ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΨΗΦΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΥΠΗΡΕΣΙΕΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ ΜΕΣΩ ΠΟΛΙΤΙΚΩΝ
POLICY-BASED NETWORK MANAGEMENT

Σοφράς Ν. Ιωάννης
ΑΜ: ΜΕ1563

ΕΠΙΒΛΕΠΟΥΣΑ: Δρ. Αρίστη Γαλάνη

ΑΘΗΝΑ, ΦΕΒΡΟΥΑΡΙΟΣ 2018

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΨΗΦΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΥΠΗΡΕΣΙΕΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ ΜΕΣΩ ΠΟΛΙΤΙΚΩΝ
POLICY-BASED NETWORK MANAGEMENT

Σοφράς Ν. Ιωάννης
ΑΜ: ΜΕ1563

ΕΠΙΒΛΕΠΟΥΣΑ: Δρ. Αρίστη Γαλάνη

| --- | --- | --- |
| ΑΡΙΣΤΗ ΓΑΛΑΝΗ | ΑΘΑΝΑΣΙΟΣ ΚΑΝΑΤΑΣ | ΓΕΩΡΓΙΟΣ ΕΥΘΥΜΟΓΛΟΥ |

ΑΘΗΝΑ, ΦΕΒΡΟΥΑΡΙΟΣ 2018

Ευχαριστίες

Με την ολοκλήρωση της συγγραφής της παρούσας διπλωματικής εργασίας θα ήθελα να ευχαριστήσω θερμά την επιβλέπουσα καθηγήτρια κα. Αρίστη Γαλάνη για την ευκαιρία που μου έδωσε να ασχοληθώ με το εν λόγω έργο. Για την εμπιστοσύνη που μου έδειξε να καλύψω στο μέγιστο βαθμό χωρίς περιορισμούς αυτό το τόσο ενδιαφέρον θέμα, καθώς και για τις πολύτιμες οδηγίες, που μου παρείχε κατά την διάρκεια εκπόνησής του.

Επίσης θα ήθελα να ευχαριστήσω τους γονείς μου για την συμπαράστασή τους, και την συνεχή στήριξή τους, κατά τη διάρκεια της φοίτησής μου στο Μεταπτυχιακό Πρόγραμμα Σπουδών του Πανεπιστημίου Πειραιώς.

Σοφράς Ιωάννης
Αθήνα, Φεβρουάριος 2018

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία έχει ως στόχο να μελετήσει και να παρουσιάσει τις πολιτικές διαχείρισης των δικτύων. Ως διαχείριση ενός δικτύου, θεωρούμε την διαδικασία στον τομέα της πληροφορικής που ασχολείται με τη λειτουργία, τη διαχείριση και την παρακολούθηση των δεδομένων. Η διαχείριση βάσει πολιτικών είναι μια τεχνολογία που μπορεί να απλοποιήσει το περίπλοκο καθήκον της διαχείρισης δικτύων και κατανεμημένων συστημάτων. Σύμφωνα με αυτό το παράδειγμα, ένας διαχειριστής μπορεί να διαχειριστεί διαφορετικές πτυχές ενός δικτύου ή ενός κατανεμημένου συστήματος με ευέλικτο και απλοποιημένο τρόπο, αναπτύσσοντας μια σειρά πολιτικών που διέπουν τη συμπεριφορά του. Οι πολιτικές είναι κανόνες ανεξάρτητοι από την τεχνολογία, που αποσκοπούν στην ενίσχυση της κωδικοποίησης των λειτουργιών των διαχειριζόμενων συσκευών, εισάγοντας ερμηνευμένη λογική που μπορεί να αλλάξει δυναμικά χωρίς τροποποίηση της υποκείμενης υλοποίησης.

Η εργασία χωρίζεται σε 3 κεφάλαια. Στην Εισαγωγή, γίνεται μια σύντομη περιγραφή των πολύ βασικών εννοιών, οι οποίες είναι απαραίτητες για την καλύτερη κατανόηση του τρόπου λειτουργίας των διάφορων πολιτικών διαχείρισης. Περιγράφονται βασικές έννοιες όπως το δίκτυο, η Διαχείριση Δικτύου και η διαχείριση δικτύων βάσει πολιτικής (Policy Based Network Management).

Στο πρώτο κεφάλαιο παρουσιάζονται και αναλύονται τα συστατικά μέρη των πολιτικών διαχείριση δικτύων. Αρχικά αναφέρονται οι λόγοι της αναγκαιότητας της εφαρμογής των πολιτικών διαχείρισης στα δίκτυα και στη συνέχεια αναλύονται βασικές έννοιες όπως η σύγκρουση πολιτικών, η λάθος πολιτική και η ανάλυση πολιτικής .

Στο δεύτερο κεφάλαιο παρουσιάζονται τα υπάρχοντα μοντέλα διαχείρισης δικτύων, βάσει πολιτικής όπως το μοντέλο PEP της IETF (Internet Engineering Task Force) , το Ponder2, το KAos. Επίσης παρουσιάζονται τα ζητήματα της ασφάλειας και της ποιότητας των υπηρεσιών(quality of service) των δικτύων που διαχειρίζονται βάσει πολιτικών.

Το τρίτο κεφάλαιο αποτελεί μια περιγραφή μιας μελέτης περίπτωσης της εφαρμογής των δικτύων βάσει πολιτικής, από τους συγγραφείς Hare και άλλων. Η μελέτη περίπτωσης περιγράφει το πρόβλημα της κατανομής του περιορισμένου όγκου δεδομένων σε επιβάτες λεωφορείων και πως αυτό θα μπορούσε να μοιραστεί βάσει των αναγκών και των εφαρμοζόμενων πολιτικών διαχείρισης.

Το τελευταίο κεφάλαιο αποτελεί την σύνοψη και τις μελλοντικές εξελίξεις των πολιτικών διαχείρισης δικτύων.

Abstract

This thesis aims to study and present network management policies. As a network management, we consider the IT process that deals with the operation, management and monitoring of data. Policy-based management is a technology that can simplify the complex task of managing networks and distributed systems. According to this example, an administrator can manage different aspects of a network or distributed system in a flexible and simplified way by developing a set of policies that govern its behavior. Policies are technology-independent rules designed to enhance the encoding of managed device functions by introducing interpreted logic that can dynamically change without modifying the underlying implementation.

The work is divided into 3 chapters. In the Introduction, a brief description of the very basic concepts, which are necessary for a better understanding of how different management policies work, is made. Basic concepts such as Network, Network Management, and Policy Based Network Management are outlined.

The first chapter presents and analyzes the components of political network management. Initially, the reasons for the need to implement management policies in the networks are discussed and then basic concepts such as policy conflict, wrong policy and policy analysis are analyzed.

The second chapter presents existing network management models, based on policies such as the IETF (Internet Engineering Task Force) PEP model, Ponder2, and Kaos. Also presented are the issues of security and quality of service of the networks they manage on the basis of policies.

The third chapter is a description of a case study on the implementation of networks based on policy, by Hare and others. The case study describes the problem of allocating limited data volume to bus passengers and how this could be shared on the basis of needs and applied management policies. The last chapter is the summary and future developments of network management policies.

Περιεχόμενα

Περιεχόμενα Εικόνων

Συντομογραφίες

API (Application Programming Interface): Δι-επαφή Προγραμματισμού Εφαρμογών
CIM (Common Information Model)
CORBA (Common Object Request Broker Architecture)
COPS (Common Open Policy Service)
DMTF (Distributed Task Force): ομάδα εργασίας διανεμημένης διαχείρισης
FTP (File Transfer Protocol): Πρωτόκολλο μεταφοράς αρχείων
HTTP (Hypertext Transfer Protocol): Πρωτόκολλο Μεταφοράς Υπερκειμένου
IAB (Internet Architecture Board): Αρχή Αρχιτεκτονικής Διαδικτύου
IESG Internet Engineering Steering Group
IETF (Internet Engineering Task Force) : Ομάδα εργασίας τεχνολογιών διαδικτύου
ISP (Internet service providers): Πάροχοι υπηρεσιών διαδικτύου
ISECOM: Institute for Security and Open Methodologies
LDAP (Lightweight Directory Access Protocol) : πρωτόκολλο ανοικτού προτύπου
MdO (Multiple domain operation): διαχειριστής πολλαπλών τομέων
NFV Network Functions Virtualization
OSI (Open Systems Interconnection model): μοντέλο αναφοράς Ανοικτής Διασύνδεσης Συστημάτων
OGSA Open Grid Service Architecture
OWL (Ontology Language): Γλώσσα οντολογιών
PBM(Policy Based Management): Διαχείριση βάσει πολιτικής
PDP (Policy Decision Point)
PEP (Policy Enforcement Point):
PCIM (Policy Core Information Model)
RAP (Resource Allocation Protocol)
SLA(Service-level agreement): Συμβόλαιο Παροχής Υπηρεσίας
SNMP: Simple Network Management Protocol
SDN (Software Defined Networking)
TCP: Transfer Control Protocol: Πρωτόκολλο ελέγχου μεταφοράς
Telnet (TELecommunication NETwork): πρωτόκολλο επικοινωνίας υπολογιστών
Qos (Quality Of Service): ποιότητα υπηρεσιών
RSVP : Resource Reservation Protocol
VPN(Virtual Private Networks): Ιδιωτικά Εικονικά δίκτυα
XML (eXtensible Markup Language) : Γλώσσα σήμανσης,
ΣΔΔ : Σύστημα Διαχείρισης Δικτύου

Αφιερωμένη στην οικογένεια μου

Εισαγωγή- Βασικές έννοιες

Σε ένα δίκτυο, οι χρήστες έχουν τη δυνατότητα να εισάγουν δυναμικά νέα προγράμματα μέσα σε κάθε κόμβο, τα οποία θα εκτελούνται για την επεξεργασία των πακέτων και των δεδομένων. Με τη μέθοδο αυτή η διαδικασία εισαγωγής νέων υπηρεσιών στο δίκτυο καθίσταται ραγδαία. Ανάλογη όμως ταχύτητα θα πρέπει να έχουμε και στην εισαγωγή νέων λειτουργιών, απαραίτητων για τη διαχείριση των νέων αυτών υπηρεσιών. Αυτό συνεπάγεται την ανάγκη για την ύπαρξη ενός εξίσου δυναμικού και επεκτάσιμου συστήματος διαχείρισης. Ακόμα, λόγω της ταχείας μεταβολής στη διαμόρφωση των ενεργών κόμβων, ενδείκνυται οι διαδικασίες διαχείρισης να είναι όσο το δυνατόν πιο αυτοματοποιημένες, ώστε να μην απαιτείται η διαρκής παρέμβαση του διαχειριστή.

Για την κάλυψη της ανάγκης αυτής σχεδιάστηκαν τα πρότυπα πλαισίου Διαχείρισης Δικτύου βάσει πολιτικών. Ένα πλαίσιο διαχείρισης δικτύων θα πρέπει να είναι σε θέση να ελέγχει ανά πάσα στιγμή τους κόμβους, αλλά και να εκμεταλλεύεται τα πλεονεκτήματα που προσφέρει μια αρχιτεκτονική για την αποτελεσματική διαχείριση του δικτύου. Πριν μελετηθούν σε βάθος οι διάφορες πολιτικές διαχείρισης δικτύων θα πρέπει να γίνει αναφορά σε ορισμένες σημαντικές έννοιες.

Ορισμός Δικτύου (Network)

Ως **Δίκτυο** (υπολογιστών) ορίζεται ένα τηλεπικοινωνιακό σύστημα από αυτόνομους ή μη αυτόνομους διασυνδεδεμένους υπολογιστές. Οι υπολογιστές θεωρούνται διασυνδεδεμένοι όταν είναι σε θέση να ανταλλάξουν πληροφορίες μεταξύ τους και αυτόνομοι όταν δεν είναι δυνατό κάποιος υπολογιστής να ελέγξει τη λειτουργία (π.χ. εκκίνηση ή τερματισμό) κάποιου άλλου. Η επιστημονική μελέτη των δικτύων υπολογιστών γίνεται από τα υπολογιστικά συστήματα, έναν βασικό κλάδο της πληροφορικής. Το θεμελιώδες ηλεκτρονικό υλικό των τηλεπικοινωνιακών συσκευών μελετάται επίσης από την ηλεκτρονική μηχανική.

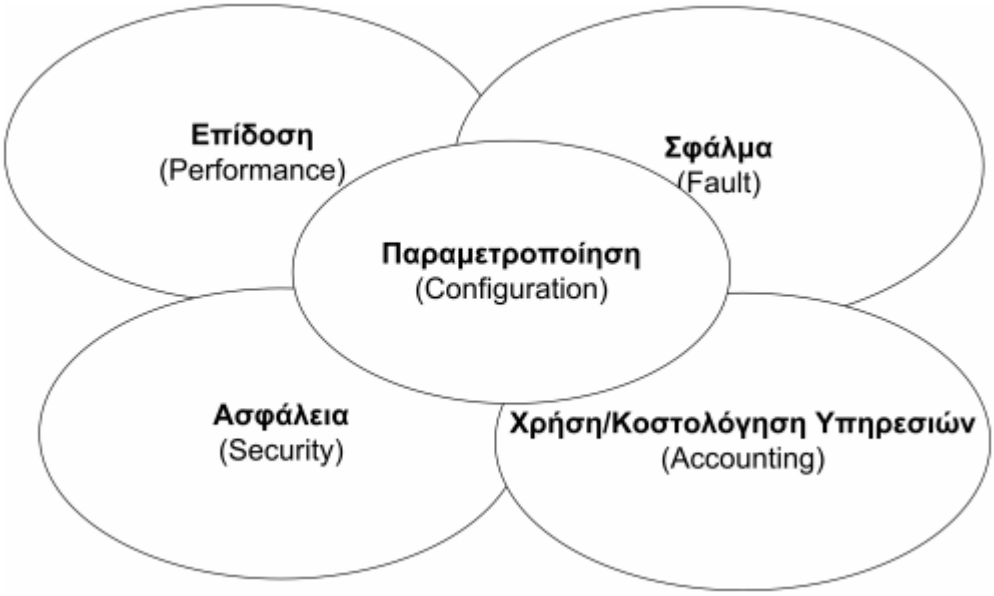
Διαχείριση Δικτύου (Network Management)

Διαχείριση δικτύου (Network management) είναι η διαδικασία διοίκησης και διαχείρισης των δικτύων ενός ή περισσοτέρων οργανισμών. (λειτουργίες που περιλαμβάνονται) Διάφορες υπηρεσίες που παρέχονται από διαχειριστές δικτύων περιλαμβάνουν ανάλυση σφαλμάτων, διαχείριση απόδοσης, διατήρηση της ποιότητας των υπηρεσιών κ.τ.λ. Το λογισμικό που επιτρέπει στους διαχειριστές δικτύου να εκτελούν τις λειτουργίες τους ονομάζεται λογισμικό διαχείρισης δικτύου (Boutaba & Polyrakis, 2001).[1] Το λογισμικό που επιτρέπει στους διαχωριστές να εκτελούν τις εργασίες της διαχείρισης ονομάζεται λογισμικό διαχείρισης δικτύου.

Ως διαχείριση ενός δικτύου υπολογιστών, θεωρούμε την διαδικασία που ασχολείται με τη λειτουργία, τη διαχείριση και την παρακολούθηση των δεδομένων. Η διαχείριση του δικτύου συχνά ορίζεται ως αποτελούμενη από πέντε (5) περιοχές απασχόλησης (ενδιαφέροντος)(εικόνα 1):

- .Διαχείριση σφαλμάτων (Fault Management)
- Διαμόρφωσης (Configuration Management)
- Λογιστική [Διοίκηση] (Accounting [Administration])
- Διαχείριση της απόδοσης (Performance Management)
- Διαχείριση Ασφαλείας (Security Management)

[1] Boutaba R., Polyrakis A(2001), COPS-PR with Meta-Policy Support, IETF Internet Draft, May



Εικόνα 1- Περιοχές διαχείρισης του OSI

Υπάρχει ένας αριθμός βοηθητικών μεθόδων για την υποστήριξη του δικτύου, και της διαχείρισης των συσκευών του δικτύου. Οι μέθοδοι περιλαμβάνουν πρωτόκολλα, προγραμματιστικές γλώσσες, τεχνικές και τεχνολογίες, όπως το SNMP, τη γραμμή εντολών (CLI), το προσαρμοσμένο XML, το CMIP, το Windows Management Instrumentation (WMI), τηνTransaction Language 1 (TL1), το CORBA, το NETCONF και το Java Management Extensions (JMX) (Bellavista et al 2010)[2].

Οι πάροχοι του internet (ISP – Internet service providers) χρησιμοποιούν μια τεχνολογία γνωστή ως επιθεώρηση πακέτων (DPI – Deep Packet Inspection), προκειμένου να ρυθμίσουν τη συμφόρηση του δικτύου και να μειώσουν τα σημεία δυσλειτουργιών στο Διαδίκτυο.

[2] Bellavista P., Corradi A., Stefanelli C.(2010), An Integrated Management Environment for Network Resources and Services. IEEE Journal on Selected Areas in Communications, Vol. 18, No. 5

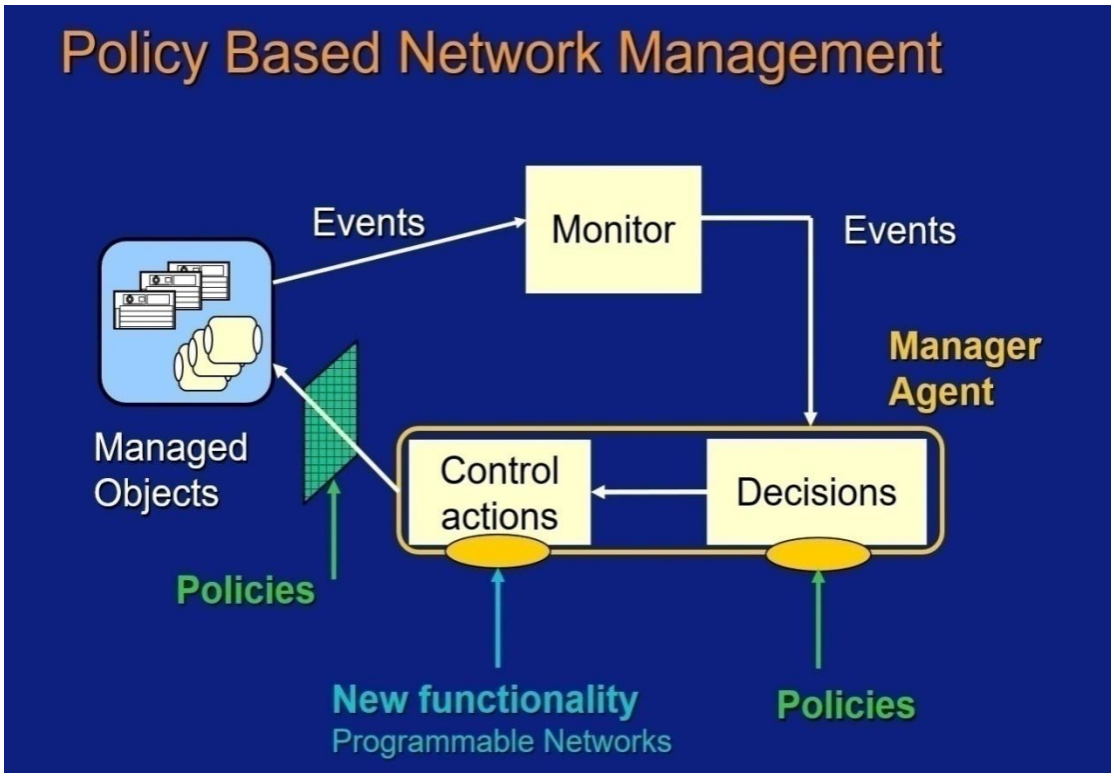
Διαχείριση δικτύου βάσει πολιτικών (Policy Based Network Management)

Η διαχείριση βάσει πολιτικών είναι μια τεχνολογία που μπορεί να απλοποιήσει και να αυτοματοποιήσει το περίπλοκο έργο της σωστής κατανομής των πόρων και της διαχείρισης δικτύων και των κατανεμημένων συστημάτων. Υπό αυτή την έννοια, ένας διαχειριστής μπορεί να διαχειριστεί διαφορετικές λειτουργιές ενός δικτύου ή ενός κατανεμημένου συστήματος με ευέλικτο και απλοποιημένο τρόπο, αναπτύσσοντας μια σειρά πολιτικών που θα εφαρμόζονται κάθε φορά. **(**Bertino, 2009)[3].

Η διαχείριση βάσει πολιτικής (PBM) αποτελεί ένα μοντέλο διαχείρισης που χωρίζει τους κανόνες που διέπουν τη συμπεριφορά ενός συστήματος από τη λειτουργικότητά του (εικόνα 2). Σήμερα είναι παρούσα στον πυρήνα πολλών αρχιτεκτονικών και μοντέλων διαχείρισης, συμπεριλαμβανομένης της διαχείρισης SLA, επιχειρησιακής, αυτόνομης, προσαρμοστικής και αυτόνομης διαχείρισης.

Στην εικόνα 2, παρουσιάζονται οι κυρίες λειτουργίες μιας πολιτικής διαχείρισης δικτύου. Τα διαχειριζόμενα αντικείμενα ελέγχονται μέσα από συγκεκριμένες πολιτικές διαχείρισης και ορίζονται από τον διαχειριστή του δικτύου.

[3] E. Bertino *et al.*, "Analysis of privacy and security policies," *IBM J. Res. Develop.*, vol. 53, no. 2, pp. 3:1–3:18, Mar. 2009. [21] S. Lange *et al.*, "Heuristic approaches to the controller



Εικόνα 2 - Διαχείριση δικτύου βάσει πολιτικής (τυπική σχεδίαση)

Από τα παραπάνω, προκύπτουν τα σημαντικότερα ζητήματα της διαχείρισης των δικτύων βάσει πολιτικής:

- Όταν είναι αναγκαίο σε ένα δίκτυο , δύναται να αλλάξουν ή να προστεθούν κάποιες νέες πολιτικές. Στην περίπτωση αυτή δεν χρειάζεται να γραφτεί κάποιος νέος κώδικας, αρκεί να επαναπροσδιοριστούν οι πολιτικές διαχείρισης.
- Η κατανομή των πόρων του δικτύου γίνεται με αποτελεσματικό τρόπο σύμφωνα με τις δυναμικές πληροφορίες και τις διαφορετικές απαιτήσεις, ανάλογα με τον τύπο των υπηρεσιών.
- Οι διαφορετικοί χρήστες χρησιμοποιούν διαφορετικές πολιτικές και αυτό είναι βολικό για τους χρήστες και ταυτόχρονα το σύστημα καθίσταται πιο επεκτάσιμο και πιο διατηρήσιμο.

