Τα εικονικά τοπικά δίκτυα και η χρήση τους στα πανεπιστημιακά δίκτυα

Virtual Local Access Networks and How They Are Used in Campus Networks

Zisis K. Katsavelis

mis1112@uom.gr

Πανεπιστήμιο Μακεδονίας

ΔΠΜΣ Πληροφοριακά Συστήματα
Δίκτυα Υπολογιστών

Καθηγητής: Α.Α. Οικονομίδης

University of Macedonia

Master Information Systems
Computer Networks

Professor: A.A. Economides

February 2012

I. ΠΕΡΙΛΗΨΗ

Τα εικονικά δίκτυα (VLANS) χρησιμοποιούνται ευρέως σημέρα σε μεγάλα δίκτυα και κυρίως στα εσωτερικά δίκτυα των πανεπιστήμιων. Παρόλο που αναπτύχθηκαν κυρίως για άλλους λόγους οι διαχειριστές των πανεπιστημιακών δικτύων κάνουν εκτεταμένη χρήση τους προσπαθόντας να διαχειριστούν, επιλύσουν,να παραμετροποιήσουν και να αξιοποιήσουν στο έπαρκο τις δυνατότητες του δικτυού τους και του εξοπλισμού τους. Η χρήση όμως των εικονικών δικτύων, εκτός από τα προτερήματα που δίνει στους διαχειριστές δημιουργεί και πολλά προβλήματα ακριβώς γιατί δεν είχαν σχεδιαστεί για τον σκοπό αυτό. Η παρεμετροποίηση του δικτύου, η εφαρμογή κανόνων (π.χ. QOS) και ο σχεδιασμός του δικτύου μπορεί να γίνει μια ιδιαίτερα επίπονη διαδικασία για αυτό τον λόγο επιστρατεύονται τα εικονικά δίκτυα. Όμως και ο χειρισμός αυτών δεν είναι ιδιαίτερα εύκολος καθώς οι λύσεις που έχουν στα χέρια τους οι διαχειριστές είναι λίγες και κατά κύριο λόγο από μεγάλες εταιρείες που δραστηροπιούνται στον χώρο αφού η ακαδημαική έρευνα δεν έχει προχωρήσει ιδιαίτερα σε αυτό το χώρο.

I. ABSTRACT

VLANs are widely used in today’s enterprise and campus networks. Although VLANs have been developed for other purposes, network administrators in campuses are extensively use them in managing, troubleshooting and configuring their network in their best efforts to maximize the utilization of their network hardware. In contrast using VLANs for different purposes of their initial design can been proven error prone. Designing the logical network topology, configuring the hardware applying policies (e.g. QOS) is a tough and time consuming process, that’s why VLANS are used in this area. VLAN management is also a

tough process and unfortunately the answers to all these problems are coming from private vendors, while the academic research in VLANS is at low levels.

ΙΙ. ΕΙΣΑΓΩΓΗ

Τα εικονικά δίκτυα αναπτύχθηκαν αρχικά από τον **Walter David "Dave" Sincoskie** (December 21, 1954 - October 20, 2010) σε προσπάθειες που έκανε για να μειώσει τον όγκο των πακέτων πολυμετάδοσης (broadcast) σε μεγάλα δίκτυα Ethernet. Η λύση που βρήκε τελικά σε αυτό το πρόβλημα ήταν η εισαγωγή κάποιου «χρώματος», που χρησιμοποιείται ως αναγνωριστικό, σε κάθε Ethernet πακέτο. Το «χρώμα» αυτό είναι σήμερα γνωστό ως 802.1Q κεφαλή (header) (Wikipedia.org).

Οι πρώτες χρήσεις των εικονικών δικτύων στα μεγάλα δίκτυα και σε αυτά των πανεπιστημίων ήταν κατά κύριο λόγο ο ίδιος λόγος για τον οποίο επινοήθηκαν δηλαδή ο περιορισμός των πακέτων πολύμετάδοσης (broadcast), και φυσικά για να σχηματιστούν τα λογικά τοπικά δίκτυα όπου σε ένα τέτοιο θα μπορούσαν να συνδεθούν οι υπολογιστές που έχουν λογική ανάγκη να είναι στο ίδιο τοπικό δίκτυο (ομάδα χρηστών με κοινές απαιτήσεις) και όχι επειδή το επιβάλουν φυσικοί περιορισμοί (γραφεία, κτήρια, αποστάσεις).

Αργότερα καθώς οι απαιτήσεις σε ασφάλεια, ταχύτητα εξυπηρέτηση μεγάλωνουν οι διαχειριστές των δικτύων άρχισαν να χρησιμοποιούν τα εικονικά δίκτυα για την λύση και άλλων προβλημάτων. Τα εικονικά δίκτυα σήμερα χρησιμοποιούνται όχι μόνο για τους λόγους που προαναφέθηκαν αλλά και για λόγους ασφαλείας , όπως η απομόνωση συσκευών, κόμβων του δικτύου η ακόμα και για την απομόνωση ολόκληρων τοπικών δικτύων. Επίσης χρησιμοποιούνται για τον έλεγχο πρόσβασης ανάλογα με τον υπολογιστή που χρησιμοποιείται, για την καλύτερη ποιότητα των υπηρεσιών , για την αποκέντρωση της διαχείρισης του δικτύου και ακόμα για την δυνατότητα φορητότητας του χρήστη και

σύνδεσης του στο ίδιο τοπικό δίκτυο ανεξάρτητα από την τοποθεσία του (Yu, Rexford, Sun , Rao & Freamster, 2011).

