τα μηνύματα στέλνεται από τον πράκτορα επιβεβαίωση λήψης με τη μορφή μηνύματος GetResponse το οποίο στέλνεται στην εφαρμογή διαχείρισης.
- Επίσης ένας πράκτορας μπορεί να εκδώσει ένα μήνυμα παγίδα σε απόκριση κάποιου γεγονότος το οποίο επηρεάζει την MIB και τους διαχειριζόμενους πόρους.
- Επειδή το SNMP βασίζεται στο UDP το οποίο είναι χωρίς σύνδεση (connectionless) πρωτόκολλο και το SNMP είναι πρωτόκολλο χωρίς σύνδεση δηλαδή καμία τρέχουσα σύνδεση ανάμεσα στο σταθμό διαχείρισης και τους πράκτορες του δεν εγκαθίσταται. Σε αντίθεση κάθε ανταλλαγή είναι και μια μεμονωμένη ενέργεια ανάμεσα στο σταθμό και τους πράκτορες του.

Πρωτόκολλο SNMP (VII)

- Εάν ένας σταθμός διαχείρισης είναι υπεύθυνος για ένα μεγάλο αριθμό πρακτόρων και αν κάθε πράκτορας έχει πολλά αντικείμενα τότε δεν συμφέρει στο σταθμό διαχείρισης να ζητά περιοδικά αναφορές κατ' απαίτηση από τους πράκτορες. Σε αντίθεση το SNMP και η συσχετιζόμενη MIB είναι σχεδιασμένα έτσι ώστε να χρησιμοποιείται η τεχνική αναφορές κατ' απαίτηση εξαιτίας παγίδων.
- Η τεχνική περιγράφεται ως εξής: Σε κάποιο αρχικό χρόνο και σε τακτά διαστήματα (πχ. Μια φορά την ημέρα) ο σταθμός διαχείρισης μπορεί να ζητήσει από τους πράκτορες του μερικές σημαντικές πληροφορίες (πχ. χαρακτηριστικά διασύνδεσης) και ίσως κάποια στατιστικά στοιχεία (πχ. μέσος όρος πακέτων που στέλνονται και λαμβάνονται από κάθε κόμβο για δεδομένη χρονική περίοδο). Μετά από αυτήν την απαίτηση ο σταθμός διαχείρισης σιωπά και ο κάθε πράκτορας είναι υπεύθυνος να στείλει κάποια αναφορά όταν συμβεί κάποιο μη συνηθισμένο γεγονός (πχ. επανεκκίνηση πράκτορα, μια σύνδεση δεν απαντά κλπ). Αυτά τα γεγονότα στα SNMP μηνύματα ονομάζονται παγίδες.
- Όταν συμβεί κάποιο γεγονός τότε ο σταθμός διαχείρισης εκτελεί κάποιες ενέργειες, ζητώντας αναφορές κατ' απαίτηση από τον πράκτορα που έχει αναφέρει το γεγονός καθώς και από τους γειτονικούς του για να εντοπίσει το πρόβλημα και να αντλήσει χρήσιμες πληροφορίες.
- Οι αναφορές κατ' απαίτηση εξαιτίας παγίδων μπορούν να βοηθήσουν στη μείωση της κυκλοφορίας διαχειριστικών πληροφοριών στο δίκτυο και να εξοικονομήσουν χρόνο επεξεργασίας στους πράκτορες.

Πρωτόκολλο SNMP (VIII)

- Η χρήση του SNMP απαιτεί ότι όλοι οι πράκτορες υποστηρίζουν κοινό πρωτόκολλο (UDP, IP). Αυτό περιορίζει την απευθείας διαχείριση συσκευών όπως είναι οι γέφυρες, κλπ. που δεν υποστηρίζουν κανένα τμήμα του TCP/IP. Επίσης μπορεί να υπάρχουν αρκετά συστήματα που δεν υποστηρίζουν TCP/IP και για τα οποία δεν κρίνεται σκόπιμο να επιβαρυνθούν με το SNMP, και την MIB.
- Στη περίπτωση στην οποία έχουμε τέτοιες συσκευές, χρησιμοποιούμε εκτός των παραπάνω απλών πρακτόρων και τους πιο σύνθετους που τους χαρακτηρίσαμε ως ενδιάμεσους ή μεσολαβητές. Οι πράκτορες αυτοί έχουν τα εξής πλεονεκτήματα:

- Διαχειρίζονται διάφορες συσκευές χρησιμοποιώντας εικονικά οποιοδήποτε πρωτόκολλο. Οι ενδιάμεσοι πράκτορες επικοινωνούν με τον απομακρυσμένο σταθμό εργασίας. Σ’ αυτή την περίπτωση οι ενδιάμεσοι πράκτορες έχουν σαν σκοπό να μετατρέψουν το μήνυμα το οποίο μεταφέρεται σε εκείνο το πρωτόκολλο το οποίο καταλαβαίνουν οι υπό διαχείριση συσκευές.

- Ο ενδιάμεσος πράκτορας μπορεί να δώσει τη δυνατότητα ώστε το σύστημα να έχει πρόσβαση σε περισσότερες από μια συσκευές. Έτσι ο κεντρικός σταθμός μπορεί να επικοινωνήσει με έναν πράκτορα για να διαχειριστεί μέσω αυτού ένα σύνολο από συσκευές που ελέγχονται από τον παραπάνω πράκτορα. Έτσι στην περίπτωση που ο πράκτορας αυτός βρίσκεται σε διαφορετικό υποδίκτυο από τον κεντρικό σταθμό διαχείρισης μπορούμε να αναγνωρίσουμε τα πλεονεκτήματα που παρέχει μια τέτοια υποδομή. Ο ενδιάμεσος πράκτορας θα αναλάβει τη χαμηλού επιπέδου λειτουργία που έχει να κάνει με τη συλλογή δεδομένων από τις συσκευές τις οποίες αυτός μπορεί να διαχειριστεί. Έτσι μεταξύ των διαφόρων πρακτόρων των απομακρυσμένων υποδικτύων και του σταθμού διαχείρισης πραγματοποιείται η ελάχιστη δυνατή κυκλοφορία δεδομένων, ενώ ο κεντρικός σταθμός κατά κάποιο τρόπο αποφεύγει την άμεση επικοινωνία με όλα τα στοιχεία του δικτύου.

- Αυτή η δομή του δικτύου είναι πολύ διαδεδομένη γιατί παρέχει μια πιο γρήγορη απάντηση σε αποτυχίες του δικτύου ή απρόσμενα γεγονότα, αλλά πρέπει να αναφερθεί ότι γενικά είναι πιο πολύπλοκη στην ανάπτυξη και διατήρηση του συστήματος του δικτύου.