ΚΕΦΑΛΑΙΟ 1 - Βασικές Έννοιες Και Συστατικά Μέρη Των Πολιτικών Διαχείρισης Δικτύων

1.1. Η αναγκαιότητα της Εφαρμογής του Policy-Based Network Management

Παρά τις μεγάλες προοπτικές που φαίνεται να έχει η PBNM(Policy-Based Network Management) αλλά και τις πολλές υποσχέσεις για το μέλλον που αφήνουν οι εταιρείες και τα προϊόντα τους, η κατάσταση που επικρατεί σήμερα είναι κάπως διαφορετική από αυτή που όλοι θα ήθελαν. Τα προϊόντα που κυκλοφορούν στην αγορά βρίσκονται σε ένα καλό επίπεδο αλλά δεν μπορούν σε καμία περίπτωση να αναπτύξουν πλήρως (προς το παρόν τουλάχιστον) την ιδέα του Policy-based Network Management. Για να υιοθετήσει τη συγκεκριμένη λύση μια επιχείρηση αλλά και να έχει τα επιθυμητά αποτελέσματα πρέπει να περάσει μέσα από τα παρακάτω στάδια:

1. Προσδιορισμός της κυκλοφορίας του δικτύου που χρειάζεται να κατηγοριοποιηθεί (Indentifying network traffic that needs to be classified): Αυτή είναι και η πιο δύσκολη φάση. Επιτυγχάνεται χρησιμοποιώντας εργαλεία όπως το RMON και το SNMP. Η φάση αυτή περιλαμβάνει την συνήθη ποσότητα του bandwidth που χρησιμοποιείται, τον χρόνο που απαιτείται για την μεταφορά πακέτων, το μέγεθος των πακέτων κ.α. Επίσης είναι σημαντικό να αποτιμηθεί η ελάχιστη καθυστέρηση (latency) κάθε εφαρμογής.

2. Σχεδιασμός και ανάπτυξη πολιτικών (Deploy of policies): Οι λύσεις που κυκλοφορούν σήμερα παρέχουν εργαλεία ανάπτυξης πολιτικών που καλύπτουν τις διάφορες ανάγκες των χρηστών του συστήματος της επιχείρησης, όχι όλες βέβαια στον ίδιο βαθμό.

3. Ανάπτυξη μηχανισμών μέτρησης της επίδρασης των πολιτικών (Deploy mechanisms to measure policiesí effects): Η πρώτης γενιάς απλοί μηχανισμοί που υπάρχουν σήμερα είναι χρήσιμοι, ειδικά όταν κάτι δεν πάει καλά. Τα υπάρχοντα προϊόντα δεν παρέχουν τέτοιες δυνατότητες σε γενικές γραμμές. Ο administrator είναι υποχρεωμένος να χρησιμοποιεί άλλες μεθόδους για να βεβαιωθεί πως μια πολιτική ενεργοποιήθηκε (π.χ. telneting).

4. Προοπτική αυτοσυντονισμού δικτύου (Potential self-tuning Network): Αυτό θα είναι το τελικό στάδιο εξέλιξης ενός προϊόντος PBNM. Η αναφορά των στατιστικών που αναφέρθηκε παραπάνω είναι το πρώτο βήμα για την εκπλήρωση αυτού του στόχου. Από την άλλη πλευρά εκφράζεται ο φόβος πως ένα τόσο αυτοδιοικούμενο σύστημα ενδεχομένως να κρύβει κινδύνους π.χ. απορύθμιση και καταστροφή κρίσιμων για την επιχείρηση διαδικασιών. Η κοινή εκτίμηση πάντως όλων των κατασκευαστών είναι πως κάτι τέτοιο θα αργήσει μερικά χρόνια.

Ο σημαντικότερος στόχος που φιλοδοξεί να εκπληρώσει η διαχείριση δικτύου βασισμένη σε πολιτικές (Policy-based Network Management) είναι να εκφράσει τους επιχειρηματικούς στόχους με τρόπο τέτοιο ώστε να γίνονται κατανοητοί από τις συσκευές του δικτύου και να πετυχαίνονται τα επιθυμητά αποτελέσματα σε τομείς όπως επίπεδο εξυπηρέτησης και ασφάλεια. Το μεγαλύτερο πλεονέκτημα που εξασφαλίζει το Policy-based Network Management (PBNM) είναι πως απαλλάσσει τον διαχειριστή δικτύου από την διαμόρφωση (configuration) κάθε συσκευής του δικτύου ξεχωριστά. Στο παρελθόν οι στόχοι μιας επιχείρησης γράφονταν σε χαρτί και μετατρέπονταν σε εντολές δικτύου από τον administrator. Το να διαχειριστεί κανείς ένα δίκτυο και ειδικά να παρέχει σωστή διαχείριση απαιτεί την διαμόρφωση πολλών και διαφορετικών συσκευών από πολλούς κατασκευαστές. Είναι πολύ δύσκολο να διαμορφώσει κανείς με το χέρι όλες τις συσκευές ενός δικτύου με τέτοιο τρόπο ώστε σε κάθε στιγμή της λειτουργίας του να τηρούνται όλες οι προτεραιότητες, να γίνεται έλεγχος κίνησης και να παρέχεται το επιθυμητό QoS.

Κάτι τέτοιο είναι σχεδόν αδύνατο ακόμη και αν όλες οι συσκευές προέρχονται από τον ίδιο κατασκευαστή. Αυτό απαιτεί απόλυτη γνώση όλων των απαιτήσεων και των περιορισμών των εφαρμογών που θα χρησιμοποιηθούν από το δίκτυο. Ακόμη οι εφαρμογές οι οποίες απαιτούν QoS από το δίκτυο όπως τηλεδιασκέψεις, voice over IP calls κ.α. συχνά ανανεώνονται με αποτέλεσμα πρόσθετη πληροφορία να χρειάζεται να είναι γνωστή κάθε στιγμή. Μια λάθος γραμμένη IP διεύθυνση ή εύρος ζώνης μπορεί να έχει ανεπιθύμητες συνέπειες για την λειτουργία του δικτύου. Το PBNM είναι μια διαδικασία που διοχετεύει περιορισμούς και ενέργειες που πρέπει να εκτελεστούν από το δίκτυο ανά πάσα στιγμή σε έναν policy server. Ο server αυτός ανάλογα με τις αιτήσεις

που δέχεται διαμορφώνει κατάλληλα το δίκτυο ώστε να επιτευχτεί ο επιθυμητός στόχος, παραδείγματος χάριν να παραχθεί το απαιτούμενο QoS για την εκτέλεση της εφαρμογής.

Η Διαχείριση Δικτύων Βάσει Πολιτικών στηρίζεται σε ορισμένες θεμελιώδεις έννοιες, οι οποίες χρησιμοποιούνται σε όλα τα συστήματα πολιτικών, είτε αυτά βασίζονται στις προδιαγραφές της IETF είτε όχι. Σύμφωνα και με τις προδιαγραφές για την ορολογία της διαχείρισης με πολιτικές της IETF, ορίζονται οι παρακάτω βασικές έννοιες.

Πολιτική

Στο χώρο της διαχείρισης η έννοια της πολιτικής μπορεί να καθοριστεί από δύο απόψεις.

• Ένας σαφής στόχος με συγκεκριμένη πορεία και μεθοδολογία ενεργειών, που καθορίζει τις παρούσες και τις μελλοντικές αποφάσεις. Οι πολιτικές υλοποιούνται και εκτελούνται μέσα σε συγκεκριμένα πλαίσια, όπως για παράδειγμα οι πολιτικές που έχουν οριστεί σε μια επιχειρηματική οντότητα.

• Ένα σύνολο κανόνων για την κατανομή, τη διαχείριση και τον έλεγχο της πρόσβασης στους πόρους του δικτύου.

Ο καθορισμός των βημάτων που πρέπει να ακολουθηθούν για την εφαρμογή ενός κανόνα πολιτικής, όταν οι συνθήκες του κανόνα αυτού έχουν ικανοποιηθεί. Οι ενέργειες μιας πολιτικής μπορεί να οδηγήσουν στην εκτέλεση μιας ή περισσότερων λειτουργιών που θα επηρεάσουν ή/και θα διαμορφώσουν την κυκλοφορία και τους πόρους του δικτύου. Οι ενέργειες ενός κανόνα μπορεί να έχουν συγκεκριμένη σειρά.

Η αναπαράσταση αυτή δεν είναι απαραίτητο να είναι πλήρως καθορισμένη, αλλά είναι δυνατό να παρέχεται έμμεσα σε μια υλοποίηση ή σε ένα πρωτόκολλο. Όταν οι συνθήκες που αντιστοιχούν σε ένα κανόνα πολιτικής μπορούν να εκτιμηθούν σε αληθή κατάσταση, τότε ο κανόνας θα πρέπει να εφαρμοστεί, (λαμβάνοντας όμως υπόψη και άλλα θέματα όπως οι προτεραιότητες των κανόνων και οι στρατηγικός απόφασης).

1.2. Βασικές έννοιες

1.2.1. Σύγκρουση Πολιτικών

Η σύγκρουση πολιτικών είναι δυνατό να συμβεί όταν οι ενέργειες δύο κανόνων (που ικανοποιούνται ταυτόχρονα) αντιβαίνουν η μία της άλλης. Σε μια τέτοια περίπτωση η οντότητα που είναι υπεύθυνη για την υλοποίηση της πολιτικής δεν είναι σε θέση να αποφασίσει ποια ενέργεια θα πρέπει να εκτελεστεί. Για το λόγο αυτό υπάρχουν μηχανισμοί για τον εντοπισμό και την αποφυγή ή ακόμα και την επίλυση παρομοίων καταστάσεων. Σε αντιδιαστολή με τη "Σύγκρουση Πολιτικών" έχουμε και το "Λάθος πολιτικής" (Movahedi, 2012)[4].

1.2.2. Λάθος Πολιτικής

Συμβαίνει όταν η προσπάθεια επιβολής των κανόνων μιας πολιτικής αποτυγχάνει, είτε λόγω μιας προσωρινής κατάστασης είτε λόγω ασυμφωνίας μεταξύ των ενεργειών μιας πολιτικής και των δυνατοτήτων της διαχειριζόμενης συσκευής.

Απόφαση Πολιτικής

Η απόφαση μιας πολιτικής έχει δύο απόψεις:

• Μια άποψη είναι αυτή της "διαδικασίας" που έχει να κάνει με την αποτίμηση των συνθηκών ενός κανόνα πολιτικής

• Η άλλη άποψη είναι αυτή του "αποτελέσματος", η οποία αφορά στις ενέργειες για την εφαρμογή, στην περίπτωση που οι συνθήκες ενός κανόνα πολιτικής παίρνουν αληθή τιμή.

[4] Movahedi, Ayari, Langar, Pujolle "A Survey of Autonomic Network Architectures and Evaluation Criteria", in *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 464-490, Second Quarter 2012

Ενδεικτικά παραδείγματα πολιτικών είναι :

- Πολιτικές εξουσιοδότησης (Authorization policies) οι οποίες ορίζουν ποιες ενέργειες μπορεί να πραγματοποιήσει ένα υποκείμενο πάνω σε ένα σύνολο αντικειμένων. Στην ουσία είναι πολιτικές ελέγχου πρόσβασης, που έχουν ως στόχο την προστασία των πόρων και των υπηρεσιών από μη εξουσιοδοτημένη πρόσβαση.
- Πολιτικές Υποχρέωσης (Obligation Policies) οι οποίες καθορίζουν τις λειτουργίες που πρέπει ή δεν πρέπει να εκτελεστούν από τους διαχειριστές ενός συστήματος όταν συμβαίνουν συγκεκριμένα γεγονότα. Ο στόχος τους είναι να δίνουν τη δυνατότητα για αυτοματοποιημένη αντιμετώπιση μελλοντικών καταστάσεων.
- Πολιτικές Φιλτραρίσματος Πληροφοριών (Information Filtering Policies) είναι οι πολιτικές αυτές που χρησιμοποιούνται για να μετατρέψουν τις παραμέτρους εισόδου / εξόδου σε μία λειτουργία.
- Πολιτικές Αντιπροσωπείας (Delegation Policies) αφορούν την αντιπροσώπευση η οποία συχνά χρησιμοποιείται σε συστήματα ελέγχου πρόσβασης για να φροντίσει μία προσωρινή μεταφορά δικαιωμάτων πρόσβασης. Η ικανότητα αυτή, ενός χρήστη να μεταβιβάσει τα δικαιώματα του σε έναν άλλο πρέπει να είναι ελεγχόμενη.
- Πολιτικές Καταστολής (Refrain policies) είναι οι πολιτικές που ορίζουν τις λειτουργίες τις οποίες τα υποκείμενα δεν πρέπει να εκτελούν σε συγκεκριμένα αντικείμενα, ακόμα κι αν και αν στην πραγματικότητα μπορούν να τις εκτελέσουν (Damianou et al, 2010)[5].

[5] Dulay, N., E. Lupu, M. Sloman and N. Damianou (2001). A Policy Deployment Model for the Ponder Language. In Proceedings of the IM 2001: 7th IEEE/IFIP International Symposium on Intergrated Network Management, Seattle, USA, 14-18 May 2001, pp. 529-544.

1.2.3. Εργαλείο Διαχείρισης Πολιτικών

Το εργαλείο αυτό αποτελεί το σημείο επαφής του συστήματος με τον διαχειριστή του δικτύου. Χρησιμοποιώντας την παρεχόμενη δι-επαφή (interface), ο διαχειριστής έχει τη δυνατότητα να καθορίσει νέες πολιτικές για το σύστημα, να τροποποιήσει κάποιες από τις ήδη υπάρχουσες ή ακόμα και απλώς να έχει μια εικόνα όλων των πολιτικών που είναι εγκατεστημένες στο σύστημα την τρέχουσα χρονική στιγμή. Η περιγραφή των πολιτικών μπορεί να γίνει χρησιμοποιώντας μια γλώσσα υψηλότερου επιπέδου, η οποία παρέχει αφηρημένα αντικείμενα στον διαχειριστή. Στην περίπτωση αυτή, το εργαλείο θα πρέπει επίσης να πραγματοποιεί τη μετάφραση των πολιτικών υψηλού επιπέδου σε ένα σύνολο κανόνων που θα μπορούν να γίνουν κατανοητοί από τον Καταναλωτή Πολιτικών.

Η τελική μορφοποίηση των πολιτικών είναι στενά συνδεδεμένη με το μοντέλο και σχήμα πληροφορίας που έχει επιλεχθεί. Πριν γίνει η αποθήκευση μιας νέας πολιτικής, το εργαλείο διαχείρισης πολιτικών θα πρέπει πρώτα να την εξετάσει ως προς τη συντακτική ορθότητα, δηλαδή θα πρέπει να ελέγξει κατά πόσο είναι σύμφωνη με το μοντέλο πληροφορίας πολιτικών.

Επίσης στο επίπεδο αυτό γίνεται και ο καθολικός έλεγχος σύγκρουσης, για να διαπιστωθεί εάν η νέα πολιτική έρχεται σε σύγκρουση με κάποια άλλη που βρίσκεται ήδη στο σύστημα. Για παράδειγμα, αυτό μπορεί να συμβεί εάν έχουμε δύο πολιτικές, οι συνθήκες των οποίων είναι δυνατό να ικανοποιηθούν ταυτόχρονα, ενώ οι αντίστοιχες ενέργειές τους είναι αντιφατικές. Ο συγκεκριμένος έλεγχος συγκρούσεων μπορεί να μην είναι πλήρης, καθώς ενδέχεται να εξετάσει μόνο στατικές συνθήκες.

1.2.4. Βάση Αποθήκευσης Πολιτικών

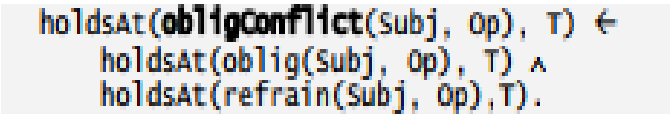
Η βάση αυτή χρησιμοποιείται για την αποθήκευση των πολιτικών, αφού αυτές έχουν οριστεί και επικυρωθεί από το εργαλείο διαχείρισης πολιτικών. Στο τμήμα αυτό της αρχιτεκτονικής συμπεριλαμβάνεται και το πρωτόκολλο το οποίο επιτρέπει την

πρόσβαση στη βάση για γραφή και ανάγνωση των πολιτικών. Το γενικότερο πλαίσιο δεν επιβάλλει την υλοποίηση συγκεκριμένων τεχνολογιών για την κατασκευή της βάσης ή και για το πρωτόκολλο πρόσβασης.

Μια βέλτιστη επιλογή αποτελεί η χρήση ενός directory server για την αποθήκευση των πολιτικών, με την επικοινωνία να γίνεται βάσει του πρωτοκόλλου LDAPv3. Η μορφή με την οποία αποθηκεύονται οι πολιτικές ακολουθεί την προδιαγραφή CIM της DMTF.

1.2.5. Ανάλυση πολιτικής

Σε ένα περιβάλλον όπου χρειάζεται να συνυπάρχουν πολλές πολιτικές, υπάρχει πάντοτε η πιθανότητα ότι ορισμένες πολιτικές θα βρίσκονται σε σύγκρουση είτε λόγω ενός σφάλματος εξειδίκευσης είτε λόγω περιορισμών που σχετίζονται με την εφαρμογή. Επομένως, είναι σημαντικό να παρέχεται ένα μέσο ανίχνευσης των συγκρούσεων στις προδιαγραφές πολιτικής. Οι διάφοροι τύποι συγκρούσεων που μπορούν να συμβούν προκύπτουν όταν καθορίζονται δύο πολιτικές με βάση τα ίδια θέματα, στόχους και ενέργειες, αλλά είναι αντίθετης μορφής (π.χ. υποχρέωση και απόρριψη). Αυτός ο τύπος σύγκρουσης είναι ανεξάρτητος από τον τομέα, δεδομένου ότι ενδέχεται να προκύψουν συγκρούσεις ανεξάρτητα από τον τομέα εφαρμογής για τον οποίο καθορίζονται οι πολιτικές. Άλλοι τύποι συγκρούσεων που εντοπίζονται στη βιβλιογραφία εμπίπτουν στην κατηγορία των συγκρούσεων που σχετίζονται με την εφαρμογή. Αυτές περιλαμβάνουν διενέξεις καθήκοντος, συγκρούσεις συμφερόντων, πολλαπλές διενέξεις διαχειριστών, συγκρούσεις προτεραιοτήτων για πόρους και συγκρούσεις αυτοδιαχείρισης. Λαμβάνοντας υπόψη τους τύπους συγκρούσεων που περιγράφηκαν παραπάνω, είναι δυνατόν να οριστούν κανόνες που μπορούν να χρησιμοποιηθούν για την αναγνώριση συγκρουόμενων καταστάσεων στις προδιαγραφές πολιτικής. Ο κώδικας της υποχρεώσεων Conflict που ορίζεται παρακάτω(εικόνα 3) ανιχνεύει μια σύγκρουση μεταβλητότητας.



Εικόνα 3 - κώδικας υποχρεώσεων Conflict

Σε περίπτωση διενέξεων συγκεκριμένης εφαρμογής, οι κανόνες πρέπει να ορίζονται χρησιμοποιώντας περιορισμούς που περιλαμβάνουν ειδικά δεδομένα για την εφαρμογή εκτός από τις πληροφορίες πολιτικής. Υπάρχουν διάφοροι κανόνες για την ανίχνευση των συγκρούσεων που σχετίζονται με συγκεκριμένες εφαρμογές, όπως οι συγκρούσεις συμφερόντων, οι συγκρούσεις καθηκόντων και οι συγκρούσεις αυτοδιαχείρισης.

1.2.6. Συγκρούσεις πολιτικών

Όπως συμβαίνει με οποιοδήποτε προγραμματιζόμενο σύστημα, μια πολιτική μπορεί να φέρει ορισμένες ασυνέπειες που προκύπτουν από αντιφατικούς κανόνες που διέπουν τη συμπεριφορά της.

Αυτές είναι γνωστές ως συγκρούσεις πολιτικής και προκύπτουν ως αποτέλεσμα σφαλμάτων εξειδίκευσης, παραλείψεων ή αντιφατικών λειτουργιών διαχείρισης και, σε ορισμένες περιπτώσεις, μπορεί να έχουν καταστροφικές επιπτώσεις στη λειτουργία του διαχειριζόμενου συστήματος.

Έχουν επίσης περιγραφεί ως ανάλογες με τα σφάλματα λογισμικού που συμβαίνουν όταν δύο ή περισσότερες πολιτικές ενεργοποιούνται ταυτόχρονα επιβάλλοντας αντιφατικές λειτουργίες διαχείρισης στο σύστημα.

Οι τομείς εφαρμογών που εξετάστηκαν στη βιβλιογραφία περιλαμβάνουν την ποιότητα της υπηρεσίας (QoS –Quality of Service) σε δίκτυα IP, κατανεμημένα συστήματα, ασφάλεια τείχους προστασίας και έλεγχο κλήσεων σε τηλεπικοινωνιακά δίκτυα. Οι συγκρούσεις πολιτικής μπορούν επίσης να ταξινομηθούν σύμφωνα με το χρονοδιάγραμμα κατά το οποίο μπορούν να ανιχνευθούν: οι στατικές συγκρούσεις μπορούν να ανιχνευθούν μέσω ανάλυσης εκτός γραμμής κατά την ώρα των

προδιαγραφών πολιτικής, ενώ οι δυναμικές διενέξεις μπορούν να ανιχνευθούν μόνον όταν εφαρμόζονται πολιτικές, στην τρέχουσα κατάσταση του διαχειριζόμενου συστήματος.

Για παράδειγμα, μπορεί να προκύψουν συγκρούσεις μεταξύ πολιτικών για τη δυναμική κατανομή πόρων και εκείνων που ορίζουν ποσοστώσεις για χρήστες ή κλάσεις υπηρεσιών. Ως εκ τούτου, η αυτοματοποίηση θα πρέπει να αποτελεί βασική πτυχή των μηχανισμών δυναμικής ανάλυσης, ώστε ο επιχειρησιακός αντίκτυπος μιας σύγκρουσης να μπορεί να περιοριστεί στο ελάχιστο.

Ορισμένες δημοφιλείς προσεγγίσεις για την ανίχνευση συγκρούσεων βασίζονται σε: μετα-πολιτικές (κανόνες ανίχνευσης), πολιτικές σχέσεις, χώρους εφαρμογής, και μοντέλα πληροφοριών.

Η λύση είναι το τελευταίο μέρος της ανάλυσης πολιτικής, το οποίο στοχεύει στην αντιμετώπιση ανιχνευόμενων ασυνεπειών, κατά προτίμηση με αυτοματοποιημένο τρόπο, προκειμένου να αποκατασταθεί η συνοχή μεταξύ των πολιτικών. Η διαδικασία επίλυσης των συγκρούσεων μπορεί να περιλαμβάνει την ανάκληση, την καταστολή, την ιεράρχηση ή την τροποποίηση πολιτικών και, σε ορισμένες περιπτώσεις, την επιβολή μιας νέας πολιτικής συνολικά, ώστε να αποκατασταθεί η συνοχή μεταξύ των κανόνων πολιτικής. Η σχετική μεθοδολογία εξαρτάται σε μεγάλο βαθμό από το είδος των πολιτικών που εμπλέκονται και από τον τομέα στον οποίο συμβαίνουν συγκρούσεις. Αν και η ανθρώπινη παρέμβαση είναι αναπόφευκτη σε ορισμένες περιπτώσεις, αρκετές ερευνητικές προσπάθειες επικεντρώθηκαν σε τεχνικές αυτοματοποίησης της διαδικασίας επίλυσης. (Diamanou et al, 2010)[6].