Βέβαια αν και τα παραπάνω προβλήματα αντιμετωπίσθηκαν μερικώς, δημιουργήθηκαν νέα προβλήματα στην θέση τους που έχουν να κάνουν με την δύσκολη και απαιτητική παραμετροποίηση των εικονικών δικύων σε ένα μεγάλο δίκτυο, που αποτελείται από πολλές και διαφορετικές ομάδες χρηστών, όπως αυτό ενός πανεπιστημίου. Η παραπάνω δυσκολία οδηγεί συχνά σε προβλήματα δρομολόγησης στο επίπεδο δικτύου (IP routing), σε προβλήματα ανάκαμψης από προβληματικές συνδέσεις και σε προβλήματα σχετιζόμενα με το πρωτόκολλο του «επικαλύπτον δέντρο» (Spanning Tree Protocol) (Yu, Rexford, Sun , Rao & Freamster, 2011).

Για την λύση αυτών των προβλημάτων υπάρχει το GARP VLAN πρωτόκολλο (Tanenbaum, 1997) όπως επίσης και άλλα γνωστά από μεγάλες ιδιωτικές εταιρείες όπως το Cisco VTP (cisco.com). Τα πρωτόκολλα αυτά δίνουν απαντήσεις στα προβλήματα διαχείρισης των εικονικών δικτύων όμως έχουν και αυτά τα μειονεκτήματα τους.

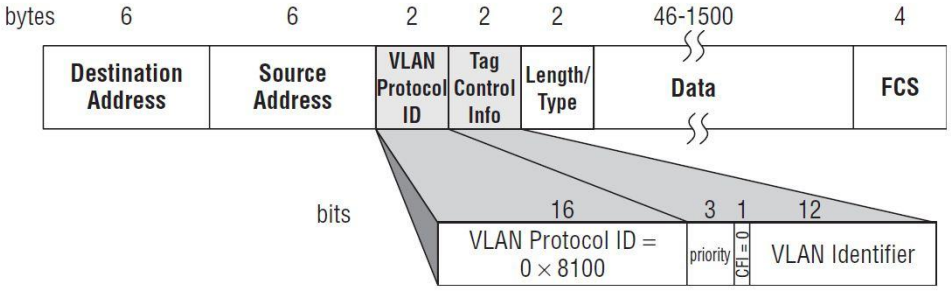
Τελευταία στους διαχειριστές των δικτύων αναπτύσσεται η τάση να απαγκυστρωθούν από τα εικονικά τοπικά δίκτυα ολοκληρωτικά και να στραφούν σε άλλες τεχνολογίες. Ήδη υπάρχει ακαδημαϊκή έρευνα και πειραματισμός σε νέες τεχνολογίες που έχουν σαν βάση την πολλά υποσχόμενη και ανερχόμενη τεχνολογία του OpenFlow (Yu, Rexford, Sun , Rao & Freamster, 2011; McKeown, Anderson, Balakrishnan, Parulkar, Peterson, Rexford, Shencker & Turner, 2008).

ΙΙΙ. ΥΛΟΠΟΙΗΣΗ ΤΩΝ ΕΙΚΟΝΙΚΩΝ ΤΟΠΙΚΩΝ ΔΙΚΤΥΩΝ

Για την υλοποίηση ενός VLAN χρειαζόμαστε ένα μεταγωγέα (switch) που καταλαβαίνει από εικονικά τοπικά δίκτυα (VLAN aware switch) ή οι υπολογιστές που

συνδέονται στο δίκτυο να έχουν κάρτες δικτύου που να μπορούν να διαχειριστούν εικονικά τοπικά δίκτυα. Συνήθως, επειδή είναι δύσκολο για του διαχειριστές των δικτύων να υποχρεώσουν όλους τους χρήστες να εφοδιαστούν με κάρτες δικτύου που να καταλαβαίνουν από εικονικά τοπικά δίκτυα, υλοποιούνται με την χρήση των ειδικών μεταγωγών (χωρίς αυτό να σημαίνει ότι δεν μπορούν να γίνουν και υλοποιήσεις με συστήματα που έχουν και τους 2 τρόπους) (Seifert & Edwards, 2008).

Σε κάθε περίπτωση, τα πλαίσια Ethernet είναι αυτά που ανήκουν σε ένα τοπικό εικονικό δίκτυο και όχι ο υπολογιστής ή ο μεταγωγέας (Seifert, 1998). Σε κάθε πλαίσιο που παραλαμβάνει ένας μεταγωγέας που καταλαβαίνει από εικονικά δίκτυα, τοποθετεί μία υπογραφή (tag) (εικόνα 1) που αποτελεί αναγνωριστικό για το εικονικό δίκτυο που ανήκει αυτό το πλαίσιο. Οι κανόνες αντιστοίχησης των πλαισίων με τις υπογραφές των εικονικών τοπικών δικτύων έχουν δημιουργηθεί από τους διαχειριστές του δικτύου, οι οποίοι έχουν αναλάβει να ρυθμίσουν και όλες τις συσκευές του δικτύου χειροκίνητα η με αυτόματο τρόπο (με χρήση αυτοματοποιημένων συστημάτων σαν το MVPR) (Yu, Rexford, Sun , Rao & Freamster, 2011; Seifert & Edwards, 2008; Seifert, 1998).

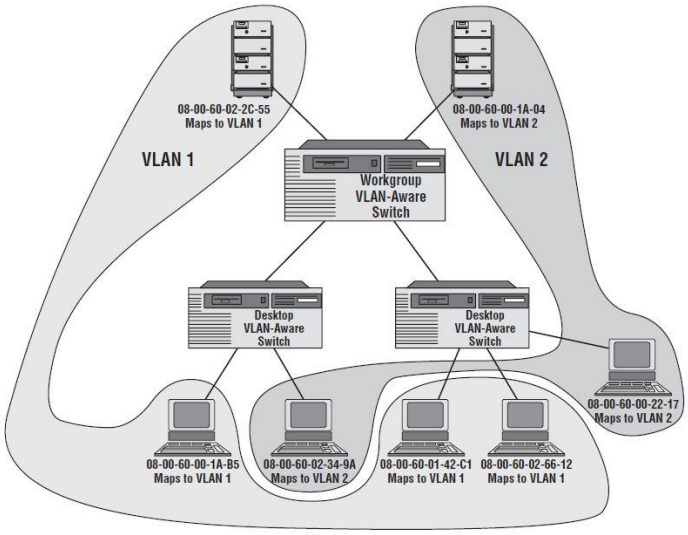


Εικόνα 1: Πλαίσιο με την υπογραφή ενός εικονικού τοπικού δικτύου (Vlan-tagged Ethernet Frame) (Seifert & Edwards, 2008).