Το χρονικό πλαίσιο στο οποίο μπορούν να ανιχνευθούν συγκρούσεις επηρεάζει τη μεθοδολογία ανάλυσης και τις απαιτήσεις για την αντιμετώπισή τους. Οι στατικές συγκρούσεις τυπικά ανιχνεύονται μέσω ανάλυσης από το διαχειριστή του συστήματος. οι συγκρούσεις αντιπροσωπεύουν ασυνέπειες μεταξύ πολιτικών και συνήθως επιλύονται με

[6] Dulay, N., E. Lupu, M. Sloman and N. Damianou (2001). A Policy Deployment Model for the Ponder Language. In Proceedings of the IM 2001: 7th IEEE/IFIP International Symposium on Intergrated Network Management, Seattle, USA, 14-18 May 2001, pp. 529-544.

την τροποποίηση των πολιτικών. Αντίθετα, οι διενέξεις χρόνου εκτέλεσης πρέπει να ανιχνεύονται από μια διαδικασία που παρακολουθεί την εφαρμογή πολιτικής και ανιχνεύει ασυνεπείς καταστάσεις στην εκτέλεση του συστήματος. Η επίλυση πρέπει να επιτυγχάνεται αυτόματα, για παράδειγμα μέσω της επιβολής κανόνων ανάλυσης. Η έλλειψη αυτοματοποίησης στον χειρισμό των διενέξεων χρόνου εκτέλεσης μπορεί να έχει καταστροφικές συνέπειες για τη σωστή λειτουργία του συστήματος, ειδικά κατά τη διαχείριση της QoS για εφαρμογές ευαίσθητες σε καθυστέρηση. **(**Bertino, 2009)[7].

[7] E. Bertino *et al.*, "Analysis of privacy and security policies," *IBM J. Res. Develop.*, vol. 53, no. 2, pp. 3:1–3:18, Mar. 2009. [21] S. Lange *et al.*, "Heuristic approaches to the controller

ΚΕΦΑΛΑΙΟ 2 - Πολιτικές Και Μοντέλα Διαχείρισης Των Δικτύων

2.1. Επίπεδα αφαίρεσης των πολιτικών διαχείρισης των δικτύων

Σε μία πολιτική διαχείρισης δικτύου υπάρχουν ορισμένα επίπεδα τα οποία διαφέρουν ανάλογα με τις προδιαγραφές της εκάστοτε πολιτικής. Αυτά τα επίπεδα ονομάζονται επίπεδα αφαίρεσης και αντιπροσωπεύουν διαφορετικές μεθόδους διαχείρισης των δικτύων, καθώς και διαφορετικές σχέσεις μεταξύ των πολιτικών στα διαφορετικά επίπεδα. Ανάλογα με τα επίπεδα αφαίρεσης υπάρχουν πολιτικές διαχείρισης υψηλού επιπέδου και χαμηλού επιπέδου.

Επίπεδα λήψης πολιτικών

Οι πολιτικές σε ένα σύστημα διαχείρισης μπορούν να εκπροσωπούνται και να καθορίζονται με διάφορους τρόπους, παρέχοντας επεκτασιμότητα και ευελιξία στα συστήματα διαχείρισης. Τα παρακάτω είναι τα επίπεδα που προτείνουν οι συγγραφείς στο (Astudillo et al, 2010)[8].

1) πολιτική υψηλού επιπέδου: Οι πολιτικές αυτές καθορίζονται από τους υπεύθυνους χάραξης πολιτικής. Αυτός ο τύπος πολιτικών περιλαμβάνει:

• τους επιχειρηματικούς στόχους της εταιρείας ή του οργανισμού.

• Οι SLA που ορίζονται μεταξύ παρόχων, παρόχων και των πελατών τους ή εσωτερικά σε έναν οργανισμό.

[8]Carlos A. Astudillo, Graduate Student Member, IEEE, Adriana M. Gustin, Graduate Student Member, IEEE and Oscar J. Calderón, Member, IEEE(2010) Policy Creation Model for Policy-Based Management in Telecommunications Networks

• Οι ανάγκες των συμμετεχόντων στο δίκτυο, μεταξύ των οποίων: χρήστες / πελάτες, εφαρμογές, υπηρεσίες, πάροχοι και φορείς εκμετάλλευσης δικτύων. Αυτές οι πολιτικές ορίζονται στη φυσική γλώσσα και αντιπροσωπεύουν τους στόχους της συμπεριφοράς του δικτύου και τις επιθυμίες των εμπλεκόμενων μερών. Οι πολιτικές σε αυτό το επίπεδο δεν εμφανίζονται στο σύστημα διαχείρισης και πρέπει να εξειδικευτούν στις πολιτικές μέσου επιπέδου για να τους επιτρέψουν να εισέλθουν.

2) Πολιτική χαμηλού επιπέδου: Αυτές οι πολιτικές ορίζονται για μια συγκεκριμένη συσκευή, με συγκεκριμένη διαμόρφωση και αντιπροσωπεύουν το κατώτατο επίπεδο μιας πολιτικής, επειδή εφαρμόζονται απευθείας στο στοιχείο δικτύου που εμπλέκεται στις πολιτικές. Αυτές οι πολιτικές είναι κατασκευασμένες σε κατανοητή και μοναδική μορφή για κάθε συσκευή και μετατρέπονται σε αυτή τη μορφή μέσω του PDP. Συνήθως σε αυτό το επίπεδο οι πολιτικές δεν πρέπει να καθορίζονται επειδή χάνουν το στόχο της διαχείρισης βάσει πολιτικής η οποία επιδιώκει να παρέχει υψηλού επιπέδου διαχείριση σε μεγάλο αριθμό συσκευών ταυτόχρονα (Astudillo et al, 2010)[9].

[9] Carlos A. Astudillo, Graduate Student Member, IEEE, Adriana M. Gustin, Graduate Student Member, IEEE and Oscar J. Calderón, Member, IEEE(2010) Policy Creation Model for Policy-Based Management in Telecommunications Networks

2.2. Η διαχείριση των δικτύων

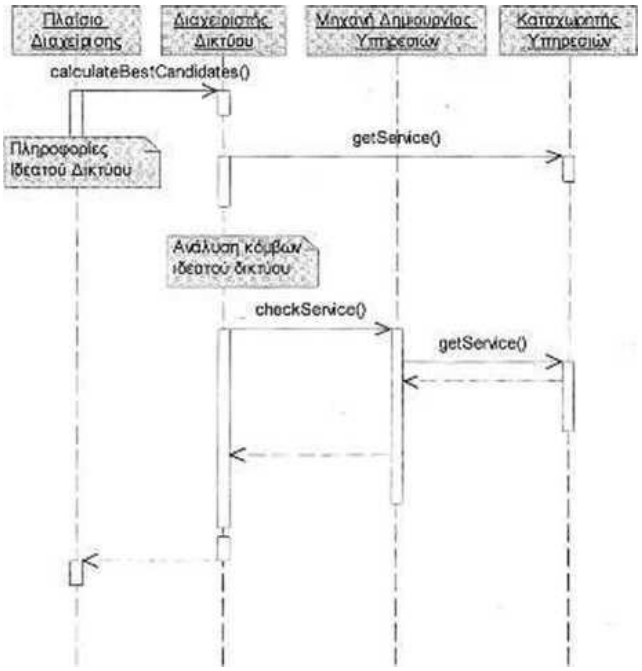
2.2.1. Διαχείριση πολιτικής δικτύου σε Επίπεδο Δικτύου

Ο διαχειριστής δικτύου είναι ο χρήστης ο οποίος διατηρεί μια γενική εποπτεία του δικτύου, σχετική με τις προσφερόμενες υπηρεσίες, ενώ αποτελεί και ένα σημείο εισόδου στην αρχιτεκτονική του πλαισίου παροχής υπηρεσιών. Ως κεντρικό σημείο της δικτυακής αρχιτεκτονικής, παρέχει τις κατάλληλες μεθόδους για τη διαχείριση των δικτυακών περιγραφών μιας υπηρεσίας και για την επεξεργασία τους για την εξαγωγή των απαιτήσεων μιας υπηρεσίας, για τη μετακίνηση κώδικα σε καθορισμένους κόμβους, για την εγκατάσταση και διαμόρφωση στιγμιότυπων μιας υπηρεσίας σε ένα σύνολο κόμβων και για την εύρεση των κόμβων που είναι κατάλληλοι για να φιλοξενήσουν μια υπηρεσία.

Ο Διαχειριστής Δικτύου μπορεί να επεξεργαστεί τη δικτυακή περιγραφή μιας υπηρεσίας και να εξάγει τις απαιτήσεις που περιέχονται σε αυτήν, όσον αφορά στην τοπολογία του δικτύου και την ανάθεση δικτυακών πόρων. Για παράδειγμα ένα XML paper που θα μπορεί να κάνει την μετάφραση των εγγράφων XML που περιέχουν την περιγραφή μιας υπηρεσίας. Είναι το μοναδικό συστατικό της αρχιτεκτονικής στο επίπεδο δικτύου που να έχει αυτή τη λειτουργικότητα και έχει αποκλειστική πρόσβαση στις περιγραφές των υπηρεσιών. Στην περίπτωση που κάποιο άλλο συστατικό χρειαστεί πληροφορίες που περιλαμβάνονται στη δικτυακή περιγραφή μιας υπηρεσίας, θα πρέπει να έρθει σε επαφή με το Διαχειριστή Δικτύου.

Παράλληλα, διατηρεί και σε μια βάση δεδομένων πληροφορίες για τις υπηρεσίες που έχουν εγκατασταθεί στο δίκτυο και για τα στιγμιότυπα των συστατικών που εκτελούνται στους κόμβους. Οι πληροφορίες αυτές είναι διαθέσιμες για τη διαχείριση των υπηρεσιών αυτών. Η απαραίτητη επικοινωνία με τους διαχειριζόμενους κόμβους γίνεται χρησιμοποιώντας την τεχνολογία των Κινητών Διαμεσολαβητών. Ένα

παράδειγμα ενός πλαισίου παροχής υπηρεσιών που εκμεταλλεύεται τα πλεονεκτήματα των διαμεσολαβητών(Romero, 2016)[10].



Εικόνα 4 - Διαχείριση πολιτικής δικτύου σε Επίπεδο Δικτύου
Πηγή: Romero, 2016

Η βασική λειτουργία του διαχειριστή δικτύου είναι η αντιστοίχιση μιας υπηρεσίας στο δίκτυο, δηλαδή ο εντοπισμός των κόμβων στους οποίους θα εγκατασταθεί και ο έλεγχος για το κατά πόσο αυτό είναι δυνατό. Βάσει και της δικτυακής περιγραφής της υπηρεσίας, αυτό μπορεί να γίνει για συστατικά υπηρεσίας που εγκαθίστανται πάνω σε ένα μονοπάτι και συγκεκριμένα μπορούν να καθορίσουν αν θα εγκατασταθούν στην αρχή ή το τέλος του μονοπατιού.

[10] J. Pérez-Romero, O. Sallent, R. Ferrús, R. Agustí, "Knowledge-based 5G Radio Access Network Planning and Optimization", The Thirteenth International Symposium on Wireless Communication Systems (ISWCS-2016), Poznan, Poland, September, 2016.

Σύμφωνα και με το επιχειρηματικό μοντέλο του δικτύου, ένας πάροχος υπηρεσιών μπορεί να εγκαταστήσει μια υπηρεσία σε ένα ιδεατό δίκτυο το οποίο δημιουργεί χρησιμοποιώντας το πλαίσιο διαχείρισης του δικτύου. Κατά τη διάρκεια της διαδικασίας αυτής, το πλαίσιο διαχείρισης επικοινωνεί με το διαχειριστή δικτύου του πλαισίου παροχής υπηρεσιών και του μεταδίδει ένα σύνολο υποψηφίων κόμβων, ώστε να διαθέσει τους απαραίτητους πόρους για την υπηρεσία. Οι πληροφορίες που παρέχονται μέσω μιας δι-επαφής CORBA έχουν τη μορφή δομών με τις ακόλουθες παραμέτρους (Movahedi, 2012)[11] :

• IP διεύθυνση του κάθε κόμβου

• Αναγνωριστικό του περιβάλλοντος εκτέλεσης που αναλογεί στο συγκεκριμένο πάροχο υπηρεσιών και στο οποίο μπορούν να εγκατασταθούν τα συστατικά μιας υπηρεσίας.

• Ταξινόμηση του κόμβου (αν είναι εσωτερικός / εξωτερικός σε ένα μονοπάτι). Ο διαχειριστής δικτύου αποφασίζει βάσει της δικτυακής περιγραφής της υπηρεσίας σε ποιο κόμβο μπορεί να εγκατασταθεί κάθε συστατικό της υπηρεσίας. Στη συνέχεια χρησιμοποιεί την μηχανή δημιουργίας υπηρεσιών του κόμβου αυτού για τον έλεγχο (check service) της υπηρεσίας, βάσει της περιγραφής κόμβου. Η μηχανή δημιουργίας υπηρεσιών μπορεί να απαντήσει αν υπάρχει υλοποίηση της υπηρεσίας για το συγκεκριμένο κόμβο. Αφού εντοπιστούν όλοι οι κόμβοι, ο διαχειριστής δικτύου εισάγει ένα επιπλέον πεδίο στις πληροφορίες του ιδεατού δικτύου, που υποδεικνύει σε ποιο κόμβο θα γίνει εγκατάσταση συστατικών, ώστε να μπορέσουν να ανατεθούν οι απαιτούμενοι υπολογιστικοί πόροι και επιστρέφει την πληροφορία αυτή στο πλαίσιο διαχείρισης, το οποίο και είναι αρμόδιο για τη διαχείριση πόρων (Movahedi, 2012)[12].

[11] Movahedi, Ayari, Langar, Pujolle "A Survey of Autonomic Network Architectures and Evaluation Criteria", in *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 464-490, Second Quarter 2012

[12] Movahedi, Ayari, Langar, Pujolle "A Survey of Autonomic Network Architectures and Evaluation Criteria", in *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 464-490, Second Quarter 2012

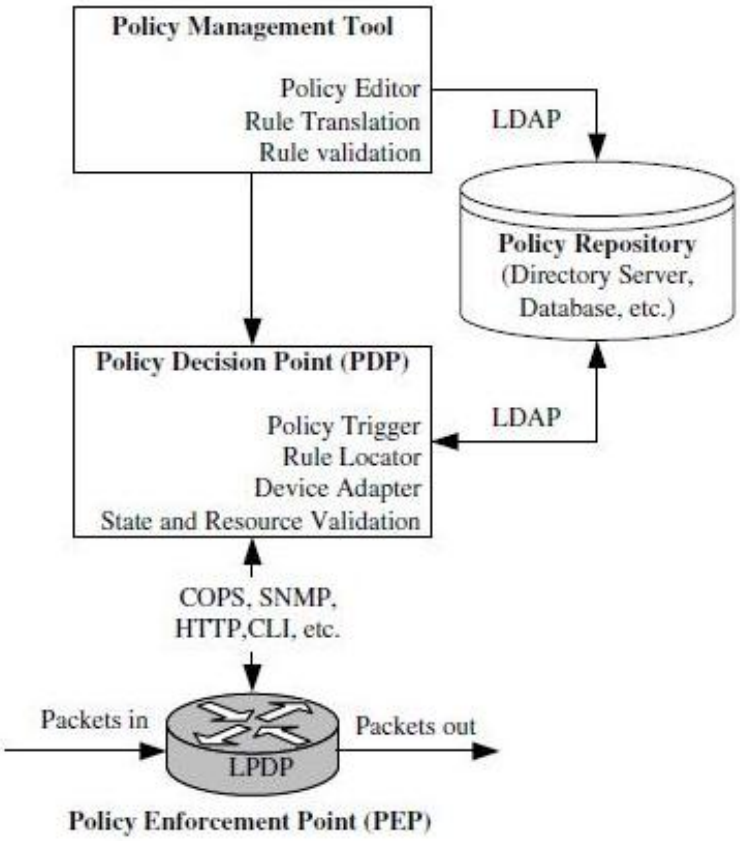
Policy Enforcement Point (PEP)

Οι επιχειρήσεις κατά κύριο λόγο, καθορίζουν τους στόχους για τη συμπεριφορά ενός δικτύου με βάσει ανθρώπινα κριτήρια. Οι υλοποιήσεις δικτύου παρέχουν μια ποικιλία εφαρμογών ελέγχου για την επεξεργασία κατά προτεραιότητας της κυκλοφορίας, τη διαχείρισης του εύρους ζώνης, της ασφάλειας και του ελέγχου της συμπεριφοράς του δικτύου. Η σύνδεση μεταξύ των επιχειρηματικών στόχων υψηλού επιπέδου και των υλοποιήσεων του δικτύου, ορίζεται ως Policy based network και αποτελείται από πολιτικές. Οι πολιτικές αυτές καθορίζονται συνήθως σε ένα κεντρικό repository και έχουν πρόσβαση σε κόμβους που πρέπει να λάβουν πολιτικές αποφάσεις (Policy Decision Point ή PDP) ή να εφαρμόσουν τέτοιες αποφάσεις (Policy Enforcement Point ή PEP) (Chan, 2011)[13].

Ένα τυπικό δίκτυο που βασίζεται στην πολιτική, περιλαμβάνει :

- Μια κονσόλα διαχείρισης δικτύου(εικόνα 5), στην οποία οι πολιτικές εισάγονται, επεξεργάζονται ή καλούνται από μια αποθήκη πολιτικής.
- Ένας εξυπηρετητής, αναφέρεται ως σημείο λήψης πολιτικής (PDP – Policy Decision Point), ο οποίος ανακτά τις πολιτικές από το χώρο αποθήκευσης πολιτικών και ενεργεί για τις πολιτικές για λογαριασμό των PEPs (Policy Enforcement Points). Τα σημεία επιβολής πολιτικής (PEPs), είναι ο router, τα switches και άλλες συσκευές δικτύου που προωθούν τις πολιτικές, χρησιμοποιώντας access control lists, σε αλγόριθμους και ούτω καθεξής.
- Ένα σύνολο πολιτικών (Repository), ένας directory server πολιτικών που βασίζεται στο πρωτόκολλο LDAP (Light weight Directory Access Protocol)

[13] Chan, K., D. Durham, S. Gai, S. Herzog, K. McCloghrie, F. Reichmeyer, J. Seligson, A. Smith and R. Yavatkar (2001), *COPS Usage for Policy Provisioning, RFC 3084*, March 2001.



Εικόνα 5 - πολιτική ενίσχυσης σημείου

Πηγή: Chan, 2011

2.3. IETF

2.3.1. Η Ομάδα εργασίας της πολιτικής IETF

Η IETF (Internet Engineering Task Force) είναι μια μεγάλη, ανοικτή, μη κυβερνητική διεθνής κοινότητα που αποτελείται από σχεδιαστές δικτύων, φορείς εκμετάλλευσης, πωλητές και ερευνητές, προερχόμενοι κυρίως από βιομηχανικές χώρες που ασχολούνται με την εξέλιξη της αρχιτεκτονικής του διαδικτύου και γενικότερα για την ομαλή λειτουργίας του. Η IETF είναι ανοιχτή σε οποιοδήποτε άτομο ενδιαφέρεται να

συμμετάσχει και να συνεισφέρει με τις γνώσεις του. Το πραγματικό τεχνικό έργο της IETF, που περιλαμβάνει την ανάπτυξη προτύπων για το διαδίκτυο, πραγματοποιείται με την συνεργασία ατόμων, χωρισμένα σε ομάδες σε διαφορετικούς τομείς (π.χ. δρομολόγηση, μεταφορά, ασφάλεια κ.λπ.). Μεγάλο μέρος της εργασίας γίνεται μέσω λιστών αλληλογραφίας (Mahon, 2002).[14]

Η IETF διοργανώνει συναντήσεις τρεις φορές το χρόνο. Οι ομάδες εργασίας του IETF ομαδοποιούνται σε περιοχές και διοικούνται από διευθυντές περιοχής (Area Directors). Οι διευθυντές είναι μέλη της ομάδας καθοδήγησης του Internet Engineering (IESG). Η παροχή αρχιτεκτονικής εποπτείας είναι η Αρχή Αρχιτεκτονικής Διαδικτύου (IAB), η οποία είναι αρμόδια να εκδικάσει προσφυγές όταν κάποιος διαμαρτύρεται κατά του IESG. Ο Γενικός Διευθυντής Περιοχής λειτουργεί επίσης ως πρόεδρος του IESG και της IETF και είναι μέλος της IAB (Ortalo, 2001)[15].

Η ομάδα IETF δημιουργήθηκε για τον καθορισμό ενός τυποποιημένου πλαισίου για ένα σύστημα διαχείρισης πολιτικής, και την προδιαγραφή ενός επεκτάσιμου μοντέλου πληροφορίας. Τα βασικά αποτελέσματα της έρευνας της ομάδας αυτής είναι:

• Ο καθορισμός των γενικότερων απαιτήσεων ενός συστήματος διαχείρισης με πολιτικές, καθώς και η περιγραφή αντιπροσωπευτικών σεναρίων λειτουργίας που συνέβαλλαν στη σχεδίαση ενός πλαισίου διαχείρισης δικτύων με πολιτικές.

• Η προδιαγραφή ενός γενικού πλαισίου για τον καθορισμό πολιτικών σε μια διαχειριστική περιοχή του δικτύου και για τον έλεγχο ενός συνόλου σημείων απόφασης και σημείων εφαρμογής. Ως διαχειριστική περιοχή ορίζεται ένα σύνολο συστατικών τα οποία βρίσκονται υπό την αποκλειστική δικαιοδοσία μιας διαχειριστικής οντότητας. Το πλαίσιο αυτό είναι σε θέση να αναπαριστά, να διανέμει και να διαχειρίζεται κανόνες πολιτικών καθώς και όλη τη σχετική πληροφορία. Το αρχικό πεδίο εφαρμογής του

---

[14] Mahon,(2002) H. *Requirements for a Policy Management System*. IETF Internet draft work in progress, Available from http://www.ietf.org, 22 October

[15] Ortalo R. (2001), *A Flexible Method for Information System Security Policy Specification*. In Proceedings of 5th European Symposium on Research in Computer Security (ESORICS98). 1998. Louvain-la-Neuve, Belgium, Springer-Verlag.

πλαισίου αυτού είναι η παροχή ποιότητας υπηρεσίας στο δίκτυο. Επίσης, η αρχική υπόθεση είναι ότι το πλαίσιο αυτό χρησιμοποιείται σε μικρά τοπικά δίκτυα (LANs) (Craven, 2009)[16].

• Η περιγραφή ενός μοντέλου για την απεικόνιση των πολιτικών και όλων των σχετικών πληροφοριών. Το μοντέλο πληροφορίας πολιτικών είναι βασισμένο στις προδιαγραφές του CJM/DEN και αποτελεί μια γενική μορφή για την αναπαράσταση των πολιτικών. Επιπλέον πραγματοποιήθηκε επέκταση του μοντέλου αυτού για την υποστήριξη πολιτικών προσανατολισμένων στην παροχή ποιότητας υπηρεσίας. Η προσπάθεια αυτή, είναι εστιασμένη στην εύρεση μιας γενικής λύσης, ανεξάρτητης από συγκεκριμένες τεχνολογίες υλοποίησης, που να μπορεί να εφαρμοστεί σε ένα μεγάλο εύρος δικτυακών συσκευών. Για τον λόγο αυτό αποφεύχθηκε η χρήση συγκεκριμένων πρωτοκόλλων για την επικοινωνία μεταξύ των συστατικών του πλαισίου, καθώς και η ενσωμάτωση στο μοντέλο πληροφοριών παραμέτρων που εξαρτώνται αποκλειστικά από τον κατασκευαστή μιας συσκευής.

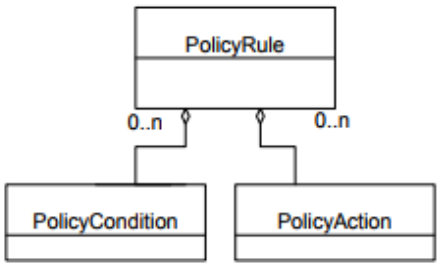
Παρά το ότι το γενικό πλαίσιο που καθορίστηκε από την ομάδα «policy» μπορεί να υποστηρίξει πολλά διαφορετικά πρωτόκολλα, το επικρατέστερο από αυτά είναι το COPS, το οποίο καθορίστηκε από μια άλλη ομάδα της IETF, την «RAP» (Resource Allocation Protocol). Ο στόχος της ομάδας αυτής είναι ο καθορισμός ενός πρωτοκόλλου για την ανταλλαγή δεδομένων πολιτικής και η περιγραφή της εφαρμογής του για την παροχή ποιότητας υπηρεσίας με χρήση του πρωτοκόλλου RSVP.

[16] R. Craven *et al.*, "Expressive policy analysis with enhanced system dynamicity," in *Proc. 4th ASIACCS*, New York, NY, USA, 2009, pp. 239–250.

2.3.2. Πολιτικές της ομάδας IETF

Μία από τις σημαντικότερες διεξαγόμενες ερευνητικές δραστηριότητες σχετικά με τις προδιαγραφές πολιτικών των δικτύων, εκτελείται από την ομάδα εργασίας της πολιτικής IETF. Δεν χρησιμοποιείται μια γλώσσα για να καθορίσουν πολιτικές, αλλά ένα μοντέλο αντικειμενοστραφών πληροφοριών (Moore et al. 2001)[17]. Αυτό το μοντέλο αποτελεί επέκταση του κοινού μοντέλου πληροφόρησης (CIM) που αναπτύχθηκε από την ομάδα εργασίας διανεμημένης διαχείρισης (Distributed Task Force, DMTF).

Ένας κανόνας πολιτικής διαμορφώνεται ως ένα σύνολο συνθηκών πολιτικής και δράσεων. Σύμφωνα με αυτή την έννοια, ένας κανόνας πολιτικής εκφράζει τη δήλωση: «*εάν ισχύει ένα σύνολο συνθηκών, τότε εκτελείται ένα σύνολο ενεργειών*». Οι κανόνες πολιτικής, οι συνθήκες και οι δράσεις συμβολίζονται ως κλάσεις αντικειμένων και οι ενώσεις τους διαμορφώνονται με τάξεις αντικειμένων συσχετισμού. Για παράδειγμα, μια παράμετρος Policy Condition συνδέεται με μια παράμετρο Policy Rule, με την συνθήκη Policy Condition In Policy Rule, και μια περίπτωση πολιτικής Action συνδέεται με τον ίδιο κανόνα με την πολιτική σύνδεσης Policy Action In Policy Rule (Geffner & Boner, 1998)[18] (Εικόνα 6)



Εικόνα 6 - παράμετρος Policy Condition που συνδέεται με μια πολιτική Policy Action

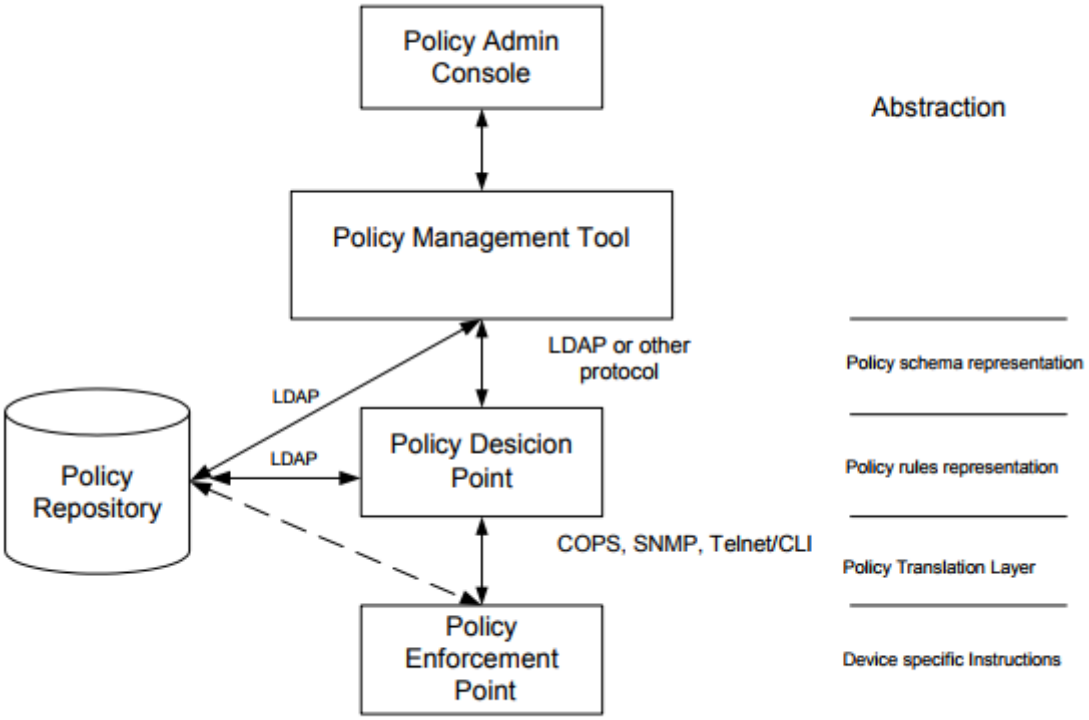
Πηγή: Moore et al. 2001

[17] Moore, B., E. Ellesson, J. Strassner and A. Westerinen (2001), Policy Core Information Model -- Version 1 Specification, RFC 3060, February 2001.

[18] Geffner, H., and Boner, B. 1998. High-level planning and control with incomplete information using POMDP's. In *working notes of the AAAI faU symposium on Cognitive Robotics.*

Οι πολιτικές δικτύου με σκοπό την **ποιότητα των υπηρεσιών** Quality Of Service (QoS) στο πλαίσιο της πολιτικής του οργανισμού IETF αντιπροσωπεύονται σύμφωνα με το μοντέλο πληροφοριών που ορίζεται από τον Snir (2001). Αυτό το μοντέλο (εικόνα 7) επεκτείνει το μοντέλο PCIM (Policy Core Information Model) με δράσεις πολιτικής, τιμές και μεταβλητές που σχετίζονται με το QoS, προκειμένου να προστεθεί ειδική σημασιολογία QoS στο πλαίσιο που ορίζεται από τον Moore (2001). Οι ενέργειες πολιτικής που ορίζονται στο QPIM (QoS Policy Information Model) είναι δράσεις διαχείρισης για δίκτυα διαφοροποιημένων υπηρεσιών (DiffServ) και ολοκληρωμένες υπηρεσίες (IntServ). Ένα παράδειγμα ενός κανόνα πολιτικής που ορίζεται στο QPIM για την καθιέρωση μιας συμπεριφοράς EF Per Hop (EF-PHB) σε έναν κόμβο DiffServ είναι το ακόλουθο:

If (traffic belongs to EF aggregate) then do EF-actions



Εικόνα 7 - IETF- policy enforcement architecture

Πηγή: Snir (2001)

Αυτή η ενέργεια για παράδειγμα, θα ρυθμίσει/προγραμματίσει τον κόμβο ώστε να παρέχει στο μέγιστο εύρος ζώνης του συνόλου της κυκλοφορίας EF το 50% του συνολικού εύρους ζώνης συνδέσμου.

Εκτός από την παροχή ενός μοντέλου πληροφοριών για την εκπροσώπηση των πολιτικών, το πλαίσιο IETF έχει ορίσει ένα σχήμα για την αποθήκευση πολιτικών σε έναν κατάλογο, ο οποίος χρησιμοποιεί το πρωτόκολλο πρόσβασης LDAP (LightWeight Directory Access Protocol). Το LDAP είναι μια νέα και πιο απλή έκδοση του DAP (Directory Access Protocol), η οποία δεν απαιτεί τα ανώτερα επίπεδα του OSI (διότι «τρέχει» απευθείας πάνω από TCP/IP) και είναι πιο εύκολο να υλοποιηθεί σε servers. Το LDAP είναι ένα πρωτόκολλο επικοινωνίας μεταξύ client/server καταλόγων (directories). Ο σκοπός του είναι να αποτελέσει τον μηχανισμό επικοινωνίας μεταξύ του policy server και των καταλόγων του συστήματος. Γεγονός είναι πως η βιομηχανία προχωρά σε υιοθέτηση του νέου προτύπου με στόχο την ενοποίηση (integration) των νέων εφαρμογών που χρησιμοποιούν τις υπηρεσίες καταλόγων (directory applications), από τον προσωπικό υπολογιστή έως το επιχειρησιακό δίκτυο (enterprise network).

Το πρωτόκολλο LDAP τρέχει πάνω από το επίπεδο μεταφοράς ενός δικτύου που στην περίπτωση του Διαδικτύου αυτό είναι το TCP. Χρησιμοποιεί τη δικτυακή διαστρωμάτωση TCP/IP για τα επίπεδα δικτύου και μεταφοράς, σε αντίθεση με την περίπλοκη διαστρωμάτωση του μοντέλου OSI.

Αυτό έχει γίνει για τις κατηγορίες που ορίζονται στο PCIM (Strassner et al, 2001)[19]. Η αποθήκευση πολιτικών σε έναν κεντρικό κατάλογο αποτελεί βασική συνιστώσα του πλαισίου διαχείρισης βάσει πολιτικής. Αυτό ακολουθεί τις έννοιες του Directory Enabled Networking (Strassner, 2001)[20] που έχει γίνει αποδεκτή ως μια ισχυρή

[19] Strassner, J., A. Westerinen and B. Moore (2001), Information Model for Describing Network Device QoS Datapath Mechanisms, Internet Draft, draft-ietf-policy-qos-deviceinfo-model-03.txt, May 2001.

[20] Strassner, J., A. Westerinen and B. Moore (2001), Information Model for Describing Network Device QoS Datapath Mechanisms, Internet Draft, draft-ietf-policy-qos-deviceinfo-model-03.txt, May 2001.

τεχνολογία για τη διαχείριση μεγάλων δικτύων. Η αρχιτεκτονική που πρότεινε η IETF για την εφαρμογή των πολιτικών παρουσιάζεται στην εικόνα 7.

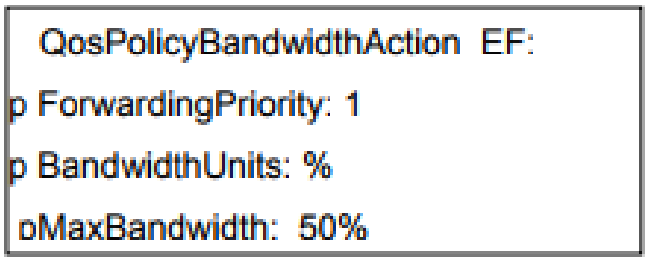
Σε αυτή την αρχιτεκτονική, κάθε σημείο λήψης πολιτικής (PDP- Policy Decision Point) είναι υπεύθυνο για τη διαχείριση ενός ή περισσοτέρων PEP (Policy Enforcement Point). Το PDP είναι υπεύθυνο για τη μετάφραση μιας πολιτικής σε μια μορφή που η συσκευή μπορεί να καταλάβει. Το PEP μεταφέρει στον PDP ποιες ενέργειες είναι σε θέση να εκτελέσει και πώς επιθυμεί να καθορίσει την πολιτική του (για παράδειγμα, τη συγκεκριμένη μορφή των συνθηκών και των ενεργειών που του μεταδίδονται). Αυτό μπορεί να κοινοποιηθεί με διάφορα μέσα, συμπεριλαμβανομένων των αποκλειστικών πρωτοκόλλων πολιτικής όπως το COPS (Durham et al. 2000).[21]

Στην αρχιτεκτονική IETF, οι κατάλογοι χρησιμοποιούνται για την αποθήκευση πολιτικών αλλά όχι για την ομαδοποίηση αντικειμένων και στόχων. Δεν έχουν τις έννοιες του θέματος και του στόχου που μπορούν να χρησιμοποιηθούν για να προσδιορίσουν σε ποια συστατικά μια πολιτική ισχύει, οπότε η χαρτογράφηση των πολιτικών σε συστατικά πρέπει να γίνει με άλλα μέσα (δηλ. τους ρόλους δι-επαφής).

Επιπλέον, δεν υποστηρίζουν τους κανόνες πολιτικής που μπορούν να ενεργοποιηθούν δυναμικά από γεγονότα για την αναμόρφωση του διαχειριζόμενου συστήματος ανάλογα με τις μεταβαλλόμενες συνθήκες. Το έργο πολιτικής στο IETF φαίνεται να επικεντρώνεται μόνο στο επίπεδο του δικτύου, και δεν έχουν εξετάσει την αλληλεπίδραση μεταξύ της εφαρμογής και της πολιτικής δικτύου.

Για παράδειγμα, εάν η κυκλοφορία ανήκει στο σύνολο EF, τότε πραγματοποιούνται ενέργειες EF. Η συνθήκη χρησιμοποιείται για τον προσδιορισμό και την ταξινόμηση της κυκλοφορίας που εισέρχεται στον κόμβο. Η ενέργεια για την παροχή ενός PHB είναι μια παρουσία της κλάσης Qos Policy Bandwidth Action. Αυτή η κλάση χρησιμοποιείται για τον έλεγχο του εύρους ζώνης, της καθυστέρησης και της συμπεριφοράς προώθησης της ροής όπου ισχύει αυτή η ενέργεια. Για τον παραπάνω κανόνα, αυτή η περίπτωση ενέργειας μπορεί να περιγραφεί ως εξής (εικόνα 8):

[21] Chan, K., D. Durham, S. Gai, S. Herzog, K. McCloghrie, F. Reichmeyer, J. Seligson, A. Smith and R. Yavatkar (2001), *COPS Usage for Policy Provisioning, RFC 3084*, March 2001.



Εικόνα 8 - Παράδειγμα πολιτικής με δημιουργία κλάσης

2.4. Ponder2

Το Ponder2 συνδυάζει ένα σύστημα γενικής χρήσης, διανεμημένου αντικειμένου με μια υπηρεσία τομέα, έναν ερμηνευτή πολιτικής υποχρεώσεων, έναν διερμηνέα εντολών και την επιβολή εξουσιοδότησης. Η Υπηρεσία Τομέα παρέχει μια ιεραρχική δομή για τη διαχείριση αντικειμένων. Ο Διευθυντής Πολιτικής Υποχρεώσεων διαχειρίζεται το συμβάν, την προϋπόθεση, και τους κανόνες δράσης (ECA). Ο διερμηνέας εντολών δέχεται ένα σύνολο εντολών, που συντάσσονται από μια γλώσσα υψηλού επιπέδου που ονομάζεται Ponder Talk, μέσω ενός αριθμού δι-επαφών επικοινωνίας που μπορούν να εκτελούν κλήσεις σε ένα Managed Object που είναι καταχωρημένο στην υπηρεσία τομέα. (diamanou et al, 2000)[22]

Η Ενίσχυση Εξουσιοδότησης καλύπτει τόσο τις θετικές όσο και τις αρνητικές πολιτικές εξουσιοδότησης, παρέχει τη δυνατότητα καθορισμού λεπτομερών εξουσιοδοτήσεων για κάθε αντικείμενο και υλοποιεί κατάλληλους αλγορίθμους τοποθέτησης τομέα για την επίλυση συγκρούσεων. Το Ponder είναι το όνομα μιας γλώσσας προδιαγραφών πολιτικής που αναπτύχθηκε στο Imperial College εδώ και

[22] Dulay, N., E. Lupu, M. Sloman and N. Damianou (2001). A Policy Deployment Model for the Ponder Language. In Proceedings of the IM 2001: 7th IEEE/IFIP International Symposium on Intergrated Network Management, Seattle, USA, 14-18 May 2001, pp. 529-544.

αρκετά χρόνια. Το ponder έχει δημιουργήσει ένα σύνολο εργαλείων και υπηρεσιών για τον καθορισμό, την ανάλυση και την επιβολή αυτών των πολιτικών. Έτσι, το όνομα Ponder συνδέθηκε όχι μόνο με τη γλώσσα αλλά με ολόκληρο το σύνολο εργαλείων. (Moore, 2001)[23]

Το Ponder2 είναι ένας σημαντικός επανασχεδιασμός το οποίο έχει βελτιώσει την προηγούμενη έκδοση. Παρόλο που μερικές από τις υποκείμενες έννοιες φέρουν ομοιότητα με τις βασικές δομές του Ponder, ολόκληρο το πλαίσιο έχει βελτιωθεί. Σε αντίθεση με την προηγούμενη έκδοση, η οποία σχεδιάστηκε για γενική διαχείριση δικτύων και συστημάτων, το Ponder2 έχει σχεδιαστεί ως ένα πλήρως εκτεταμένο πλαίσιο που μπορεί να χρησιμοποιηθεί σε διαφορετικά επίπεδα κλίμακας από μικρές, ενσωματωμένες συσκευές μέχρι πολύπλοκες υπηρεσίες και εικονικές οργανώσεις.

Το Ponder2 περιλαμβάνει ένα αυτόνομο, γενικό σύστημα διαχείρισης αντικειμένων με την χρήση μηνυμάτων που περνάει στα αντικείμενα. Ενσωματώνει την ευαισθητοποίηση σχετικά με τα γεγονότα και τις πολιτικές και εφαρμόζει ένα πλαίσιο εκτέλεσης πολιτικής. Έχει μια διαμόρφωση υψηλού επιπέδου και μια γλώσσα ελέγχου που ονομάζεται PonderTalk και τα διαχειριζόμενα αντικείμενα που διευθύνονται από προγράμματα γραμμένα σε γλώσσα Java. Ο σχεδιασμός και η εφαρμογή του Ponder2 έχουν σχεδιαστεί για να επιτύχουν τους ακόλουθους στόχους (Neisse, 2008)[24]:

• Απλότητα. Ο σχεδιασμός του συστήματος πρέπει να είναι όσο το δυνατόν απλός και να ενσωματώνει όσο το δυνατόν λιγότερα ενσωματωμένα στοιχεία.

• Επεκτασιμότητα. Πρέπει να είναι δυνατή η δυναμική επέκταση του περιβάλλοντος πολιτικής με νέες λειτουργίες, η διασύνδεση με νέες υπηρεσίες υποδομής και η διαχείριση νέων πόρων.

[23] Moore, B., E. Ellesson, J. Strassner and A. Westerinen (2001), Policy Core Information Model -- Version 1 Specification, RFC 3060, February 2001.

[24] Neisse, P. D. Costa, M. Wegdam, and M. van Sinderen(2008), "An information model and architecture for context-aware management domains." in POLICY. IEEE Computer Society, 2008, pp. 162–169. [Online]. Available: http://dblp.uni-trier. de/db/conf/policy/ policy2008.html#NeisseCWS08

• Αυτοεξυπηρέτηση. Το περιβάλλον πολιτικής δεν πρέπει να βασίζεται στην ύπαρξη υπηρεσιών υποδομής, και πρέπει να περιέχει όλα όσα είναι απαραίτητα για την εφαρμογή πολιτικών στους διαχειριζόμενους πόρους.

• Ευκολία στη χρήση. Το περιβάλλον πρέπει να διευκολύνει τη χρήση πολιτικών σε νέα περιβάλλοντα και να δημιουργεί πρωτότυπα συστήματα πολιτικής για διαφορετικές εφαρμογές.

• Δια-δραστικότητα. Πρέπει να είναι δυνατό οι διαχειριστές και οι προγραμματιστές να αλληλεπιδρούν απλά με το περιβάλλον πολιτικής, και τα διαχειριζόμενα αντικείμενα να εκδίδουν εντολές και να δημιουργούν νέες πολιτικές.

• Μεγιστοποίηση. Το περιβάλλον πολιτικής πρέπει να είναι εκτελέσιμο σε συσκευές με περιορισμένους πόρους, όπως τα PDAs και τα κινητά τηλέφωνα, καθώς και να μπορεί να διαχειρίζεται πιο παραδοσιακά κατανεμημένα συστήματα. Το Ponder2 μπορεί να αλληλεπιδράσει με άλλα στοιχεία λογισμικού και υλικού και χρησιμοποιείται σε περιβάλλοντα που κυμαίνονται από μεμονωμένες συσκευές μέχρι δίκτυα προσωπικού δικτύου, ad-hoc δίκτυα και κατανεμημένα συστήματα.

Το Ponder2 εφαρμόζει ένα αυτο-διαχειριζόμενο κύτταρο (SMC). Οι υπηρεσίες διαχείρισης αλληλεπιδρούν μεταξύ τους μέσω ασύγχρονων συμβάντων που διαδίδονται μέσω ενός διαύλου γεγονότων με βάση το περιεχόμενο. Οι πολιτικές του παρέχουν τοπική προσαρμογή κλειστού βρόχου, τα διαχειριζόμενα αντικείμενα δημιουργούν συμβάντα, οι πολιτικές ανταποκρίνονται και εκτελούν δραστηριότητες διαχείρισης στο ίδιο σύνολο διαχειριζόμενων αντικειμένων. (Russello et al, 2007)[25]

[25] G. Russello, C. Dong, and N. Dulay,(2007) "Authorization and conflict resolution for hierarchical domains," in 8th IEEE Int. Workshop on Policies for Distributed Systems and Networks(POLICY), Bologna, Italy, 2007, pp. 201–210.

Το βασικό σύστημα Ponder2 περιλαμβάνει τύπους συμβάντων, πολιτικές, τομείς και εξωτερικά κατοχυρωμένα αντικείμενα. Εναπόκειται στον χρήστη να δημιουργήσει ή να επαναχρησιμοποιήσει διαχειριζόμενα αντικείμενα για άλλους σκοπούς. Ένα διαχειριζόμενο αντικείμενο, συμπεριλαμβανομένων όλων αυτών που αναφέρθηκαν, πρέπει να φορτωθεί δυναμικά στο SMC από μια κατάλληλη βιβλιοθήκη, δημιουργώντας έτσι ένα διαχειριζόμενο αντικείμενο (για παράδειγμα μια κλάση Java). Στη συνέχεια το αντικείμενο μπορεί τώρα να στέλνει μηνύματα για να δημιουργήσει νέες εμφανίσεις διαχειριζόμενων αντικειμένων. (Russello et al, 2007)[26] Αυτά τα διαχειριζόμενα αντικείμενα είναι αυτά που υλοποιούν όλη τη φιλοσοφία του συστήματος.