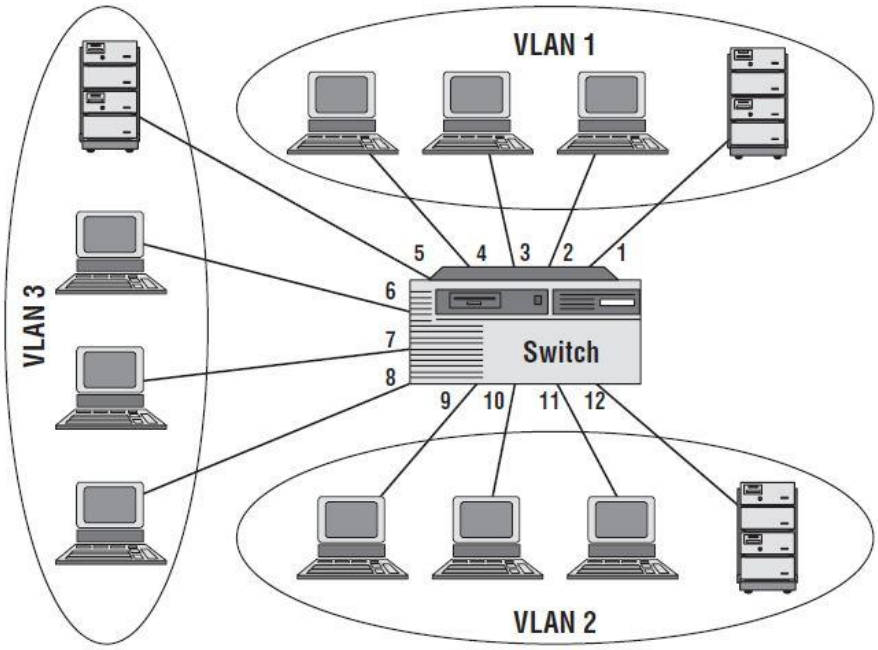
Οι κανόνες που αντιστοιχούν οι μεταγωγείς τα πλαίσια με τις αντίστοιχες υπογραφές ανήκουν στις εξής κατηγορίες (Seifert & Edwards, 2008):

- Βάση της διεύθυνσης, επίπεδου σύνδεσης δεδομένων, του υπολογιστή: Ο μεταγωγέας γωρίζει ποια διέυθυθνση (MAC address) ανήκει σε ποίο εικονικό δίκτυο, ανάλογα με τις ρυθμίσεις που έχει κάνει ο διαχειριστής του δικτύου. (εικόνα 2)
- Βάση θύρας του μεταγωγέα (port switch): Ανεξάρτητα με τον υπολογιστή ή συσκευή που θα συνδεθεί ο μεταγωγέας αντιστοιχίζει κάθε θύρα του με ένα ή περισσότερα εικονικά δίκτυα ανάλογα με τις ρυθμίσεις που έχει κάνει ο διαχειριστής. (εικόνα 3)
- Βάση του πρωτοκόλλου (protocol stack) που χρησιμοποιεί ο υπολογιστής: Κάθε υπολογιστής μπορεί να ανήκει σε περισσότερα από ένα εικονικά δίκτυα αν διαθέτει διαφορετικά πρωτόκολλα επικοινωνίας για τις εφαρμογές του. (εικόνα 4)

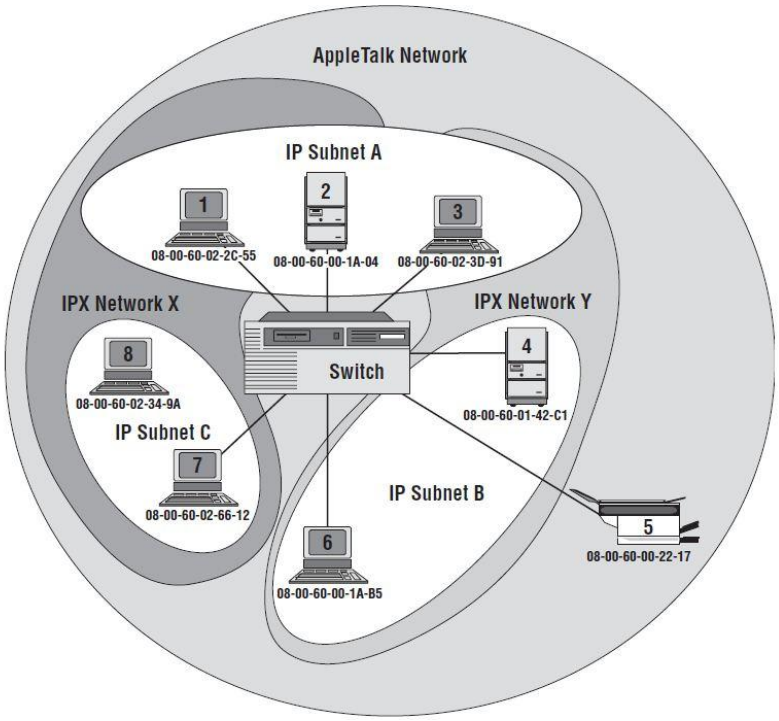
Ο δεύτερος τρόπος χρησιμοποιείται περισσότερο ως αποδοτικότερος εξαιτίας της απλότητας και της ταχύτητας ενώ ο πρώτος αν και πολυπλοκότερος μπορεί εξυπηρετήσει και άλλους σκοπούς και έτσι έχει περισσότερα πλεονεκτήματα σε αντάλαγμα με την απόδοση. Ο τρίτος τρόπος αποφεύγεται εξαιτίας του γεγονότος ότι εμπλέκει χωρίς σαφήνεια τα επίπεδα 2 και 3 (και μερικές φορές το επίπεδο 4) του Internet model (Sripanidkulchai, Issaeriyapat & Meesublak, 2008; Shuizhen, 2011).



Εικόνα 2: Οι μεταγωγείς γνωρίζουν ποιά MAC αντιστοιχεί σε ποιό VLAN (Seifert & Edwards, 2008).

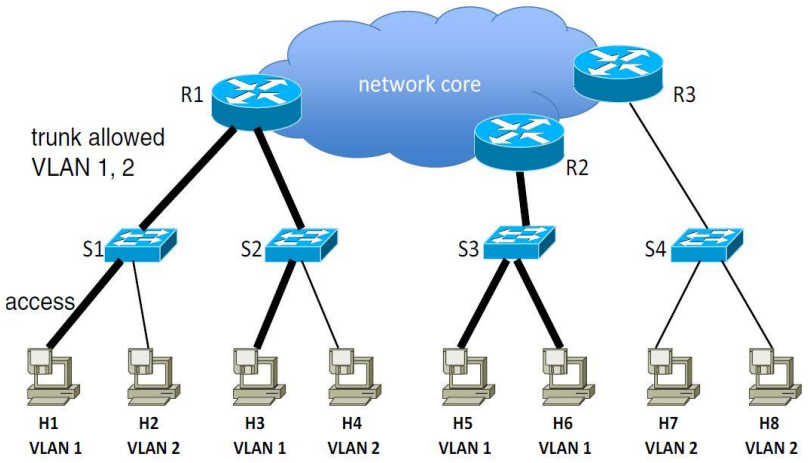


Εικόνα 3: Ο μεταγωγέας γνωρίζει ποιες θύρες του ανήκουν σε ποιο VLAN (Seifert & Edwards, 2008).



Εικόνα 4: Ο μεταγωγέας βλέποντας ποιο πρωτόκολλο χρησιμοποιείται καταλαβαίνει και σε ποιο VLAN ανήκει το πλαίσιο (Seifert & Edwards, 2008).

Φυσικά όπως γίνεται αντιληπτό οι μεταγωγείς που γνωρίζουν από εικονικά δίκτυα προωθούν την κίνηση των πλαισίων βάση των κανόνων που έχουν τεθεί από τους διαχειριστές. Ετσι τα πακέτα που βρίσκονται στο VLAN 1 παραδείγματος χάριν σε καμία περίπτωση δεν θα προωθηθούν σε θύρες ή υπολογιστές που ανήκουν στο VLAN 2. (εικόνα5)



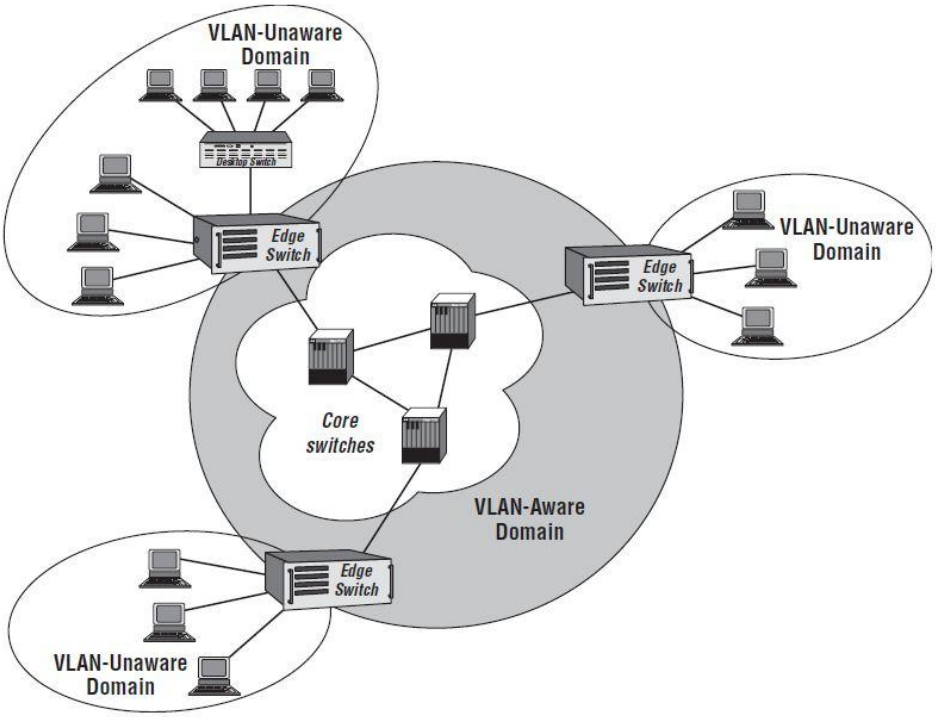
Εικόνα 5: Ένα τυπικό πανεπιστημιακό δίκτυο (Sun, 2010).