Μόλις φορτωθεί, το Ponder2 δεν κάνει καμία διάκριση μεταξύ των διαχειριζόμενων αντικειμένων. Και οι δύο τύποι μπορούν να στείλουν μηνύματα που να τους ζητούν να κάνουν κάτι, και έπειτα και οι δύο να επιστρέφουν απαντήσεις. Στην περίπτωση των εργοστασιακά διαχειριζόμενων αντικειμένων επιστρέφουν μια νέα εμφάνιση του υποκείμενου τύπου τους. Το υπόβαθρο του Ponder ήταν ένα εξαιρετικά επιτυχημένο περιβάλλον πολιτικής το οποίο χρησιμοποίησαν πολλοί, τόσο στον τομέα της βιομηχανίας όσο και στον ακαδημαϊκό κόσμο.

Ωστόσο, το ponder2 υπέφερε από τα ίδια μειονεκτήματα με τα υφιστάμενα πλαίσια που βασίζονται σε πολιτικές. Τα σχέδιά τους εξαρτώνται από την κεντρική υποστήριξη υποδομής, όπως οι κατάλογοι LDAP και τα αποθετήρια CIM. Το μοντέλο ανάπτυξης βασιζόταν συχνά σε συγκεντρωτικές προβλέψεις και στη λήψη αποφάσεων. Ως εκ τούτου, δεν προσέφεραν τα μέσα ώστε τα συστατικά στοιχεία εκτέλεσης πολιτικής να αλληλεπιδρούν μεταξύ τους, να συνεργάζονται ή να ενοποιούνται σε μεγαλύτερες δομές. Οι προδιαγραφές πολιτικής θεωρήθηκαν ως δραστηριότητα off-line και τα πλαίσια πολιτικής δεν τους επέτρεπαν να αλληλεπιδρούν εύκολα με τα διαχειριζόμενα συστήματα. Συνεπώς, τέτοια πλαίσια ήταν δύσκολο να εγκατασταθούν και να εκτελεστούν. Το Ponder2 έχει ήδη εφαρμοστεί σε πολλά ερευνητικά προγράμματα για

[26] G. Russello, C. Dong, and N. Dulay,(2007) "Authorization and conflict resolution for hierarchical domains," in 8th IEEE Int. Workshop on Policies for Distributed Systems and Networks(POLICY), Bologna, Italy, 2007, pp. 201–210.

την παρακολούθηση της υγείας με τη χρήση δικτύων αισθητήρων και ενεργοποιητών, μη επανδρωμένων αυτόνομων οχημάτων καθώς και μεγάλων υποδομών βασισμένων σε υπηρεσίες ιστού.

2.5.KAos

Το KAoS είναι ένα πλαίσιο υπηρεσιών και τομέων υπηρεσιών που δημιουργήθηκε από το Ινστιτούτο της Φλόριντα για την Ανίχνευση Ανθρώπου και Μηχανής. Χρησιμοποιεί το πρότυπο της γλώσσας Ontology Language (OWL) του W3C για την εκπροσώπηση και τη συλλογή των πολιτικών, και μια τεχνολογία φύλαξης λογισμικού για την αποτελεσματική εφαρμογή μιας σύνθετης έκδοσης των πολιτικών της. Έχει χρησιμοποιηθεί σε διάφορα κυβερνητικά χρηματοδοτούμενα έργα για τη διαχείριση κατανεμημένων κεντρικών υπολογιστών και δικτύων και για τον συντονισμό των ομάδων ανθρώπινου παράγοντα-ρομπότ, συμπεριλαμβανομένων των μοντέλων ARBA του CoABS Grid, Cougaar και CORBA (Kagal, 2003).[27]

2.5.1. Υπηρεσία Πολιτικής του KAoS

Οι υπηρεσίες του KAoS έχουν επεκταθεί για να λειτουργούν εξίσου καλά τόσο με την χρήση πρακτόρων (π.χ. CoABS Grid, Cougaar, SFX, Brahms) όσο και με παραδοσιακούς πελάτες σε διάφορες γενικές κατανεμημένες πλατφόρμες υπολογιστών (π.χ. CORBA, Grid Computing (Globus GT3)). Το KAoS χρησιμοποιεί έννοιες οντολογιών που κωδικοποιούνται στην γλώσσα OWL για την ανάπτυξη πολιτικών. Αυτές οι πολιτικές περιορίζουν τις επιτρεπόμενες ενέργειες που εκτελούνται από φορείς (πελάτες ή πράκτορες).

[27] Kagal, L., Finin, T., & Joshi, A. (2003). A policy-based approach to security for the Semantic Web. In D. Fensel, K. Sycara, & J. Mylopoulos (Ed.), *The Semantic Web—ISWC 2003. Proceedings of the Second International Semantic Web Conference, Sanibel Island, Florida, USA, October 2003, LNCS 2870.* (pp. 402-418).: Springer.

Η Υπηρεσία Πολιτικής KAoS κάνει διάκριση μεταξύ των εξουσιοδοτήσεων (δηλαδή των περιορισμών που επιτρέπουν ή απαγορεύουν κάποια ενέργεια) και των υποχρεώσεων (δηλαδή, οι περιορισμοί που απαιτούν κάποια ενέργεια να εκτελείται όταν συμβαίνει ένα γεγονός που βασίζεται σε κατάσταση ή συμβάν ή αλλιώς εξυπηρετεί την άρση μιας τέτοιας απαίτησης). Η εφαρμογή της πολιτικής καθορίζεται από μια κατηγορία καταστάσεων όπου ο ορισμός μπορεί να περιέχει στοιχεία που προσδιορίζουν το απαιτούμενο ιστορικό, και τη στιγμή που αναλαμβάνεται δράση. Στην περίπτωση της πολιτικής υποχρεώσεων, η υποχρεωτική ενέργεια μπορεί να επισημανθεί με διαφορετικούς περιορισμούς που περιορίζουν τις δυνατότητες εκπλήρωσής της. Το KAoS προσφέρει γενικό και ήδη δοκιμασμένο μηχανισμό τουλάχιστον στους ακόλουθους τομείς (Uszok, 2010)[28] :

- Πολιτική εκκίνησης και διαμόρφωση συστήματος πολιτικής

Κατά τη διάρκεια της εκκίνησης, το KAoS φορτώνει αρχικά τις οντότητες πολιτικής KAoS που ορίζουν τις έννοιες που χρησιμοποιούνται για να περιγράψουν το περιβάλλον και τις πολιτικές των γενικών παραγόντων στο πλαίσιο αυτό. Εναλλακτικά, μπορεί να φορτωθεί μια προηγούμενη αποθηκευμένη διαμόρφωση που περιέχει χώρους ονομάτων, πολιτικές κ.λπ. Μια τέτοια διαμόρφωση μπορεί να αποθηκευτεί ανά πάσα στιγμή κατά την εκτέλεση του συστήματος, για να διατηρηθούν οι δημιουργημένες πολιτικές και οι ορισμοί οντολογιών. Ontology Name space (Uszok, 2010)[29]

[28] Uszok, A., Bradshaw, J. M., Jeffers, R., Suri, N., Hayes, P., Breedy, M. R., Bunch, L., Johnson, M., Kulkarni, S., & Lott, J. (2003). KAoS policy and domain services: Toward a description-logic approach to policy representation, deconfliction, and enforcement. *Proceedings of Policy 2003*. Como, Italy

[29] Uszok, A., Bradshaw, J. M., Jeffers, R., Suri, N., Hayes, P., Breedy, M. R., Bunch, L., Johnson, M., Kulkarni, S., & Lott, J. (2003). KAoS policy and domain services: Toward a description-logic approach to policy representation, deconfliction, and enforcement. *Proceedings of Policy 2003*. Como, Italy

- Περιήγηση και διαχείριση

Το KAoS επιτρέπει την περιήγηση φορτωμένων οντολογιών: εξέταση του περιεχομένου τους, τάξεις, ιδιότητες, παρουσίες και χώρους ονομάτων. Επίσης, επιτρέπει τη δυναμική προσθήκη νέων οντολογιών σχετικά με τις έννοιες που εκτείνονται από τη γενική οντολογία, με έννοιες συγκεκριμένες για το σχετικό ελεγχόμενο περιβάλλον.

- Δημιουργία κλάσης τομέα και δράστη

Το KAoS επιτρέπει διαφορετικούς τρόπους έκφρασης του θέματος της πολιτικής, είτε μέσω ρητής προσχώρησης σε τομέα, είτε έμμεσα μέσω αξιών των ιδιοτήτων που ορίζονται ως κλάσεις οντολογιών. Εναλλακτικά, οι πολιτικές μπορούν να οριστούν ως αφηρημένες τάξεις.

- Δημιουργία Πολιτικών

Οι πολιτικές μπορούν να δημιουργηθούν εκ νέου, χρησιμοποιώντας μια ειδικά σχεδιασμένη δι-επαφή χρήστη API ή KPAT GUI. Μέσω της δι-επαφής χρήστη, ρυθμίζονται οι απαραίτητοι παράμετροι και οι τιμές που θέλει ο διαχειριστής δικτύου να ισχύουν για μια συγκεκριμένη πολιτική διαχείρισης. Η κωδικοποίηση OWL της δημιουργηθείσας πολιτικής δημιουργείται χρησιμοποιώντας δημοφιλές και καλά υποστηριζόμενο από το HP Lab Jena toolkit. Ωστόσο η πολυπλοκότητα αυτής της αναπαράστασης αποκρύπτεται από τους χρήστες και σε μεγάλο βαθμό και από τις συνδεδεμένες εφαρμογές.

- Διανομή πολιτικής

Μετά την δημιουργία μιας πολιτικής, αυτή πρέπει να διανέμεται μέσω της υπηρεσίας καταλόγου KAoS στους φρουρούς, οι οποίοι αποτελούν σημεία λήψης αποφάσεων πολιτικής, και βρίσκονται κοντά στις τρέχουσες οντότητες. Συνήθως ένας φρουρός συνδέεται με ένα Java VM.

- Περιγραφή

Χρησιμοποιείται για να διαπιστώσει εάν η συγκεκριμένη πολιτική θα πρέπει να διανεμηθεί σε μια πύλη ελέγχου που ελέγχει συγκεκριμένους συντελεστές (το KAoS πρέπει να καθορίσει εάν ενδεχομένως εμπίπτει στο πεδίο εφαρμογής της συγκεκριμένης πολιτικής). Στη συνέχεια, η πολιτική μεταφράζεται από το μορφότυπο OWL σε πιο αποτελεσματική μορφή κατακερματισμού και τα απαραίτητα αποτελέσματα κατάταξης στις έννοιές της (δηλαδή υποκλάσεις) αποθηκεύονται στη συσκευασμένη πολιτική που αποστέλλεται στον Guard, προκειμένου να καταστεί αποτελεσματική η διαδικασία λήψης αποφάσεων. (Bradshaw, 2011)[30]

2.6.WS-POLICY

Η προσέγγιση WS-Policy παρέχει μια ευέλικτη και επεκτάσιμη γλώσσα με σκοπό την συγγραφή των απαιτήσεων και των γενικών χαρακτηριστικών των οντοτήτων σε ένα σύστημα που βασίζεται στις υπηρεσίες XML Web. Η Πολιτική WS ορίζει ένα πλαίσιο και ένα μοντέλο για την έκφραση αυτών των ιδιοτήτων ως πολιτικές διαχείρισης. Η Πολιτική WS ορίζει μια πολιτική ως μια συλλογή πολιτικών που αποτελείται από εναλλακτικές πολιτικές. Ορισμένες από αυτές τις πολιτικές καθορίζουν τις βασικές απαιτήσεις και τις δυνατότητες που τελικά θα ισχύουν σε ένα δίκτυο (π.χ., σύστημα ελέγχου ταυτότητας, επιλογή πρωτοκόλλου μεταφοράς). Άλλες πολιτικές σχετίζονται με πιο κρίσιμα ζητήματα όπως για παράδειγμα την πολιτική απορρήτου, και τα χαρακτηριστικά του QoS.

---

[30] Bradshaw, J. M., Uszok, A., Jeffers, R., Suri, N., Hayes, P., Burstein, M. H., Acquisti, A., Benyo, B., Breedy, M. R., Carvalho, M., Diller, D., Johnson, M., Kulkarni, S., Lott, J., Sierhuis, M., & Van Hoof, R. (2003). Representation and reasoning for DAML-based policy and domain services in KAoS and Nomads. *Proceedings of the Autonomous Agents and Multi-Agent Systems Conference (AAMAS 2003)*. Melbourne, Australia, New York, NY: ACM Press

Βασικός στόχος μιας Πολιτικής WS είναι να παρέχει τους μηχανισμούς που απαιτούνται για να επιτρέψουν στις εφαρμογές υπηρεσιών Web να καθορίσουν τις πληροφορίες πολιτικής. Ειδικότερα, αυτή η προδιαγραφή ορίζει τα εξής:

• Ένα XML Infoset που ονομάζεται «έκφραση πολιτικής» και περιέχει συγκεκριμένες πληροφορίες σχετικά με τις πολιτικές Web για συγκεκριμένες περιοχές.

• Ένα βασικό σύνολο κατασκευών που υποδεικνύει πως εφαρμόζονται οι επιλογές και / ή οι συνδυασμοί πολιτικής συγκεκριμένων τομέων σε περιβάλλον υπηρεσιών Web.

Ένα παράδειγμα σύνταξης μιας πολιτικής WS-Policy παρουσιάζεται στην εικόνα 9:

```
(01) <wsp:Policy
      xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
      xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy" >
(02)  <wsp:ExactlyOne>
(03)        <sp:Basic256Rsa15 />
(04)        <sp:TripleDesRsa15 />
(05)  </wsp:ExactlyOne>
(06) </wsp:Policy>
```

Εικόνα 9 - Παράδειγμα πολιτικής WS-Policy

Στο παραπάνω παράδειγμα η πολιτική ασφάλειας καθορίζει τους κανόνες όπως αυτοί ορίζονται στο WS-SecurityPolicy. Οι γραμμές (01-06) αντιπροσωπεύουν μια πολιτική για μια σειρά αλγορίθμων που απαιτούνται για την εκτέλεση λειτουργιών κρυπτογράφησης με συμμετρικές ή ασύμμετρες μεθόδους ασφαλείας. Οι γραμμές (02-05) ορίζουν τον χειριστή πολιτικής π.χ. «Exactly One».

2.7. DMTF

Η DMTF (Distributed Management Task Force) ξεκίνησε υιοθετώντας την προδιαγραφή Directory Enabled Network (DEN), που είχε ως στόχο την αντιστοίχιση δικτυακών υπηρεσιών σε ένα κατάλογο. Τα αντικείμενα του καταλόγου μπορούν να αντιπροσωπεύουν δίκτυα/υποδίκτυα, υπηρεσίες, συσκευές, εφαρμογές, χρήστες ή τοποθεσίες. Οι σχέσεις μεταξύ των αντικειμένων αυτών καθορίζονται και διαχειρίζονται μέσα στον ίδιο τον κατάλογο. Η πρόσβαση στα δεδομένα διαχείρισης γίνεται μεταξύ δεσμών με τα αντικείμενα του καταλόγου. Με τη μέθοδο αυτή έχουμε ένα μοναδικό μοντέλο για την πρόσβαση στα αντικείμενα, γεγονός που επιτρέπει τη συνεργασία μεταξύ διαφορετικών συστημάτων διαχείρισης.

Ο απώτερος στόχος του DEN είναι η χρήση ενός μοναδικού καταλόγου σαν μια κεντροποιημένη αποθήκη, που περιέχει τη σχέση μεταξύ χρηστών και εφαρμογών καθώς και τις σχέσεις τους με τις δικτυακές υπηρεσίες, για την επίτευξη της συνεργασίας και της ανταλλαγής κοινής πληροφορίας. Η DMTF προχώρησε στον καθορισμό του σχήματος CIM (Common Information Model), που αποτελείται από ένα αντικειμενοστραφές μοντέλο για την αναπαράσταση της πληροφορίας που αποθηκεύεται στον κατάλογο ενός δικτύου που ακολουθεί την προδιαγραφή DEN. Το CIM είναι δομημένο σε τρία επίπεδα. Το κεντρικό μοντέλο απεικονίζει έννοιες που είναι κοινές σε όλες τις περιοχές της διαχείρισης. Το κοινό μοντέλο απεικονίζει έννοιες που είναι κοινές σε ορισμένες περιοχές διαχείρισης, αλλά παραμένουν ανεξάρτητες από συγκεκριμένες τεχνολογίες ή υλοποιήσεις. Οι κοινές περιοχές είναι του συστήματος, των εφαρμογών και των συσκευών. Το τρίτο επίπεδο του CIM είναι τα σχήματα επέκτασης, που αναπαριστούν επεκτάσεις του κοινού μοντέλου προσανατολισμένες σε συγκεκριμένες τεχνολογίες. (Craven, 2009)[31]

Το CIM καθαυτό αποτελεί αποκλειστικά ένα μοντέλο για την αναπαράσταση δεδομένων διαχείρισης και δεν υπεισέρχεται σε λεπτομέρειες γύρω από τη διαχείριση

[31] R. Craven *et al.*, "Expressive policy analysis with enhanced system dynamicity," in *Proc. 4th ASIACCS*, New York, NY, USA, 2009, pp. 239–250.

βάσει πολιτικών. Παρ' όλα αυτά όμως από την αρχή υιοθετήθηκε ως βασικό μοντέλο πληροφορίας για συστήματα διαχείρισης βάσει πολιτικών

2.8. Το Πρωτόκολλο COPS

Το COPS αποτελεί ένα πρωτόκολλο επικοινωνίας μεταξύ του Καταναλωτή Πολιτικών και του Στόχου Πολιτικών, προκειμένου ο πρώτος να μπορεί να εφαρμόσει τις αποφάσεις που απορρέουν από τους εγκατεστημένους στο δίκτυο κανόνες. Το πρωτόκολλο αυτό έχει οριστεί από την IETF και ο βασικός του στόχος ήταν να αποτελέσει μια συγκεκριμένη υλοποίηση των γενικών προδιαγραφών διαχείρισης με πολιτικές, προσανατολισμένη στην παροχή ποιότητας υπηρεσίας, κατά κύριο λόγο σε δίκτυα που χρησιμοποιούν μηχανισμούς RSVP. Εκτός από το πρωτόκολλο επικοινωνίας, το COPS προϋποθέτει και την ύπαρξη μιας αρχιτεκτονικής διαχείρισης ανάλογης με αυτήν που περιγράφει ως πρότυπο.

Το COPS (Common Open Policy Sen-ice) εισάγει νέες ονομασίες για τα βασικά στοιχεία της αρχιτεκτονικής διαχείρισης με πολιτικές. Πιο συγκεκριμένα, το Σημείο Απόφασης Πολιτικών (PDP) αντιστοιχεί στον Καταναλωτή Πολιτικών του γενικού μοντέλου, ενώ το Σημείο Εφαρμογής Πολιτικών (PEP) είναι ανάλογο του Στόχου Πολιτικών. Βασικός στόχος κατά τον καθορισμό του πρωτοκόλλου αποτέλεσε η δημιουργία μιας απλής αλλά επεκτάσιμης δομής. Το πρωτόκολλο επιστρατεύει μια αρχιτεκτονική πελάτη/εξυπηρετητή, σύμφωνα με την οποία το PEP στέλνει αιτήσεις, ανανεώσεις στοιχείων και διαγραφές στο απομακρυσμένο PDP, ενώ το PDP αποστέλλει τις αποφάσεις πίσω στο PEP. Το πρωτόκολλο χρησιμοποιεί το TCP ως πρωτόκολλο μεταφοράς, για την αξιόπιστη ανταλλαγή μηνυμάτων μεταξύ των πελατών πολιτικών.

2.9. Η ασφάλεια στην διαχείριση πολιτικών δικτύων

2.9.1. Τι είναι ασφάλεια

Ως Ασφάλεια θεωρείται η συνδυαστική προσπάθεια για προστασία και αντιμετώπιση οποιουδήποτε προβλήματος ή δυσλειτουργίας. Ισχύει για κάθε ευάλωτο ή πολύτιμο περιουσιακό στοιχείο, όπως ένα άτομο, μία κατοικία, μία κοινότητα, ένα οποιοδήποτε στοιχείο ή πληροφορία. Όπως αναφέρεται από το Ινστιτούτο Ασφάλειας Ανοικτών Μεθοδολογιών (ISECOM) στο OSSTMM 3, η ασφάλεια παρέχει "μια μορφή προστασίας όπου δημιουργείται ένας διαχωρισμός μεταξύ των περιουσιακών στοιχείων και της απειλής". Αυτοί οι διαχωρισμοί αποκαλούνται γενικά "έλεγχοι" και μερικές φορές περιλαμβάνουν αλλαγές στο περιουσιακό στοιχείο ή την απειλή. (Taureck, 2006)[32]

2.9.2. Ασφάλεια στην διαχείριση των δικτύων

Στις απαιτήσεις ασφάλειας περιλαμβάνονται οι εξής (Ju et al, 2011)[33]:

- Ταυτοποίηση και εξουσιοδότηση. Οι μηχανισμοί ταυτοποίησης απαιτούνται για την επιβεβαίωση της ταυτότητας χρηστών και υπηρεσιών. Οι πάροχοι υπηρεσιών πρέπει να υλοποιούν μηχανισμούς εξουσιοδότησης για να επιβάλουν πολιτικές χρήσης των υπηρεσιών. Το σύστημα Grid θα πρέπει να ακολουθεί τις πολιτικές ασφάλειας κάθε περιοχής, ενώ επίσης μπορεί να χρειάζεται να εξακριβώνει τις πολιτικές ασφάλειας των χρηστών. Η εξουσιοδότηση θα πρέπει να διευθετεί διάφορα μοντέλα και

[32] Taureck, R., (2006) Securitization theory – The Story So Far: Theoretical inheritance and what it means to be a post-structural realist. Paper presented at the 4th annual CEEISA convention, University of Tartu, 25-27 June.

[33] Ju H., Choi M., Hong J(2011), EWS-Based Management Application Interface and Integration Mechanisms for Web-Based Element Management, Journal of Network and Systems Management, Vol.9, No.1

υλοποιήσεις ελέγχου πρόσβασης.

- Πολλαπλές υποδομές ασφάλειας. Οι κατανεμημένες λειτουργίες συνεπάγονται την ανάγκη ενσωμάτωσης και δια-λειτουργικότητας με πολλαπλές υποδομές ασφάλειας. Η OGSA χρειάζεται να ολοκληρωθεί και να λειτουργεί με υπάρχουσες αρχιτεκτονικές και μοντέλα ασφάλειας.

- Λύσεις περιμετρικής ασφάλειας. Πόροι μπορεί να χρειάζεται να προσπελαύνονται υπερβαίνοντας όρια οργανισμών. Η OGSA απαιτεί πρότυπους και ασφαλείς μηχανισμούς που μπορούν να αναπτυχθούν για την προστασία οργανισμών, ενώ θα επιτρέπουν επίσης την αλληλεπίδραση μεταξύ διαφορετικών περιοχών χωρίς να υπονομεύουν τοπικούς μηχανισμούς ασφάλειας όπως firewalls και πολιτικές ανίχνευσης εισβολής.