Στην παραπάνω εικόνα, εάν ο υπολογιστής 1 στείλει για παράδειγμα ένα ARP πακέτο θα το λάβουν μόνο οι υπολογιστές που ανήκουν στο VLAN1. Οι μεταγωγείς του δικτύου θα φροντίσουν ώστε το πακέτο αυτό να μην φτάσει ποτέ σε κάποιον άλλο υπολογιστή. Επίσης στην παραπάνω εικόνα ο μεταγωγέας 1 προωθεί κίνηση και των δύο εικονικών δικτύων. Όταν λάβει πλαίσια από τον υπολογιστή 1 θα τα προωθήσει μόνο στην θύρα που επικοινωνεί με τον δρομολογητή 1 και όχι στην θύρα που επικοινωνεί με τον υπολογιστή 2. Εάν υποθέσουμε ότι όλοι οι υπολογιστές της εικόνας 5 δεν γνωρίζουν από εικονικά δίκτυα τότε οι μεταγωγείς 1,2,3 πρέπει να γνωρίζουν οποσδήποτε (VLAN-aware) ενώ δεν ισχύει το ίδιο για τον μεταγωγέα 4 υπο την προυπόθεση ότι όλα τα

πλαίσια που φτάνουν σε αυτόν από τον δρομολογητή 3 δεν φέρουν υπογραφή (tag) κάποιου εικονικού δικτύου.

Από τα παραπάνω είναι φανερό ότι με την υλοποίηση των εικονικών τοπικών δικτύων οι μεταγωγείς χωρίζονται σε δύο κατηγορίες: στους μεταγωγείς πυρήνα (core switches) και στους μεταγωγείς συνόρου (edge switches) (Seifert & Edwards, 2008). Οι μεταγωγείς συνόρου συνδέουν τις περιοχές που γνωρίζουν για τα εικονικά τοπικά δίκτυα(Vlan-aware domain) και τις περιοχές που δεν γνωρίζουν (Vlan-unaware domain). Οι περιοχές που δεν γνωρίζουν από τα εικονικά τοπικά δίκτυα στέλνουν πλαίσια που φυσικά δεν περιέχουν καμία υπογραφή κάποιου εικονικού δικτύου. Η δουλεία που κάνουν οι μεταγωγείς συνόρου είναι όταν λαμβάνουν τέτοια πλαίσια να τοποθετούν την αντίστοιχη υπογραφή και μετά να τα προωθούν στις περιοχές που γνωρίζουν από εικονικά δίκτυα. Φυσικά δουλεία τους είναι και η αντίστροφη διαδικασία. Όταν λαμβάνουν πλαίσιο που φέρει υπογραφή από εικονικό δίκτυο πρέπει πρώτα να την βγάλουν πριν προωθήσουν το πλαίσιο αυτό σε περιοχή που δεν έχει γνώση των εικονικών δικτύων.

Οι μεταγωγείς πυρήνα (core switches) ανήκουν στο κυρίως δίκτυο ενός πανεπιστημίου. Διαχειρίζονται μόνο πλαίσια που φέρουν υπογραφή κάπιου εικονικού δικτύου ενώ όποιο πλαίσιο δεν φέρει υπογραφή τότε αυτό καταστρέφεται. Ο μεταγωγέας πυρήνα παίρνει απόφαση με το που θα στείλει κάθε πλαίσιο μόνο από την υπογραφή του εικονικού δικτύου. Έτσι η διαδικασία εύρεσης σε ποια θύρα θα προωθήσει το κάθε πλαίσιο είναι απλή και γρήγορη αφού υπάρχουν μόνο 4.094 δυνατές υπογραφές για τα εικονικά δίκτυα (IEEE 802,1 Q standard) (Wikipedia.org) ενώ σε αντίθετη περίπτωση θα είχε τόσες εγγραφές ίσο με τον αριθμό των υπολογιστών που θα εξυπηρετούσε (Seifert, 1998).



Εικόνα 6: Περιοχές που γνωρίζουν ή δεν γνωρίζουν από εικονικά δίκτυα μεταγωγείς πυρήνα και μεταγωγείς συνόρου (Seifert & Edwards, 2008).

Από τη εικόνα 6 είναι εμφανές ότι οι μεταγωγείς συνόρου ενώνουν τις περιοχές που δεν γνωρίζουν από εικονικά δίκτυα με αυτές που γνωρίζουν. Οι μεταγωγείς πυρήνα ανήκουν σε περιοχές που γνωρίζουν από εικονικά δίκτυα.

IV. ΧΡΗΣΕΙΣ ΤΩΝ ΕΙΚΟΝΙΚΩΝ ΔΙΚΤΥΩΝ. ΠΛΕΟΝΕΚΤΗΜΑΤΑ. ΜΕΙΟΝΕΚΤΗΜΑΤΑ

Μείωση της εκπομπής (broadcast) : Μια από τις ποιο διαδεδομένες χρήσεις είναι η χρήση των εικονικών δικτύων για τον περιορισμό της κίνησης στο δίκτυο που δημιουργείται από τα τα πακέτο εκπομπής (broadcast traffic). Δεν είναι λίγες οι περιπτώσεις που οι διαχειριστές των δικτύων χωρίζουν μεγάλα τοπικά δίκτυα σε περισσότερα από ένα εικονικά τοπικά δίκτυα για να περιορίσουν το φαινόμενο αυτό

(Yu, Rexford, Sun , Rao & Freamster, 2011). Με αυτό τον τρόπο μειώνεται η κίνηση στο δίκτυο εξεικονομώντας πόρους και επίσης μειώνεται ο φόρτος εργασίας των μεταγωγών μοιράζετε σε όλους ανάλογα με τις ρυθμίσεις των διαχειριστών και σε μερικές περιπτώσεις εξαλήφετε τελείως. Χωρίς την χρήση των εικονικών δικτύων ένας μεταγωγέας (switch) που δεν θα γνώριζε μία MAC διεύθυνση θα πλημύριζε το δίκτυο για να μπορέσει να την εντοπίσει. Βέβαια το βασικό μειονέκτημα σε αυτήν την περίπτωση είναι το πρέπει να γίνουν και άλλες ρυθμίσεις, μεγαλώνοντας με αυτό τον τρόπο την πολυπλοκότητα των ρυθμίσεων των δρομολογητών, σε περίπτωση που οι διαχειριστές θέλουν αυτά τα εικονικά δίκτυα να επικοινωνούν μεταξύ τους (cisco.com) που στις περισσότερες περιπτώσεις δεν είναι αναγκαίο.

Λόγοι ασφάλειας: Η εκπομπή και η ανταλλαγή μεγάλης πληροφορίας όπως επίσης και η τεχνική της πλημύρας στο δίκτυο (flooding traffic) είναι μια αποδοτική μέθοδος για περιπτώσεις DoS (Denial of Service) επιθέσεων. Επίσης υπάρχει οι πιθανότητα κάποιος κακόβουλος χρήστης να εκμεταλλευτεί την πληροφορία αυτή που διακινείτε στο δίκτυο και να προσποιηθεί πως είναι κάποιος άλλος αποσπώντας έτσι χρήσιμες πληροφορίες που δεν θα έπρεπε να έχει πρόσβαση (Yu, Rexford, Sun , Rao & Freamster, 2011). Με την χρήση των εικονικών δικτύων οι διαχειριστές μπορούν να περιορίσουν την πρόσβαση που έχει ένας πιθανών κακόβουλος χρήστης σε ζωτικής σημασίας χώρους για το δίκτυο. Στο ίδιο εικονικό δίκτυο ανήκουν μόνο χρήστες που επιτρέπεται να επικοινωνούν ελεύθερα μεταξύ τους. Έτσι στα περισσότερα πανεπιστήμια οι εξυπηρετητές ηλεκτρονικής αλληλογραφίας, ηλεκτρονικών υπηρεσιών, οι βάσεις δεδομένων αναζήτησης και άλλα τέτοια συστήματα ανήκουν σε ξεχωριστά εικονικά δίκτυα που δεν περιλαμβάνουν κανέναν χρήστη εκτός από συγκεκριμένους διαχειριστές δικτύου (ucdavis.edu). Με αυτό τον τρόπο αυξάνεται το επίπεδο προστασίας του δικτύου όμως δημιουργούνται νέα ευαίσθητα σημεία στην ασφάλεια του δικτύου που

οφείλονται στην χρήση των εικονικών δικτύων όπως επιθέσεις τύπου Vlan hopping, CDP (Cisco Discovery Protocol Attacks), PVLAN (Private Vlan Attacks), STA (Spanning Tree Attack), VMPS/VQP που δεν θα υπήρχαν αν δεν γινόταν χρήση των εικονικών δικτύων (Rouiller, n.d.). Βέβαια για τον περιορισμό των παραπάνω αναφερόμενων επιθέσεων και για την μεγιστοποίηση της ασφάλειας των δικτύων που γίνετε χρήση των εικονικών δικτύων γίνονται προσπάθειες συνδιασμού και άλλων τεχνολογιών. Χαρακτηριστική περίπτωση είναι αυτή του πανεπιστημίου της Μοσούλης στο Ιράκ όπου τα εικονικά δίκτυα συνδυάζονται με AAA Server για την μεγιστοποίηση της ασφάλειας του δικτύου (Salah, n.d.)

Απλοποίηση των κανόνων πρόσβασης (Access Control Policies): Τα εικονικά δίκτυα προσφέρουν έναν αποδοτικό τρόπο για την εφαρμογή των κανόνων πρόσβασης (Yu, Rexford, Sun , Rao & Freamster, 2011). Οι διαχειριστές μπορούν να ομαδοποιήσουν τους χρήστες, ανάλογα με τους κανόνες πρόσβασης που θέλουν να τους επιβάλουν, και να τους τοποθετήσουν στα ίδια τοπικά εικονικά δίκτυα. Με αυτό τον τρόπο οι χρήστες αυτοί μπορούν να έχουν συγκεκριμένες IP διευθύνσεις από συγκεκριμένο εύρος (IP range) κάνοντας έτσι του κανόνες πρόσβασης μικρότερους σε μέγεθος πιο εύκολους στην χρήση τους και παραμετροποίηση τους (Yu, Rexford, Sun , Rao & Freamster, 2011; Sripanidkulchai, Issaeriyapat & Meesublak, 2008).

Υποστήριξη ποιότητας υπηρεσίας (Quality of Service support): Η ομαδοποίηση των χρηστών σε εικονικά δίκτυα μπορεί να γίνει και ανάλογα με τον βαθμό εξυπηρέτησης που θέλουν οι διαχειριστές του δικτύου να λάβει κάθε χρήστης. Έτσι χωρίζοντας του χρήστες σε διαφορετικά εικονικά δίκτυα ανάλογα με τον βαθμό εξυπηρέτησης οι ρυθμίσεις για του κανόνες ποιότητας υπηρεσίας (QoS policy) γίνονται λιγότεροι και πιο εύκολοι στην διαχείρηση τους (Yu, Rexford, Sun , Rao & Freamster, 2011). Βέβαια τις περισσότερες φορές κάποια συγκεκριμένα πρωτόκολλα είναι αυτά