- Απομόνωση. Διάφορα είδη απομόνωσης πρέπει να διασφαλίζονται, όπως η απομόνωση χρηστών, η απομόνωση επίδοσης και η απομόνωση μεταξύ προσφορών περιεχομένου εντός του ιδίου συστήματος Grid.

- Μεταβίβαση. Απαιτούνται μηχανισμοί που επιτρέπουν τη μεταβίβαση δικαιωμάτων πρόσβασης από αιτούντες υπηρεσίας σε παρόχους υπηρεσιών. Ο κίνδυνος κακής χρήσης των μεταβιβασμένων δικαιωμάτων πρέπει να ελαχιστοποιείται, περιορίζοντας π.χ. τα δικαιώματα που μεταφέρονται μέσω μεταβίβασης στην προτεινόμενη εργασία με τον περιορισμό του χρόνου ζωής τους.

- Ανταλλαγή πολιτικών ασφάλειας. Οι πάροχοι υπηρεσιών και οι αιτούντες υπηρεσιών θα πρέπει να είναι σε θέση να ανταλλάσσουν δυναμικά πληροφορίες πολιτικών ασφάλειας για να εγκαθιδρύσουν μεταξύ τους ένα πλαίσιο ασφάλειας μέσα από διαπραγμάτευση.

- Ανίχνευση εισβολής, προστασία και ασφαλής σύνδεση. Απαιτούνται ισχυρές δυνατότητες παρακολούθησης για την πραγματοποίηση ανίχνευσης εισβολής και τον προσδιορισμό κακής χρήσης, σκόπιμα επιβλαβούς ή μη περιλαμβανομένων επιθέσεων ιών ή σκουληκιών(worms). Επίσης θα πρέπει να είναι δυνατή η προστασία κρίσιμων περιοχών ή λειτουργιών, αποδιώχνοντας επιθέσεις που κατευθύνονται προς αυτές.

2.10. Βασικές απαιτήσεις και αρχιτεκτονική

Οι βασικές απαιτήσεις για το σχεδιασμό ενός πλαισίου διαχείρισης δικτύων είναι οι ακόλουθες:

- Ευελιξία

Στα δίκτυα των υπολογιστών, μια πολιτική μπορεί να αναπαρασταθεί τόσο χρησιμοποιώντας καθορισμένες δομές και μοντέλα πληροφορίας, οι οποίες αναγκαστικά περιορίζονται από τις δυνατότητες των τυποποιημένων σχημάτων, όσο και με την χρήση κώδικα. Μια πολιτική θα πρέπει να καθορίζεται με τέτοιο τρόπο έτσι ώστε υπάρχει ευελιξία και να μπορεί εύκολα να τροποποιηθεί, όταν αυτό είναι απαραίτητο.

- Επεκτασιμότητα

Ένα σύστημα διαχείρισης δικτύου με χρήση πολιτικών, το οποίο θα πρέπει να υλοποιείται λαμβάνοντας υπόψη την τεχνολογία των δικτύων και να έχει τη δυνατότητα να επεκτείνει δυναμικά τη λειτουργικότητά του, κατεβάζοντας και εγκαθιστώντας νέα συστατικά. Με τον τρόπο αυτό μπορεί να αντιμετωπίσει επαρκώς τη μεταβαλλόμενη υποδομή και τα νέα πρωτόκολλα.

- Αυτοματοποίηση και κατανομή των διαχειριστικών διαδικασιών

Ένας σημαντικός στόχος μιας αρχιτεκτονικής διαχείρισης είναι και το να αυτοματοποιήσει και να κατανείμει τα διαχειριστικά έργα στο μεγαλύτερο δυνατό βαθμό, ώστε να μειωθεί ο χρόνος απόκρισης του συστήματος. Τα δίκτυα επιτρέπουν την εισαγωγή του κώδικα της διαχείρισης σε όλους τους κόμβους, επομένως μπορούν να αυτοματοποιήσουν διαδικασίες όπως για παράδειγμα η αυτό-αναδιάρθρωση του κόμβου ύστερα από μεταβολή των συνθηκών του δικτύου.

- Αντιπροσωπεία

Η αντιπροσωπεία, δηλαδή η ανάθεση συγκεκριμένης διαχειριστικής λειτουργίας του δικτύου από το διαχειριστή σε κάποιο πελάτη, μπορεί να μειώσει σημαντικά το κόστος και την επιβάρυνση του συστήματος διαχείρισης. Ο πελάτης θα

μπορεί να διαχειρίζεται ο ίδιος τους πόρους του, χωρίς να υπάρχει κάποια άλλη απαίτηση από τον πάροχο του δικτύου. Τα δίκτυα μπορούν να προσφέρουν ικανούς και επαρκείς τρόπους για την πραγματοποίηση της διαδικασίας αυτής.

• Παροχή διαχειριστικής λειτουργίας στις εφαρμογές. Η ιδανική διάρθρωση του κόμβου και του δικτύου, μπορεί να είναι διαφορετική για κάθε εφαρμογή και να μεταβάλλεται ανάλογα με την κατάσταση του δικτύου. Τα δίκτυα παρέχουν το τεχνολογικό υπόβαθρο για να μπορεί ένας πελάτης να παραμετροποιεί τους πόρους που του έχουν ανατεθεί, π.χ. χρησιμοποιώντας τις κατάλληλες πολιτικές μπορεί να βελτιστοποιεί τη χρήση των πόρων μιας εφαρμογής σε διάφορες καταστάσεις του δικτύου.

Αρχιτεκτονική

Για να δημιουργήσουμε μια δομή στην πολιτική ασφάλειας σε ένα δίκτυο, θα πρέπει να υπάρχει μια ολοκληρωμένη αρχιτεκτονική. Η αρχιτεκτονική αυτή θα πρέπει να οδηγεί σε επί μέρους πολιτικές που να είναι συνεπείς με την συνολική αρχιτεκτονική ασφάλειας στο δίκτυό μας. Εάν, για παράδειγμα, θεσπίσουμε μία ισχυρή πολιτική ασφάλειας ως προς την πρόσβαση από το Διαδίκτυο, αλλά μία ασθενή πολιτική ασφάλειας για πρόσβαση μέσω τηλεφωνικού δικτύου, δεν θα υπήρχε συνέπεια με την συνολική φιλοσοφία ισχυρών περιορισμών ασφαλείας σε προσβάσεις από το εξωτερικό του δικτύου. Επομένως, πρέπει να ορίζονται :

- Οι παρεχόμενες δικτυακές υπηρεσίες
- Οι περιοχές της εταιρείας που θα παρέχουν τις υπηρεσίες αυτές
- Ποιος θα έχει πρόσβαση στις υπηρεσίες αυτές
- Πώς θα παρέχεται πρόσβαση σε αυτές
- Ποιος θα τις διαχειρίζεται
- Πώς θα γίνεται ο χειρισμός συμβάντων κλπ.
- Επίσης, σημασία έχει και ο λεγόμενος διαχωρισμός των υπηρεσιών

Η κεντρική ιδέα είναι ότι για λόγους ασφαλείας – αλλά και αποδοτικότητας – είναι σκόπιμο να παρέχεται κάθε υπηρεσία από ξεχωριστό εξυπηρέτη, και άρα και δικτυακό κόμβο. Εδώ πρέπει να λαμβάνεται υπ' όψιν και η διαβάθμιση της παροχής μίας υπηρεσίας ανά τύπο πελάτη, αλλά και το ότι κάθε υπολογιστής-εξυπηρέτης μπορεί να βρίσκεται σε διαφορετική περιοχή του δικτύου από πλευράς επιπέδου ασφαλείας.

Τα βασικά μοντέλα είναι δύο: 'Deny all' και 'Allow all'.

Σύμφωνα με το πρώτο, κλείνουμε όλες τις υπηρεσίες και επιλεκτικά ενεργοποιούμε υπηρεσίες κατά περίπτωση και όταν χρειάζονται. Αυτό μπορεί να γίνει σε επίπεδο δικτύου ή και κατά υπολογιστή. Λόγω της ακραίας μορφής περιορισμού είναι δύσκολο να επιτευχθεί μία τέτοια πολιτική με επιτυχία. Σύμφωνα με το δεύτερο, ενεργοποιούμε όλες τις υπηρεσίες σε κάθε υπολογιστή, ιδίως τις συνηθισμένες, ενώ επιτρέπουμε σε όλα τα συνηθισμένα πρωτόκολλα που είναι διαθέσιμα σε επίπεδο δρομολογητή να διατρέχουν όλο το δίκτυο. Για οποιεσδήποτε τρύπες ασφαλείας προχωράμε σε περιορισμό ή επιδιόρθωσή τους, είτε σε επίπεδο υπολογιστή, είτε σε επίπεδο δικτύου. Προφανώς αυτή η προσέγγιση προσφέρει εξ' ορισμού και την χαμηλότερη ασφάλεια. Αν και τα δύο μοντέλα παραπάνω θεωρούνται ορθά, προκύπτει σοβαρό πρόβλημα όταν προσπαθούμε να τα αναμείξουμε άκριτα. Για παράδειγμα, δεν είναι ορθή η προσέγγιση της ισχυρής ασφάλειας στα άκρα του δικτύου και χαμηλής στο εσωτερικό του.

Πιο συγκεκριμένα, το να έχουμε ανώνυμη υπηρεσία FTP στο ίδιο μηχάνημα που στεγάζει την υπηρεσία WWW, μπορεί να επιτρέψει σε έναν επίδοξο εισβολέα να ανεβάσει ένα αρχείο μέσω της πρώτης υπηρεσίας και να το εκτελέσει μέσω της δεύτερης. Μία συνηθισμένη πρακτική είναι για τους διαχειριστές να προσπαθούν να προστατεύσουν μεμονωμένους υπολογιστές, παρά ολόκληρο το δίκτυο. Το σκεπτικό είναι ότι είναι ευκολότερο να γίνει κάτι τέτοιο, ενώ η πιθανότητα για τους εισβολείς να επιτεθούν σε έναν υπολογιστή (λόγω των δεδομένων που στεγάζει) είναι μεγαλύτερη. Εν τούτοις, το ορθό είναι να προστατεύεται ολόκληρο το δίκτυο, αλλά και η σχετική υποδομή. Εδώ δεν περιλαμβάνονται απλά τα υποδίκτυα και οι δρομολογητές, αλλά όλες οι υπηρεσίες και η πρόσβαση των χρηστών.

2.11. Η παροχή ποιότητας υπηρεσιών στην διαχείριση των δικτύων βάσει πολιτικών Quality of Service

2.11.1. Ορισμός του QoS

Η ερευνητική δραστηριότητα που έχει λάβει χώρα για την εύρεση των απαιτήσεων για ποιότητα υπηρεσίας είναι μεγάλη. Αυτό βοηθάει σε αρκετό βαθμό την περαιτέρω έρευνα ανάπτυξης αρχιτεκτονικών για την παροχή Ποιότητας Υπηρεσιών στο Διαδίκτυο. Από τις υπάρχουσες μελέτες οι ανάγκες κατηγοριοποιούνται σύμφωνα με τις παρακάτω περιοχές[34]:

- Σύμφωνα με τις ανάγκες των πελατών
- Σύμφωνα με τις ανάγκες των απαιτητικών εφαρμογών
- Σύμφωνα με τις ανάγκες των εταιριών που παρέχουν πρόσβαση στο διαδίκτυο ή που παρέχουν υπηρεσίες

Τύποι παροχής ποιότητας υπηρεσίας

Υπάρχουν πολλοί τρόποι να χαρακτηρίσει κανείς και να δώσει ένα ορισμό της ποιότητας υπηρεσίας. Γενικά μιλώντας, Ποιότητα Υπηρεσίας είναι η ικανότητα ενός στοιχείου του δικτύου (Network Element) να παρέχει κάποια επίπεδα εγγύησης για τη σωστή παράδοση των δεδομένων. Όπως αναφέρθηκε προηγουμένως μερικές εφαρμογές είναι περισσότερο απαιτητικές σε ποιότητα υπηρεσίας σε σχέση με κάποιες άλλες, για αυτό το λόγο έχουμε δυο βασικούς τύπους παροχής ποιότητας υπηρεσιών.

Οι δύο αυτοί τύποι είναι:

- *Δέσμευση Πόρων - Resource Reservation (Ολοκληρωμένες Υπηρεσίες - Integrated Services):* Οι πόροι του δικτύου διανέμονται σύμφωνα με μια εφαρμογή αίτησης ποιότητας υπηρεσίας, και είναι εξαρτώμενοι από την Πολιτική Διαχείρισης

[34] F. Kelly, “Notes on Effective Bandwidths”, in "Stochastic Networks: Theory and Applications" (Editors: F. Kelly, S. Zachary and I.B. Ziedins), pp. 141-168, Oxford University Press, 2009

Εύρους Ζώνης (Bandwidth Management Policy).

- *Καθορισμός Προτεραιοτήτων - Prioritization (Διαφοροποιημένες Υπηρεσίες - Differentiated Services):* Η δικτυακή κίνηση κατηγοριοποιείται, και διανέμονται σε αυτή πόροι του δικτύου σύμφωνα με τα κριτήρια τα οποία έχουν ποιότητα υπηρεσίας, Τα στοιχεία του δικτύου δίνουν προνομιακή μεταχείριση στους κατηγοριοποιητές προσδιορίζοντας τις περισσότερο απαιτητικές εφαρμογές.

Αυτοί οι τύποι ποιότητας υπηρεσιών μπορούν να εφαρμοστούν σε εφαρμογές ξεχωριστών ροών *(Flows)* ή σε εφαρμογές ομαδοποιημένων ροών (*Aggregate*), ώστε τελικά να υπάρχει ένας διαφορετικός τρόπος να χαρακτηρίσουμε τον τύπο της ποιότητας υπηρεσίας[35]:

- *Ανά Ροή - Per Flow*: Η «Ροή» ορίζεται ως μια ξεχωριστή, προς τη μια κατεύθυνση, ροή δεδομένων μεταξύ δύο εφαρμογών (αποστολέα και δέκτη), χαρακτηρίζεται μοναδικά από πέντε στοιχεία τα οποία είναι τα εξής: πρωτόκολλο μετάδοσης, διεύθυνση αποστολέα, αριθμός πόρτας αποστολέα, διεύθυνση παραλήπτη, αριθμός πόρτας παραλήπτη (transport protocol, source address, source port number, destination address, destination port number).
- *Ανά Ομαδοποιημένο Σύνολο - Per Aggregate*: Μια ομαδοποιημένη ροή περιλαμβάνει μια ή περισσότερες απλές ροές. Αυτές οι ροές χαρακτηρίζονται επιπλέον, πέραν από τα στοιχεία που αναφέρθηκαν ανωτέρω, από μια ετικέτα (Label) ή έναν αριθμό προτεραιότητας ή μπορεί ακόμα να περιλαμβάνει και πληροφορίες για απόδειξη γνησιότητας (authentication). Εφαρμογές, τοπολογία δικτύου και πολιτικές υπαγορεύουν ποιος τύπος της ποιότητας υπηρεσίας είναι περισσότερο κατάλληλος για μεμονωμένες ροές ή ενοποιημένες. Για την εξυπηρέτηση αυτών των διαφορετικών Ποιοτήτων Υπηρεσιών, υπάρχει ένας αριθμός διαφορετικών πρωτοκόλλων και αλγορίθμων για αυτό ακριβώς το σκοπό.
- *Πρωτόκολλο Δέσμευσης Πόρων – ReServation Protocol (RSVP)*. Παρέχει τη σηματοδοσία για την κράτηση των πόρων του δικτύου (είναι γνωστό και σαν

[35] D. Clark and J. Wroclawski, "An Approach to Service Allocation in the Internet", Internet draft , Jul. 1997

Ολοκληρωμένες Υπηρεσίες - Integrated Sendees). Μολονότι τυπικά το RSVP χρησιμοποιείται για την ανά ροή, μπορεί επίσης να χρησιμοποιηθεί και για τη δέσμευση πόρων για ενοποιημένες ροές.

Ο έντονος ανταγωνισμός οδηγεί τις εταιρείες να υιοθετήσουν νέα επιχειρηματικά μοντέλα βασισμένα στο δίκτυο και να αναπτύξουν εφαρμογές ηλεκτρονικού επιχειρείν. Σε ένα ιδιαίτερα ανταγωνιστικό περιβάλλον, οι διαχειριστές δικτύων πρέπει να είναι σε θέση να παρέχουν εγγυημένη απόδοση - ποιότητα υπηρεσιών (QoS- quality of service). Όμως, η αύξηση της κυκλοφορίας στα δίκτυα που προκαλείται από απαιτητικές εφαρμογές καθιστά πιο δύσκολη την παροχή ποιοτικών υπηρεσιών. Μια σωστή διαχείριση δικτύου για παροχή ποιότητας υπηρεσιών πρέπει να διαθέτει επαρκές εύρος ζώνης, αλλά και έξυπνη διαχείριση του εύρους ζώνης. Συνεπώς, μια σωστή διαχείριση δικτύου βάσει πολιτικών θα πρέπει να είναι σε θέση να κατανέμει κατάλληλα τους πόρους του δικτύου.

Τα συστήματα διαχείρισης QoS που βασίζονται σε πολιτικές, όπως η διαχείριση πολιτικής των Extreme Networks, επιτρέπουν στους διαχειριστές δικτύων να εφαρμόζουν το QoS όσον αφορά την απόδοση υψηλού επιπέδου και τους επιχειρηματικούς στόχους. Ένας διαχειριστής δικτύου μπορεί να ορίσει μια πολιτική που δίνει ένα εγγυημένο εύρος ζώνης και προτεραιότητα σε όσους χρήστες είναι απαραίτητο[36].

Από την οπτική γωνία ενός δικτύου που παρέχει υπηρεσίες, υπάρχουν συγκεκριμένα σημαντικά ποσοτικά χαρακτηριστικά τα οποία μπορούν να ελεγχθούν έτσι ώστε να παρέχονται συγκεκριμένα επίπεδα ποιότητας υπηρεσίας. Αυτά είναι τα παρακάτω:

- Αιτήσεις και διασυνδέσεις (Calls and Connections) Η καθυστέρηση που υφίστανται τα πακέτα λόγω της κίνησης στο δίκτυο είναι ένας σημαντικός παράγοντας που επηρεάζει αισθητά το QoS. Διάφοροι παράγοντες καθυστέρησης, έχουν διαφορετική επίδραση σε διαφορετικά είδη υπηρεσιών :
- End-to-end delay: είναι το χρονικό διάστημα της μεταφοράς του πακέτου από τον αποστολέα στον παραλήπτη, μέσω του δικτύου. Όσο πιο μεγάλο είναι το delay, τόσο πιο μεγάλη είναι η πίεση που υποβάλλεται στο πρωτόκολλο μεταφοράς για

[36] Gonia, K. (2004). Latency and QoS for voice over IP No. 21) SANs Institute.

να λειτουργήσει αποδοτικά. Για το πρωτόκολλο TCP, τα ψηλά επίπεδα καθυστέρησης υπονοούν μεγαλύτερα ποσά δεδομένων που κρατούνται στο δίκτυο εν αναμονή, πράγμα που σημαίνει ότι θα υπάρχει πίεση στους timers και στους counters που σχετίζονται με το πρωτόκολλο. Πρέπει να σημειωθεί ότι το TCP είναι ένα πρωτόκολλο με “αυτορυθμιζόμενο ρολόι". Ο ρυθμός μετάδοσης του αποστολέα προσαρμόζεται δυναμικά με την ροή των σημάτων πληροφορίας που έρχονται από τον παραλήπτη, μέσω της αντίστροφης κατεύθυνσης των acknowledgments (ACK), που ειδοποιούν τον αποστολέα ότι τα δεδομένα έχουν παραλειφθεί επιτυχώς. Όσο πιο μεγάλη είναι η καθυστέρηση μεταξύ του αποστολέα και του παραλήπτη, τόσο περισσότερο μη ευαίσθητο είναι το πρωτόκολλο σε μικρού χρονικού διαστήματος δυναμικές αλλαγές στην φόρτιση του δικτύου. Σε εφαρμογές με interactive ήχο και video, η ύπαρξη καθυστέρησης, προκαλεί μη ανταπόκριση από το σύστημα.

- Delay variation or jitter: αναφέρεται στην ποικιλία της χρονικής διάρκειας μεταξύ όλων των πακέτων της ίδιας ακολουθίας που ακολουθούν τον ίδιο router. Με μαθηματικούς όρους, το jitter μετρείται σαν η απόλυτη τιμή της πρώτης παραγώγου της ακολουθίας των ατομικών μέτρων καθυστέρησης. Πολύ ψηλά επίπεδα του jitter, προκαλεί την δημιουργία πολύ συντηρητικών υπολογισμών του round trip time από το πρωτόκολλο TCP. Το πρωτόκολλο δηλαδή δεν λειτουργεί αποδοτικά όταν επανέρχεται σε time out για να ξανά- εγκαθιδρύσει την ροή δεδομένων. Ψηλά επίπεδα jitter, δεν μπορούν να γίνουν αποδεκτά σε εφαρμογές που βασίζονται στο UDP και είναι εφαρμογές πραγματικού χρόνου, όπως για παράδειγμα το audio ή το video signal.
- Αναγκαιότητα του QoS: Μέχρι πρόσφατα τα IP δίκτυα στηρίζονταν στην υπηρεσία χωρίς σύνδεση, όπου δεν υπήρχε καμία εγγύηση σχετικά με την ποιότητα υπηρεσίας. Ενώ οι κλασικές εφαρμογές του Internet, π.χ. TELNET, FTP, WWW, SMTP, δεν έχουν κάποια απαίτηση για ποιότητα υπηρεσίας, και μπορούν να λειτουργήσουν ορθά σχεδόν υπό οποιεσδήποτε συνθήκες, κάποιες νέες εφαρμογές όπως το voice over IP, και η μετάδοση συρμών πολυμέσων (ήχου ή/και εικόνας) μέσω διαδικτύου έχουν δημιουργήσει την απαίτηση για παροχή ποιότητας υπηρεσίας από τα IP δίκτυα. Επίσης η εφαρμογή μεθόδων ποιότητας

υπηρεσίας σε αυτά τα δίκτυα μπορεί να ανοίξει νέους δρόμους στα εικονικά ιδιωτικά δίκτυα (VPN), καθώς και να επιτρέψει την ολοκλήρωση των IP δικτύων με τα υπόλοιπα δίκτυα (PSTN, ISDN, G S M).

- Ανάγκη για Policy-enabled QoS: Ένα από τα πιο βασικά θέματα που σχετίζονται με την εφαρμογή QoS είναι ο καθορισμός του συνόλου των εφαρμογών και των χρηστών που επιτρέπεται να έχουν ιδιαίτερη πρόσβαση στους δικτυακούς πόρους. Τα διαχειριστικά κριτήρια όσον αφορά την πρόσβαση στους πόρους του δικτύου αποτελούν τις δικτυακές πολιτικές. Μία πολιτική μπορεί να καθορίσει ποιες αιτήσεις θα δεχτούν καλύτερη μεταχείριση κατά τη διαδικασία ενός πρωτοκόλλου σηματοδότησης όπως το DifiServ, και να καθορίσει τις κλάσεις υπηρεσίας και τους χρήστες που πρόκειται να λάβουν μία συγκεκριμένη υπηρεσία-DLSServ.