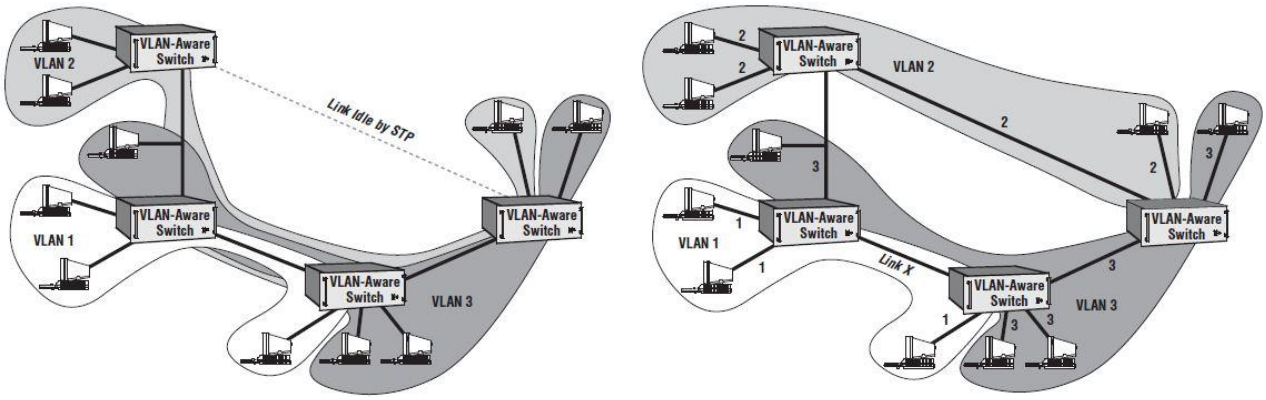
που πρέπει να πάρουν μεγαλύτερο βαθμό εξυπηρέτησης και όχι συγκεκριμένοι χρήστες. Για να εκμεταλευτούν πλήρως οι διαχειριστές λοιπόν αυτή την δυνατότητα θα πρέπει να έχουν υλοποιημένα εικονικά δίκτυα που βασίζονται στα πρωτόκολλα (protocol stack based vlans) που όπως έχουμε πεί είναι μια λύση που δεν την προτιμούν οι διαχειριστές των δικτύων. Σε αυτήν την περίπτωση, της υποστήριξης ποιότητας υπηρεσίας, ενδιαφέρων παρουσιάζει οι εφαρμογή των εικονικών δικτύων στα πανεπιστημιακά δίκτυα που έχουν υποστηρίζουν IP τηλεφωνία μέσα στο δίκτυο τους. Οι διαχειριστές τοποθετούν όλες τις MAC διευθύνσεις των τηλεφωνικών συσκευών σε ένα εικονικό δίκτυο το οποίο έχει την υψηλότερη προτεραιότητα στους κανόνες QoS και επίσης δρομολογείται κατάλληλα στο IP τηλεφωνικό κέντρο καταφέρνοντας με αυτό τον τρόπο την μεγαλύτερη δυνατή απόδοση (Jiang, Liacheng & Zhao, 2009).

Αποκεντρωμένη ομάδα διαχείρισης δικτύου και ευκολότερη αντιμετώπιση προβλημάτων: Με την χρήση των εικονικών δικτύων σε ένα πανεπιστημιακό δίκτυο είναι εφικτό η ομάδα των τεχνικών του δικτύο να διαχωρισθεί σε μικρότερες στις οποίες μπορεί να ανατεθεί ένα συγκεκριμένο εύρος αριθμών εικονικών δικτύων που θα είναι στην ευθύνη της (Yu, Rexford, Sun , Rao & Freamster, 2011). Έτσι η διαχείριση του δυναμικού των τεχνικών δικτύων γίνεται ευκολότερη και οι μικρές ομάδες είναι πάντα πιο ευέλικτες. Ο κεντρικός σχεδιασμός του δικτύου και ο στρατηγικός σχεδιασμός μπορεί να παραμείνει σε μία ομάδα που θα ηγείται των προαναφερόμενων. Με αυτό τον τρόπο ο εντοπισμός και η αντιμετώπιση των πιθανών προβλημάτων γίνεται σε συντομότερα χρονικά διαστήματα αφού οι ομάδες πρέπει να γνωρίζουν ακριβώς τις τοπολογίες των εικονικών δικτύων που τους έχουν ανατεθεί και όχι ολόκληρου του πανεπηστιμιακού δικτύου.

Κινητικότητα χρηστών: Η χρήση των εικονικών δικτύων, κυρίως όταν η αντιστοίχηση του χρήστη με το εικονικό δίκτυο που ανήκει γίνεται με βάση την MAC

διεύθυνση του, βοηθάει στην κινητικότητα των χρηστών μέσα στο χώρο του πανεπιστημίου (Yu, Rexford, Sun , Rao & Freamster, 2011). Οι χρήστες μπορούν να κινούνται ελεύθερα μεταξύ των ασύρματων σημείων πρόσβασης του πανεπιστημίου χωρίς να αλλάζουν IP διεύθυνση αφού παραμένουν στο ίδιο εικονικό δίκτυο (Jiang & Liacheng2008). Έτσι μπορούν να συνεχίζουν να εργάζονται όπως σαν να ήταν στο γραφείο τους παρόλο που κινούνται ελεύθερα με τον φορητό τους υπολογιστή στους χώρους του πανεπηστιμίου που υπάρχει ασύρματο σημείο πρόσβασης η ακόμα και ενσύρματης.

Δυνατότητα δρομολόγησης χωρίς δρομολογητή: Με την χρήση των εικονικών δικτύων είναι δυνατόν ένας διαχειριστής δικτύου να μπορέσει να δρομολογήσει την κίνηση στο δίκτυο χωρίς την ύπαρξη κάποιου δρομολογητή. Έτσι μπορεί να κατευθύνει την κίνηση συγκεκριμένων εικονικών δικτύων από άλλες διαδρομές ανάλογα με τις απαιτήσεις των χρηστών και ανάλογα με το φόρτο και το εύρος των γραμμών. Βέβαια οι δρομολογήσεις αυτές είναι στατικές και δεν μπορούν να αλλάξουν αυτόματα αν κάποιος από τους παράγοντες διαφοροποιηθεί.



Εικόνα 7 : Εκμετάλλευση ανενεργής διαδρομής λόγο STP με την χρήση των εικονικών δικτύων (Seifert & Edwards, 2008).

V. ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΕΙΚΟΝΙΚΩΝ ΔΙΚΤΥΩΝ ΑΝΕΞΑΡΤΗΤΟΥ ΧΡΗΣΗΣ

Βέβαια εκτός από τις προαναφερόμενες χρήσεις και τυχόν μειονεκτήματα που προκύπτουν από την χρήση των εικονικών δικύων, υπάρχουν και κάποια προβλήματα – μειονεκτήματα που οφείλονται καθαρά στα εικονικά δίκτυα και όχι γιατί έχουν χρησιμοποιηθεί για κάποιον συγκεκριμένο σκοπό.