Παρόλο που οι νέες υπηρεσίες που έχουν αναπτυχθεί σήμερα δημιουργούν μηχανισμούς για την εφαρμογή QoS, πρέπει να αναπτυχθεί και μία ρυθμιστική υποδομή έτσι ώστε οι διαχειριστές των δικτύων να μπορούν να ρυθμίζουν ποιοι χρήστες και ποιες εφαρμογές έχουν πρόσβαση σε ποιους πόρους/υπηρεσίες και υπό ποιες συνθήκες. Το RSVP επηρεάζει την εκχώρηση δικτυακών πόρων σύμφωνα με μία ανά-ροή τακτική ανάλογα με τις ποσοτικές απαιτήσεις των εφαρμογών, ενώ το DifiServ προσθέτει σημάδια στην επικεφαλίδα των IP πακέτων για να επιτρέψει την επιβολή προτεραιοτήτων σε συν-αθροίσματα κίνησης (δηλαδή «κλάσεις» από πολλαπλές ροές).

Η εφαρμογή τέτοιων υπηρεσιών εξαρτάται πάρα πολύ από την ευρεία υποδομή πολιτικής προτεραιοτήτων, η οποία θα επιτρέπει στους ISPs και στους διαχειριστές των δικτύων να ρυθμίζουν το δίκτυο παρά να διαμορφώνουν τις δικτυακές συσκευές. Για παράδειγμα, ένας ISP μπορεί να θέλει να εξασφαλίσει ότι η voice-over-IP ανατίθεται στην μικρής απώλειας και μικρής καθυστέρησης κλάση υπηρεσία, ενώ ταυτόχρονα να μειώνεται το πλήθος των ταυτόχρονα εξυπηρετούμενων voice-overIP εφαρμογών.

ΚΕΦΑΛΑΙΟ 3 - Μελέτη Περίπτωσης Διαχείρισης Δικτύων Βάσει Πολιτικών Για Σύνδεση Στο Διαδίκτυο Σε Οχήματα

Οι Joshua Hare Lance Hartun και Suman Banerjee (2012)[37], σε έρευνά τους προτείνουν την χρήση κατάλληλου πλαισίου πολιτικής (την οποία ονομάζουν Virtuoso) με σκοπό την διαχείριση ασύρματου δικτύου για οχήματα.

3.1. Εισαγωγή

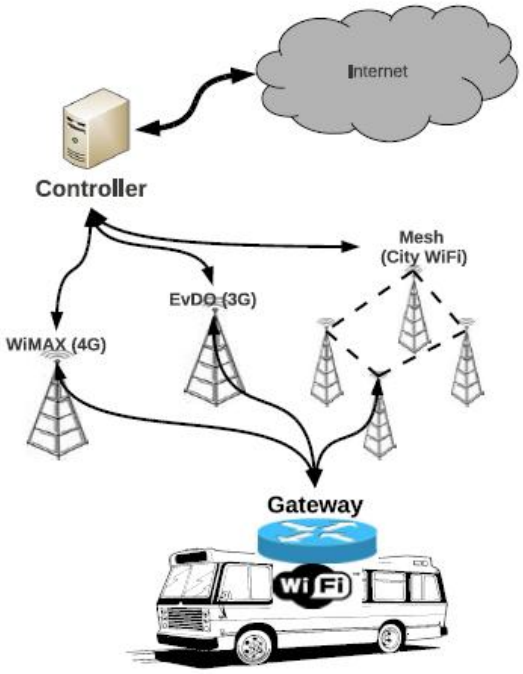
Η ζήτηση για υπηρεσίες ασύρματης πρόσβασης ευρείας περιοχής συνεχίζει να αυξάνεται με ταχείς ρυθμούς. Με την εμφάνιση εξαιρετικά ικανών και εξελιγμένων φορητών συσκευών, η ζήτηση για αυτόν τον πόρο αναμένεται να συνεχίσει να αυξάνεται με ακόμα πιο ταχείς ρυθμούς. Μια σημαντική πρόκληση που αντιμετωπίζουν οι περισσότεροι πάροχοι σχετίζεται με το να εντοπίσουν τους πιο αποτελεσματικούς τρόπους διανομής του συγκεκριμένου πόρου μεταξύ των πολλαπλών χρηστών, με διαφορετικές απαιτήσεις και προσδοκίες. Όπως συμβαίνει με κάθε περιορισμένο πόρο, ένας αποτελεσματικός τρόπος διαχείρισης του φάσματος είναι να χρησιμοποιήσουμε πολιτικές χρήσης που μεγιστοποιούν μια ειδική αντικειμενική συνάρτηση (π.χ. μια συνάρτηση χρησιμότητας).

Οι λειτουργίες χρησιμότητας, συχνά, είναι δύσκολο να προσδιοριστούν με μεγάλη ακρίβεια, καθώς η χρησιμότητα οποιωνδήποτε δεδομένων είναι μια πολύπλοκη λειτουργία που περιλαμβάνει τους χρήστες, την τοποθεσία, τον χρόνο και πολλές άλλες

[37] Joshua Hare, Lance Hartung, Suman Banerjee (2012), *Policy-Based Network Management For Generalized Vehicle-To-Internet Connectivity, Dept. of Computer Sciences, University of Wisconsin-Madison*

παραμέτρους. Στόχος, των Hare et al (2012)[38] είναι η δημιουργία ενός κοινού πλαισίου διαχείρισης ασύρματου δικτύου για χρήση σε οχήματα, βάση διαχείρισης πολιτικών.

Στην εικόνα 10, παρουσιάζεται το σύστημα «WiRover» το οποίο μπορεί να χρησιμοποιηθεί για λεωφορεία και παρέχει ταυτόχρονη σύνδεση στο internet μέσω πολλαπλών κυψελοειδών δικτύων και WiFi.



Εικόνα 10 - Επισκόπηση του συστήματος WiRover που λειτουργεί σε λεωφορεία που παρέχουν ταυτόχρονη σύνδεση στο Διαδίκτυο στους επιβάτες μέσω πολλαπλών κυψελοειδών δικτύων και WiFi

Πηγή: Hare et al, 2012

[38] Joshua Hare, Lance Hartung, Suman Banerjee (2012), *Policy-Based Network Management For Generalized Vehicle-To-Internet Connectivity, Dept. of Computer Sciences, University of Wisconsin-Madison*

3.2. Το διαδίκτυο στον τομέα της αυτοκινητοβιομηχανίας

Η δυνατότητα παροχής διαφόρων υπηρεσιών μέσω διαδικτύου, π.χ. τηλεματικής οχημάτων σε πραγματικό χρόνο, παρακολούθηση πορείας, ενημερώσεων δρόμων και καιρού, πληροφοριών πλοήγησης και άλλων μορφών ενημέρωσης, αυξάνει την αποτελεσματικότητα και την ασφάλεια των οχημάτων. Σε πολλές εγκαταστάσεις σήμερα, η συνδεσιμότητα είναι στενά ενσωματωμένη σε κάθε μεμονωμένη εφαρμογή. Για παράδειγμα, μια μονάδα πλοήγησης μπορεί να προσφερθεί με μια υπηρεσία πρόσβασης, ενώ μια ενσωματωμένη υπηρεσία έκτακτης κλήσης και εντοπισμού θέσης μπορεί να είναι προκαθορισμένη με μια διαφορετική υπηρεσία. Ωστόσο, καθώς οι ανάγκες διασύνδεσης είναι διαφορετικές (ανάλογα με την εκάστοτε εφαρμογή που χρησιμοποιεί ο χρήστης) και υπάρχει μόνο ένα σημείο πρόσβασης συνδεσιμότητας στο όχημα, υπάρχουν τουλάχιστον δύο προφανείς τρόποι για τη διασύνδεση στο Διαδίκτυο μέσω αυτών των πυλών πρόσβασης.

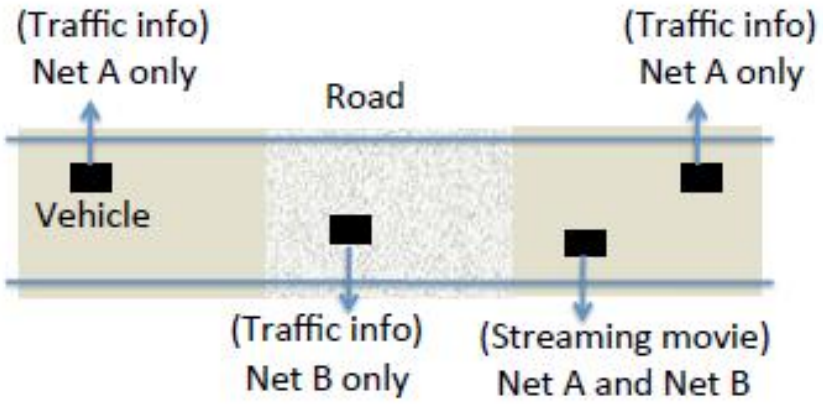
Ο πρώτος τρόπος είναι η εγγραφή στο δίκτυο από τον χρήστη. Σε αυτό το μοντέλο, η πύλη πρόσβασης σε κάθε όχημα είναι ήδη εξοπλισμένη με ένα ασύρματο μόντεμ και ο χρήστης μπορεί να χρησιμοποιεί την υπηρεσία διαδικτύου με κάποια μηνιαία χρέωση. Ο δεύτερος τρόπος είναι να χρησιμοποιήσει ο χρήστης το δικό του δίκτυο. Ωστόσο, υπάρχει μια ενδιαφέρουσα τρίτη επιλογή που προτείνουν και διερευνούν οι Hare at al(2012)[39], στο πλαίσιο, που μπορεί να θέσει τον κατασκευαστή του οχήματος (ή έναν καθορισμένο πάροχο) υπεύθυνο για τη διαχείριση των υπηρεσιών σε οχήματα.

Το μοντέλο αυτό το ονομάζουν «σύνθεση δικτύου από τον χρήστη». Σε αυτή την προσέγγιση σύνθεσης, υποθέτουμε ότι ο κατασκευαστής αυτοκινήτων (ή ένας καθορισμένος τρίτος συμβαλλόμενος) λειτουργεί ως κεντρικός πάροχος υπηρεσιών κινητών επικοινωνιών, συνάπτοντας συμφωνία παροχής δεδομένων με διάφορους παρόχους. Όταν ένας ιδιοκτήτης οχήματος θέλει να παρέχει υπηρεσίες δεδομένων, ο χρήστης λαμβάνει ένα κατάλληλο «συμβόλαιο»(συμφωνητικό) από αυτόν τον πάροχο.

[39] Joshua Hare, Lance Hartung, Suman Banerjee (2012), *Policy-Based Network Management For Generalized Vehicle-To-Internet Connectivity, Dept. of Computer Sciences, University of Wisconsin-Madison*

Υποθέτουμε ότι η πύλη πρόσβασης μπορεί να λειτουργεί μέσω των διαφορετικών κυψελοειδών δικτύων ταυτόχρονα. Αυτό, παρέχει στον πάροχο μεγάλη ευελιξία στη βελτιστοποίηση των επιδόσεων συνδεσιμότητας σε διαφορετικά οχήματα. Ένα όχημα είναι πιθανό να έχει εύκολη σύνδεση με διαφορετικά δίκτυα με βάση τις ιστορικές πληροφορίες για την απόδοση αυτών των δικτύων.

Όπως φαίνεται στην εικόνα 11, το μεσαίο τμήμα του δρόμου μπορεί να μην έχει καλή συνδεσιμότητα με κάποιον πάροχο (Net A), και επομένως όταν ένα όχημα διέρχεται από αυτή την περιοχή, το όχημα προσεγγίζει το Διαδίκτυο μόνο μέσω του δικτύου του παρόχου Net B. Σε άλλες περιπτώσεις, ο πάροχος ενδέχεται να προτιμά να χρησιμοποιεί το δίκτυο A για οχήματα (ίσως λόγω των χαμηλότερων ρυθμών μετάδοσης δεδομένων του δικύου A γενικά). Η πολυμορφία και ο συνδυασμός των δικτύων μπορούν έτσι να χρησιμοποιηθούν με πολλούς ενδιαφέροντες τρόπους από τον πάροχο για να καλύψουν διάφορες ανάγκες απόδοσης.



Εικόνα 11 - Πολλαπλά οχήματα (τα μαύρα τετράγωνα) σε έναν δρόμο χωρισμένα σε τρία αυθαίρετα τμήματα. Ένας πάροχος μπορεί να διαχειριστεί τους πόρους εύρους ζώνης σε ένα σύνολο οχημάτων προσαρμοσμένων στις ανάγκες εύρους ζώνης εφαρμογής.

Εφαρμογή πολιτικών διαχείρισης στο προτεινόμενο σύστημα WiRover

Το προτεινόμενο σύστημα WiRover αποτελείται από μια πύλη πρόσβασης τοποθετημένη στο όχημα που είναι εξοπλισμένο με πολλαπλούς ασύρματους δέκτες πρόσβασης δικτύου για τη σύνδεση σε διαφορετικά κυψελοειδή και ασύρματα δίκτυα στην περιοχή, ταυτόχρονα, όταν είναι εφικτό (Εικόνα 12). Οι επιβάτες μπορούν να έχουν πρόσβαση σε υπηρεσίες Διαδικτύου, συνδέοντας την πύλη μέσω WiFi. Επιπλέον, διάφορες υπηρεσίες οχημάτων (π.χ. τηλεματικές, ηλεκτρονικές οθόνες κ.λπ.) μπορούν επίσης να συνδεθούν στην πύλη μέσω Bluetooth, WiFi ή Ethernet. Η εμπειρία ανάπτυξης έφερε στο προσκήνιο διάφορες προκλήσεις και απαιτήσεις διαχείρισης εύρους ζώνης και διαχείρισης δεδομένων. Τα παρακάτω είναι μερικά παραδείγματα.

- Διατήρηση των ορίων δεδομένων: Η υπηρεσία WiFi που παρέχεται στους επιβάτες λεωφορείων είναι ελεύθερα διαθέσιμη σε όλους. Κάτω από τέτοια σενάρια, πολλοί επιβάτες μπορούν να δημιουργήσουν μια σχετική ζήτηση. Εάν η ζήτηση είναι μεγάλη τότε τα όρια των μηνιαίων δεδομένων θα ξεπεραστούν εύκολα οδηγώντας σε υψηλά και μεταβλητά κόστη για τη λειτουργία αυτών των συστημάτων .

Επομένως, μια βασική απαίτηση για το παραπάνω σύστημα είναι να διασφαλιστεί ότι η χρήση του διαδικτύου από τους επιβάτες των λεωφορείων δεν θα ξεπερνά τα διαθέσιμα όρια δεδομένων. Φυσικά, ένας απλός τρόπος για να εφαρμοστεί αυτό είναι να επιβληθούν αυστηροί κανόνες κατά την υπέρβαση ορισμένων ορίων. Ωστόσο, απαιτείται μια προσέγγιση διαμόρφωσης και διαχείρισης η οποία θα ικανοποιεί όλους τους επιβάτες. Για παράδειγμα, μια καλή προσέγγιση θα ήταν ο εντοπισμός, μέσω mac address των συσκευών, των επιβατών που χρησιμοποιούν αρκετό όγκο δεδομένων και ο περιορισμός χρήσης τους στα δεδομένα διαδικτύου, καθολικά ή βάζοντας ένα όριο ημερήσιας χρήσης.

Δεδομένου ότι κάθε πύλη είναι εξοπλισμένη ώστε να συνδέεται ταυτόχρονα σε πολλά δίκτυα, αυτή η διαδικασία θα μπορούσε εύκολα να συνδυαστεί με αποφάσεις αλλαγής της χρήσης δικτύων όταν αυτό είναι αναγκαίο.

- Σχέδια κοινών δεδομένων: Μια πιο ενδιαφέρουσα εκδοχή του προβλήματος αυτού προκύπτει όταν ορισμένα οχήματα μπορούν να μοιραστούν ένα κοινό σχέδιο δεδομένων. Για παράδειγμα, εάν ένα σύνολο 100 λεωφορείων έχει αθροιστικά μηνιαίο

όριο 500 GB για κάθε δίκτυο που χρησιμοποιείται, τότε θα πρέπει να σχεδιαστούν αποτελεσματικοί τρόποι διαχείρισης του συνόλου αυτών των δεδομένων σε όλα τα οχήματα. Αυτό φέρνει μια ολόκληρη νέα διάσταση στην κατανομή και διαχείριση δεδομένων.

- Αξία των δεδομένων: Είναι σαφές ότι ο σκοπός χρήσης των δεδομένων δεν είναι πάντα ο ίδιος. Οι ροές που μεταφέρουν δεδομένα διαγνωστικού και τηλεματικού οχήματος σε κεντρική εφαρμογή παρακολούθησης είναι πιο σημαντικές από τις ενδεχομένως πιθανές αναρτήσεις στα social media (Facebook, instagram κλπ.) που θα αποστέλλονται από τους επιβάτες. Σε ορισμένες περιπτώσεις, τα δεδομένα σε πραγματικό χρόνο από τις κάμερες ασφαλείας που είναι τοποθετημένες στα λεωφορεία μπορεί να είναι ακόμη πιο σημαντικά. Επομένως, όταν το σύστημα εφαρμόζει τα καθορισμένα όρια των δεδομένων, θα πρέπει να εξετάζει πρώτα τον σκοπό χρήσης των δεδομένων.

Γενικά, οι διαχειριστές πρέπει να είναι σε θέση να σχεδιάζουν και να ενημερώνουν με σαφήνεια αυτές τις πολιτικές που καθορίζουν τον τρόπο χειρισμού των διαφόρων ειδών.

- Φιλτράρισμα περιεχομένου: Βασικό αίτημα των ιδιοκτητών λεωφορείων είναι να διασφαλιστεί ότι οι επιβάτες δεν θα μπορούσαν να κατεβάσουν ακατάλληλο περιεχόμενο, βίντεο που υποκινούν βία ή ακόμα και ολόκληρες ταινίες κατά τη διάρκεια μιας διαδρομής, το οποίο και διασφαλίζεται με συγκεκριμένη πολιτική φιλτραρίσματος των urls.

Για να αντιμετωπιστούν όλες οι παραπάνω απαιτήσεις με τρόπο ευέλικτο και να μπορέσει να δοθεί η δυνατότητα στους διαχειριστές της να διαχειρίζονται αποτελεσματικά το εύρος ζώνης και τους πόρους δεδομένων του διαδικτύου, προτείνεται ένα πλαίσιο πολιτικής το οποίο οι ερευνητές Hare et al (2012)[40] ονομάζουν «Virtuoso». Πρόκειται για μια κεντρική δομή διαχείρισης μέσω της οποίας οι διαχειριστές μπορούν να εισάγουν όλες τις πολιτικές σε πολλαπλά επίπεδα, όπως πύλες, δίκτυα, εφαρμογές και διάφορα μηνύματα τα οποία στέλνονται από/προς κάθε πύλη.

[40] Joshua Hare, Lance Hartung, Suman Banerjee (2012), *Policy-Based Network Management For Generalized Vehicle-To-Internet Connectivity, Dept. of Computer Sciences, University of Wisconsin-Madison*

Μέσω αυτού του πλαισίου, οι καθολικές πολιτικές καθορίζονται από τον διαχειριστή, οι οποίες μεταφράζονται σε διάφορες τοπικές πολιτικές και μεταφορτώνονται και εκτελούνται με δυναμικό τρόπο.

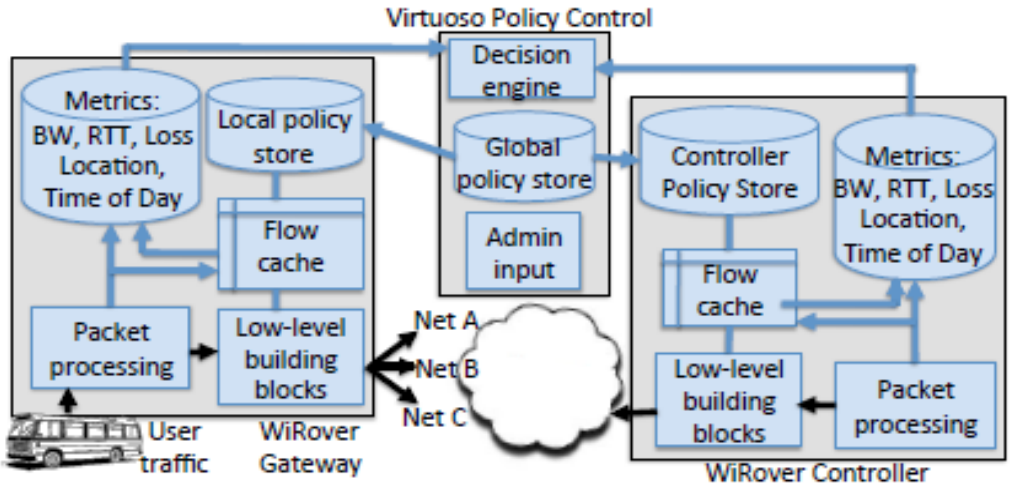
Το πλαίσιο πολιτικής «Virtuoso» εξουσιοδοτεί τον πάροχο να διαχειρίζεται τα δεδομένα και τους πόρους εύρους ζώνης σε όλους τους χρήστες (οχήματα/λεωφορεία). Εφαρμόζεται ως υπηρεσία με τεχνολογία cloud (υπολογιστικό νέφος). Όλες οι πολιτικές που καθορίζονται από τον πάροχο εισάγονται μέσω ειδικής δι-επαφής διαδικτύου. Ένας μηχανισμός απόφασης μεταφράζεται σε συγκεκριμένες πολιτικές σε επίπεδο πύλης και ελεγκτή.

Για παράδειγμα, ο διαχειριστής μπορεί να θέλει να εφαρμόσει μια πολιτική ως εξής:

Εάν η συνολική χρήση δεδομένων στο δίκτυο A σε όλα τα οχήματα υπερβαίνει τα 200 GB (όταν το όριο είναι 250 GB), τότε να περιοριστούν όλοι οι χρήστες σε ταχύτητα 50 Kbps, ενώ δεν επιθυμεί να επιβάλλει περιορισμούς για εφαρμογές που χρησιμοποιούν σύστημα πλοήγησης.

Αυτή η πολιτική θα μεταφραστεί σε διάφορες τοπικές πολιτικές (στους δρομολογητές των οχημάτων δηλαδή) που ενεργοποιούνται σε διαφορετικές χρονικές στιγμές. Στην αρχή του μήνα, δεν υπάρχει κανένα όριο για τους χρήστες, ωστόσο, μόλις επιτευχθεί το όριο των 200 GB, κάθε δρομολογητής έχει την εντολή να διαμορφώσει το tracts που συσσωρεύονται ανά χρήστη στο όριο των 50 Kbps. Αυτή η πολιτική αφαιρείται στην αρχή του επόμενου μήνα.

Στην εικόνα 12 παρουσιάζεται το προτεινόμενο μοντέλο «virtuoso» για την διαχείριση δικτύων βάσει πολιτικής σε οχήματα.



Εικόνα 12 - Επισκόπηση της λειτουργίας του προτεινόμενου μοντέλου «virtuoso». Επικοινωνία με τις πύλες του WiRover(των οχημάτων) και έλεγχος των υπο-συστημάτων

Στην εικόνα 13 παρουσιάζονται ορισμένα παραδείγματα της σύνταξης των πολιτικών για την εφαρμογή του μοντέλου «virtuoso».

Type	Command	Notes
Limit user	policy –src 10.0.0.1 –limit 200K	Limit user at 10.0.0.1 (for a given gateway) to a 200Kbps limit
Limit dest.	policy –dst youtube.com –limit 200K	Limit all YouTube traffic from this gateway to 200 Kbps
Limit network	policy –net Verizon –limit 200K	Limit all traffic using the Verizon network to 200 Kbps
Block an app	policy –drop –app torrent	Block all BitTorrent traffic on this gateway
Link Selection	policy –link WiFi –app video	All video traffic should only be sent over WiFi links
Set priority	policy –priority high –app music	All flows carrying music content has the highest scheduling priority
Packet striping	policy –bwagg Verizon,Sprint –proto TCP –dport 20	All TCP flows using port 20 should be striped across the two specific cellular networks

Εικόνα 13 - Παραδείγματα σύνταξης πολιτικών διαχείρισης για το προτεινόμενο μοντέλο virtuoso

Πηγή:Hare et al (2012)

Επίλογος - Μελλοντικές εξελίξεις

Οι νέες τεχνολογίες αναπτύσσονται για τη δημιουργία δικτύων με στόχο την υποστήριξη των αυξανόμενων απαιτήσεων των εφαρμογών δικτύου και των αναγκών του αυξανόμενου αριθμού των χρηστών. Ωστόσο, αν και το κόστος του υλικού για την κατασκευή ταχύτερων, πιο αξιόπιστων δικτύων μειώθηκε με την πάροδο του χρόνου, το κόστος διαχείρισης των σύγχρονων πολύπλοκων δικτυακών υποδομών δεν μειώνεται με παρόμοιο ρυθμό. Αυτό οφείλεται στο γεγονός ότι η διαχείριση του δικτύου παραμένει ένα δύσκολο έργο, απαιτώντας σημαντική προσπάθεια από πολλούς αρμόδιους διαχειριστές δικτύου. (Wasserman, 2017)[41]

Η αυτοματοποίηση, η απλοποίηση και η δια-λειτουργικότητα των λύσεων διαχείρισης δικτύων αποτελούν βασικούς παράγοντες που θα βοηθήσουν τους διαχειριστές να εκτελούν τα καθήκοντά τους πιο εύκολα και αποτελεσματικά και, συνεπώς, θα μειώσουν το κόστος διαχείρισης των σύγχρονων δικτύων.

Η διαχείριση με βάση την πολιτική κερδίζει όλο και περισσότερο την προσοχή της βιομηχανίας και του ακαδημαϊκού κόσμου ως μια ελπιδοφόρα λύση για την αυτοματοποίηση και την απλούστευση του έργου διαχείρισης. Εντούτοις, δεν υπάρχουν καθιερωμένες γλώσσες πολιτικής, τα πρότυπα μοντέλα πληροφοριών πολιτικής από την IETF και την DMTF έχουν περιορισμούς και είναι δύσκολο να χρησιμοποιηθούν, ενώ τα εργαλεία εμπορικής πολιτικής δεν υποστηρίζουν ακόμη υψηλό βαθμό αυτοματοποίησης και πλήρη δια-λειτουργικότητα.

Επίσης, ο τομέας της προσαρμογής των πολιτικών εξακολουθεί να χρειάζεται περαιτέρω διερεύνηση. Οι ιδέες που παρουσιάζονται στην βιβλιογραφία παρέχουν λύσεις για την προσαρμογή των πολιτικών σε επίπεδο δικτύου σύμφωνα με τις αλλαγές στις απαιτήσεις εφαρμογής και τα συμβάντα που υποδεικνύουν αποτυχίες δικτύου ή προβλήματα που παρέχουν υπηρεσίες στα επιθυμητά επίπεδα. Οι ίδιες έννοιες θα μπορούσαν να χρησιμοποιηθούν για την προσαρμογή των πολιτικών όταν καθορίζονται

[41] M. Wasserman, S. Hartman, D. Zhang(2017), Security analysis of the open networking foundation (onf) openflow switch specification, Internet-Draft draft-mrw-sdnsec-openflowanalysis-00, informational

πολιτικές σε επίπεδο εφαρμογής. Σε αυτήν την περίπτωση, οι εφαρμογές που υποστηρίζουν πολιτικές, τις ερμηνεύουν για να προσαρμόζουν τη συμπεριφορά τους ανάλογα με τα γεγονότα που λαμβάνουν από το δίκτυο, όπως το διαθέσιμο εύρος ζώνης ή σύμφωνα με τις απαιτήσεις συγκεκριμένων χρηστών, όπως ποιες πληροφορίες πρέπει να φιλτράρονται όταν το εύρος ζώνης ή οι δυνατότητες συσκευών είναι περιορισμένες.

Πρέπει να ληφθεί υπόψιν ότι ορισμένες από τις πολιτικές που αφορούν συγκεκριμένες εφαρμογές ενδέχεται να χρειαστεί να εφαρμοστούν εντός του δικτύου. Επομένως, οι εφαρμογές με ενεργοποιημένη πολιτική πρέπει να είναι σε θέση να μεταφέρουν πολιτικές στο δίκτυο. Αντίθετα, το δίκτυο ίσως χρειαστεί να μεταβιβάσει πολιτικές που θα ερμηνευτούν από την εφαρμογή για πιο αποτελεσματική προσαρμογή, για παράδειγμα σχετικά με την προσωρινή αποθήκευση ή την παρακολούθηση εξαρτημάτων που εξαρτώνται από την εφαρμογή. (Gozalvez, 2016)[42]

Έτσι, είναι απαραίτητο να αναπτυχθούν τεχνικές και δι-επαφές για την αλληλεπίδραση μεταξύ των εφαρμογών που βασίζονται στην πολιτική και των δικτύων με δυνατότητα χάραξης πολιτικής, προκειμένου να ανταλλάσσονται πληροφορίες πολιτικής. Απαιτείται σημαντική έρευνα για τη διερεύνηση της χρήσης μηχανισμών αυτοδιδασκαλίας για να διαπιστωθεί ποιες είναι οι καταλληλότερες στρατηγικές διαμόρφωσης πολιτικής από τη συμπεριφορά του συστήματος. Αυτό μπορεί να χρησιμοποιηθεί για να βελτιώσει τη λειτουργικότητα του συστήματος προσαρμογής πολιτικής για να επιλέξει πολιτικές ή να δημιουργήσει νέες όταν χρειάζεται.

[42] J. Gozalvez, M. C. Lucas-Estan, J. Sanchez-Soriano, ˜ Joint radio resource management for heterogeneous wireless systems, Wirel. Netw. 18 (4) (2016) 443–455

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Boutaba R., Polyrakis A(2001), COPS-PR with Meta-Policy Support, IETF Internet Draft, May
2. Bellavista P., Corradi A., Stefanelli C.(2010), An Integrated Management Environment for Network Resources and Services. IEEE Journal on Selected Areas in Communications, Vol. 18, No. 5
3. E. Bertino *et al.*, "Analysis of privacy and security policies," *IBM J. Res. Develop.*, vol. 53, no. 2, pp. 3:1–3:18, Mar. 2009. [21] S. Lange *et al.*, "Heuristic approaches to the controller
4. D. C. Verma, *Policy-Based Networking: Architecture and Algorithms*. Indianapolis, IN, USA: New Riders Publ., 2000.
5. Movahedi, Ayari, Langar, Pujolle "A Survey of Autonomic Network Architectures and Evaluation Criteria", in *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 464-490, Second Quarter 2012
6. Dulay, N., E. Lupu, M. Sloman and N. Damianou (2001). A Policy Deployment Model for the Ponder Language. In Proceedings of the IM 2001: 7th IEEE/IFIP International Symposium on Intergrated Network Management, Seattle, USA, 14-18 May 2001, pp. 529-544.
7. Barath Raghavan, Kashi Vishwanath, Sriram Ramabhadran, Kenneth Yocum, and Alex C. Snoeren. Cloud control with distributed rate limiting. In ACM Sigcomm, 2007.
8. Dulay, N., E. Lupu, M. Sloman and N. Damianou (2001). A Policy Deployment Model for the Ponder Language. In Proceedings of the IM 2001: 7th IEEE/IFIP International Symposium on Intergrated Network Management, Seattle, USA, 14-18 May 2001, pp. 529-544.
9. E. Bertino *et al.*, "Analysis of privacy and security policies," *IBM J. Res. Develop.*, vol. 53, no. 2, pp. 3:1–3:18, Mar. 2009. [21] S. Lange *et al.*, "Heuristic approaches to the controller

10. Taureck, R., (2006) Securitization theory – The Story So Far: Theoretical inheritance and what it means to be a post-structural realist. Paper presented at the 4th annual CEEISA convention, University of Tartu, 25-27 June.
11. Ju H., Choi M., Hong J(2011), EWS-Based Management Application Interface and Integration Mechanisms for Web-Based Element Management, Journal of Network and Systems Management, Vol.9, No.1
12. Carlos A. Astudillo, Graduate Student Member, IEEE, Adriana M. Gustin, Graduate Student Member, IEEE and Oscar J. Calderón, Member, IEEE(2010) Policy Creation Model for Policy-Based Management in Telecommunications Networks
13. Carlos A. Astudillo, Graduate Student Member, IEEE, Adriana M. Gustin, Graduate Student Member, IEEE and Oscar J. Calderón, Member, IEEE(2010) Policy Creation Model for Policy-Based Management in Telecommunications Networks
14. J. Pérez-Romero, O. Sallent, R. Ferrús, R. Agustí, "Knowledge-based 5G Radio Access Network Planning and Optimization", The Thirteenth International Symposium on Wireless Communication Systems (ISWCS-2016), Poznan, Poland, September, 2016.
15. Movahedi, Ayari, Langar, Pujolle "A Survey of Autonomic Network Architectures and Evaluation Criteria", in *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 464-490, Second Quarter 2012
16. Movahedi, Ayari, Langar, Pujolle "A Survey of Autonomic Network Architectures and Evaluation Criteria", in *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 464-490, Second Quarter 2012
17. Chan, K., D. Durham, S. Gai, S. Herzog, K. McCloghrie, F. Reichmeyer, J. Seligson, A. Smith and R. Yavatkar (2001), *COPS Usage for Policy Provisioning*, *RFC 3084*, March 2001.
18. Mahon,(2002) H. *Requirements for a Policy Management System*. IETF Internet draft work in progress, Available from http://www.ietf.org, 22 October

19. Ortalo R. (2001), *A Flexible Method for Information System Security Policy Specification*. In Proceedings of 5th European Symposium on Research in Computer Security (ESORICS98). 1998. Louvain-la-Neuve, Belgium, Springer-Verlag.

20. R. Craven *et al.*, "Expressive policy analysis with enhanced system dynamicity," in *Proc. 4th ASIACCS*, New York, NY, USA, 2009, pp. 239–250.

21. Moore, B., E. Ellesson, J. Strassner and A. Westerinen (2001), Policy Core Information Model -- Version 1 Specification, RFC 3060, February 2001.

22. Geffner, H., and Boner, B. 1998. High-level planning and control with incomplete information using POMDP's. In *working notes of the AAAI faU symposium on Cognitive Robotics.*

23. Strassner, J., A. Westerinen, E. Ellesson, B. Moore and R. Moats (2001), Policy Core LDAP Schema, Internet Draft, draft-ietf-policy-core-schema-11.txt, May 2001.

24. Strassner, J., A. Westerinen and B. Moore (2001), Information Model for Describing Network Device QoS Datapath Mechanisms, Internet Draft, draft-ietf-policy-qos-deviceinfo-model-03.txt, May 2001.

25. Chan, K., D. Durham, S. Gai, S. Herzog, K. McCloghrie, F. Reichmeyer, J. Seligson, A. Smith and R. Yavatkar (2001), *COPS Usage for Policy Provisioning, RFC 3084*, March 2001.

26. Dulay, N., E. Lupu, M. Sloman and N. Damianou (2001). A Policy Deployment Model for the Ponder Language. In Proceedings of the IM 2001: 7th IEEE/IFIP International Symposium on Intergrated Network Management, Seattle, USA, 14-18 May 2001, pp. 529-544.

27. Moore, B., E. Ellesson, J. Strassner and A. Westerinen (2001), Policy Core Information Model -- Version 1 Specification, RFC 3060, February 2001.

28. Neisse, P. D. Costa, M. Wegdam, and M. van Sinderen(2008), "An information model and architecture for context-aware management domains." in POLICY.

IEEE Computer Society, 2008, pp. 162–169. [Online]. Available: http://dblp.uni-trier. de/db/conf/policy/ policy2008.html#NeisseCWS08

29. G. Russello, C. Dong, and N. Dulay,(2007) “Authorization and conflict resolution for hierarchical domains,” in 8th IEEE Int. Workshop on Policies for Distributed Systems and Networks(POLICY), Bologna, Italy, 2007, pp. 201–210.
30. G. Russello, C. Dong, and N. Dulay,(2007) “Authorization and conflict resolution for hierarchical domains,” in 8th IEEE Int. Workshop on Policies for Distributed Systems and Networks(POLICY), Bologna, Italy, 2007, pp. 201–210.
31. Kagal, L., Finin, T., & Joshi, A. (2003). A policy-based approach to security for the Semantic Web. In D. Fensel, K. Sycara, & J. Mylopoulos (Ed.), *The Semantic Web—ISWC 2003. Proceedings of the Second International Semantic Web Conference, Sanibel Island, Florida, USA, October 2003, LNCS 2870.* (pp. 402-418).: Springer.
32. Uszok, A., Bradshaw, J. M., Jeffers, R., Suri, N., Hayes, P., Breedy, M. R., Bunch, L., Johnson, M., Kulkarni, S., & Lott, J. (2003). KAoS policy and domain services: Toward a description-logic approach to policy representation, deconfliction, and enforcement. *Proceedings of Policy 2003*. Como, Italy
33. Uszok, A., Bradshaw, J. M., Jeffers, R., Suri, N., Hayes, P., Breedy, M. R., Bunch, L., Johnson, M., Kulkarni, S., & Lott, J. (2003). KAoS policy and domain services: Toward a description-logic approach to policy representation, deconfliction, and enforcement. *Proceedings of Policy 2003*. Como, Italy
34. Bradshaw, J. M., Uszok, A., Jeffers, R., Suri, N., Hayes, P., Burstein, M. H., Acquisti, A., Benyo, B., Breedy, M. R., Carvalho, M., Diller, D., Johnson, M., Kulkarni, S., Lott, J., Sierhuis, M., & Van Hoof, R. (2003). Representation and reasoning for DAML-based policy and domain services in KAoS and Nomads. *Proceedings of the Autonomous Agents and Multi-Agent Systems Conference (AAMAS 2003)*. Melbourne, Australia, New York, NY: ACM Press
35. D. Clark and J. Wroclawski, "An Approach to Service Allocation in the Internet", Internet draft , Jul. 1997
36. Gonia, K. (2004). Latency and QoS for voice over IP No. 21) SANs Institute

37. R. Craven *et al.*, “Expressive policy analysis with enhanced system dynamicity,” in *Proc. 4th ASIACCS*, New York, NY, USA, 2009, pp. 239–250.
38. Joshua Hare, Lance Hartung, Suman Banerjee (2012), *Policy-Based Network Management For Generalized Vehicle-To-Internet Connectivity, Dept. of Computer Sciences, University of Wisconsin-Madison*
39. Joshua Hare, Lance Hartung, Suman Banerjee (2012), *Policy-Based Network Management For Generalized Vehicle-To-Internet Connectivity, Dept. of Computer Sciences, University of Wisconsin-Madison*
40. Joshua Hare, Lance Hartung, Suman Banerjee (2012), *Policy-Based Network Management For Generalized Vehicle-To-Internet Connectivity, Dept. of Computer Sciences, University of Wisconsin-Madison*
41. Joshua Hare, Lance Hartung, Suman Banerjee (2012), *Policy-Based Network Management For Generalized Vehicle-To-Internet Connectivity, Dept. of Computer Sciences, University of Wisconsin-Madison*
42. M. Wasserman, S. Hartman, D. Zhang(2017), Security analysis of the open networking foundation (onf) openflow switch specification, Internet-Draft draft-mrw-sdnsec-openflowanalysis-00, informational.
43. J. Gozalvez, M. C. Lucas-Estan, J. Sanchez-Soriano, ˜ Joint radio resource management for heterogeneous wireless systems, Wirel. Netw. 18 (4) (2016) 443–455
44. B. Pfaff, J. Pettit, K. Amidon, M. Casado, T. Koponen and S. Shenker (2009). Extending Networking into the Virtualization Layer, In Hotnets.
45. M. Bari, S. Chowdhury, R. Ahmed, and R. Boutaba, “Policy Cop: An autonomic QoS policy enforcement framework for software defined networks,” in *Proc. IEEE SDN Future Netw. Serv. (SDN4FNS)*, Trento, Italy, Nov. 2013, pp. 1–7.
46. S.A. de Chaves, C.B. Westphall, and F.R Lamin, “SLA Perspective in Security Management for Cloud Computing,” in *Proc. of Sixth International Conference on Networking and Services (ICNS), 2010*, pp. 212-217.
47. J. S. Turner and D. E. Taylor (2005). Diversifying the Internet. In *IEEE Global Telecommunications Conference (GLOBECOM')*, volume 2.

48. E. Haleplidis, K. Pentikousis, S. Denazis, J. H. Salim, D. Meyer and O. Koufopavlou (2015). Software-Defined Networking (SDN): Layers and Architecture Terminology. Technical report.

49. K. Giotis, C. Argyropoulos, G. Androulidakis, D. Kalogeras and V. Maglaris (2014). Combining OpenFlow and sFlow for an Effective and Scalable Anomaly Detection and Mitigation Mechanism on SDN Environments. *Computer Networks*, 62:122-136.

50. Mell and T. Grance (2011). The NIST Definition of Cloud Computing. Technical Report 800-145, National Institute of Standards and Technology (NIST).

51. Grozev N. and R. Buyya (2014). Inter-cloud architectures and application brokering: taxonomy and survey. *Software: Practice and Experience,* 44(3):369-390.

52. J. Roberts (2009). The Clean-Slate Approach to Future Internet Design: a Survey of Research Initiatives, *annals of telecommunications*, 64(5-6):271-276.

53. Magedanz and S. Wahle (2009). Control Framework Design for Future Internet Testbeds. *Elektrotechnik & Informationstechnik*, 126(7-8):274-279.

54. Nichols, K., S. Blake, F. Baker and D. Black (1998), Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, RFC 2474, December 1998.

55. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker and J. Turner (2008). OpenFlow: Enabling Innovation in Campus Networks. *ACM SIGCOMM Computer Communication Review,* 38(2):69-74.

56. Petcu, B. Di Martino, S. Venticinque, M. Rak, T. M3hr, G. E. Lopez, F. Brito, R. Cossu, M. Stopar, S. $perka, et al. (2013). Experiences in building a mOSAIC of clouds. *Journal of Cloud Computing: Advances, Systems and Applications*, 2(1):12.

57. Villegas, N. Bobroff, I. Rodero, J. Delgado, Y. Liu, A. Devarakonda, L. Fong,

58. S. M. Sadjadi and M. Parashar (2012). Cloud Federation in a Layered Service Model. *Journal of Computer and System Sciences,* 78(5):1330-1344.

59. Balay, S Abhyankar, S., Adams, M., Brown, J., Brune, P., Buschelman, K. & Knepley M. (2017). *PETSc Users Manual Revision 3.8* (No. ANL-95/11 Rev 3.8). Argonne National Lab.(ANL), Argonne, IL (United States).
60. W3C.(2017) Policies and Legal Information.[Online] Available from: https://www.w3.org/Consortium/Legal/2002/ipr-notice-20021231[Accessed 19-2-2018]
61. Bitter, R., Mohiuddin. T., & Nawrocki, M. (2017): LabVIEW : Advanced programming techniques Crc Press.
62. Bond, A. H., & Gasser L. (Eds.). (2014) Readings in distributed artificial intelligence Morfan Kaufmann.
63. De Faria, S. M. M. (2014). A dynamic event processing framework for high performance streams.
64. Decyk, V. K. (2015). Introduction to object-oriented concepts using Fortran90.
65. Deshmukh, M. Weps, B. Isidro, P., & Gerndt A (2015, March). Model driven language framework to automate command and data handling code generation. In Aerospace Conference, 2015 IEEE (pp. 1-9). IEEE.
66. Giachetti, R. E. (2016) Design of enterprise systems : Theory, architecture, and methods, CRC Press.
67. Harper, R. (2016) Practical foundations for programming languages. Cambridge University Press.
68. Hasu, T. (2017). Programming Language Technology for Niche Platforms.
69. Kirk, D. B., & Wen-Mei, W. H. (2016) Programming massively parallel processors: a hands-on approach. Morgan Kaufmann.
70. Morris, J. G. (2016, September). The best of both worlds: linear functional programming without compromise. In ACM SIGPLAN Notices (Vol. 51, No 9, pp. 448-461). ACM.

71. Patterson, D., Perconti, J., Dimoulas, C., & Ahmed, A. (2017). FunTAL: Reasonably mixing a functional language with assembly. ACM SIGPLAN Notices, 52(6), 495-509.

72. Protzenko, J., Zinzindohoué, J. K., Rastogi, A., Ramananandro, T., Wang, P., Zanella – Beguellin, S., ... & Swamy, N. (2017). Verified low-level programming embedded in F. Proceedings of the ACM on Programming Languages, (ICFP), 17.

ΔΙΚΤΥΟΓΡΑΦΙΑ – ΣΥΝΔΕΣΜΟΙ

https://www.ip.gr/el/dictionary/38-Security_Policy

http://www.conta.uom.gr/conta/ekpaideysh/metaptyxiaka/technologies_diktywn/teaching_m/management/netmanage.htm

http://www.netmode.ntua.gr/main/index.php?option=com_content&view=article&id=17&Itemid=49

http://www.ittoday.info/Articles/Policy-Based_Network_Management/Policy-Based_Network_Management.htm

http://prod.sandia.gov/techlib/access-control.cgi/2004/043254.pdf

https://www.networkworld.com/article/3209131/lan-wan/what-sdn-is-and-where-its-going.html

https://www.webopedia.com/TERM/S/software_defined_networking.html

https://www.sdxcentral.com/sdn/definitions/what-the-definition-of-software-defined-networking-sdn/

https://docs.microsoft.com/en-us/windows-server/networking/sdn/software-defined-networking

http://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS

https://www.techopedia.com/definition/30455/cloud-infrastructure

https://www.emc.com/corporate/glossary/cloud-infrastructure.htm

http://searchcloudcomputing.techtarget.com/definition/cloud-infrastructure

https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/

https://www.sdxcentral.com/nfv/definitions/whats-network-functions-virtualization-nfv/

https://www.sdxcentral.com/articles/contributed/nfv-and-sdn-whats-the-difference/2013/03/

http://searchsdn.techtarget.com/definition/network-functions-virtualization-NFV

https://www.cisco.com/c/en/us/solutions/service-provider/network-functions-virtualization-nfv/index.html

https://5g-ppp.eu/wp-content/uploads/2017/03/NetworkManagement_WhitePaper_1.pdf

https://5g-ppp.eu/cognative-network-management-for-5g/