Περιορισμένος αριθμός εικονικών δικτύων: Η υπογραφή που φέρει κάθε πλαίσιο για το εικονικό δίκτυο είναι ένας αριθμός των 12 bit, όπως έχει καθοριστεί από την IEEE και το πρωτόκολλο 802.11Q (Wikipedia.org) (το πρωτόκολλο 802.11 QinQ υπόσχεται θεωρητικά 16,777,216 ξεχωριστές υπογραφές για εικονικά δίκτυα) (Yu, Rexford, Sun , Rao & Freamster, 2011). Στην πράξη η περιορισμένη μνήμη των συνηθισμένων μεταγωγών (switch) συχνά περιορίζει τον αριθμό των εικονικών δικτύων που μπορεί να εξυπηρετήσει σε 300-500 (Yu, Rexford, Sun , Rao & Freamster, 2011). Για λόγους οικονομίας των υπογραφών, οι διαχειριστές των δικτύων πολλές φορές τοποθετούν χρήστες στο ίδιο εικονικό δίκτυο με χρήστες που θα έπρεπε να ανήκουν σε διαφορετικό εικονικό δίκτυο, με ότι αυτό συνεπάγεται στην ασφάλεια των χρηστών και στην παροχή υπηρεσιών. Επίσης επαναχρησιμοποιούν τις ίδιες υπογραφές των εικονικών δικτύων προσέχωντας να μην υπάρχει σύνδεση μεταξύ τους. Όμως σε ένα περιβάλλον δυναμικό όπως είναι αυτό των δικτύων αυτό είναι δύσκολο να διατηρηθεί στο μέλλον δυσκολεύοντας πολύ τις ρυθμίσεις που πρέπει να γίνονται στο δικτυακό εξοπλισμό.

Σύνθετες ρυθμίσεις: Η χρήση πολυάριθμων εικονικών δικτύων σε ένα μεγάλο δίκτυο όπως αυτό ενός πανεπηστιμίου απαιτεί προσεκτικό σχεδιασμό και προσεκτική ρύθμιση στις συσκευές του δικτύου. Οι διαχειριστές πρέπει για παράδειγμα να είναι σίγουροι πως κάθε εικονικό δίκτυο έχει πρόσβαση σε έναν ακριβώς DHCP εξυπηρετητή,

και πως κάθε εικονικό δίκτυο έχει πρόσβαση εκεί που έχουν ανάγκη οι χρήστες του καθώς επίσης να λάβει υπόψη ανενεργές συνδέσεις λόγο STP (Spanning Tree Protocol), να υπάρχουν και δευτερεύουσες συνδέσεις για προβληματικές καταστάσεις, και επίσης να μην υπερφορτώσει συγκεκριμένες συσκευές δικτύου (Yu, Rexford, Sun , Rao & Freamster, 2011). Κάθε μεταγωγέας πρέπει να ρυθμιστεί τις περισσότερες φορές χειροκίνητα κάποιον τεχνικό μια διαδικασία επίπονη και πολλές φορές πηγή προβλημάτων (Benson, Akella & Maltz, 2009). Βέβαια στην αντιμετώπιση αυτών των ζητημάτων υπάρχουν αυτοματοποιημένα συστήματα σαν το VTP, MVPR κ.α. (Seifert & Edwards, 2008; Seifert, 1998) όμως η χρήση τους δημιουργεί θέματα ασφάλειας (Rouiller, n.d.) καθώς και μεγαλύτερη κίνηση στο δίκτυο λόγο ανταλλαγής πληροφορίας χρήσιμης για την λειτουργία των συστημάτων αυτών. Βέβαια έχουν αναπτυχθεί αλγόριθμοι και μέθοδοι προς την ευκολότερη παραμετροποίηση των συσκευών του δικτύου (Sun, 2010; Prashant, Yu-Wei, Nan & Sanjay, 2007; Okayama, Yamai, Miyashita, Kawano & Okamoto, 2005).

VI. ΣΥΜΠΕΡΑΣΜΑΤΑ

Η χρήση των εικονικών τοπικών δικτύων στα πανεπηστιμιακά δίκτυα είναι εκτεταμένη και δίνει απαντήσεις σε προβλήματα ανάλογα με την φαντασία του κάθε διαχειριστή δικτύου. Βέβαια τα προβλήματα που δημιουργεί η χρήση της τεχνολογίας αυτής είναι αρκετά και πολλές φορές ικανά στο να δημιουργήσουν μεγάλα κενά ασφαλείας, προβληματικά δίκτυα και υπερφορτωμένα δίκτυα, και χαοτικές ρυθμίσεις. Ήδη έχουν ξεκινήσει πειραματικά δίκτυα (Yamasaki, Miyamoto, Yamato & Hideaki, 2011) με την χρήση νέων τεχνολογιών βασισμένες πάνω στην τεχνολογία OpenFlow (McKeown, Anderson, Balakrishnan, Parulkar, Peterson, Rexford, Shencker & Turner, 2008) που προσπαθεί να περιορίσει και σε μερικές περιπτώσεις να καταργήσει την χρήση των εικονικών δικτύων. Όλα αυτά δείχνουν πως η εποχή της εκτεταμένης χρήσης

των εικονικών δικτύων φτάνει σιγά σιγά προς το τέλος της και πως η ακαδημαική έρευνα πρέπει να κατεθυηνυεί προς την ανακάλυψη νέων τεχνολογιών που θα δίνουν απαντήσεις στα ίδια προβλήματα που χρησιμοποιούνται μέχρι τώρα τα εικονικά δίκτυα χωρίς όμως τα μειονεκτήματα τους.

Προς αυτή την κατεύθυνση θα ήταν χρήσιμες συγκριτικές μελέτες μεταξύ των καινούργιων τεχνολογιών και των εικονικών δικτύων πάνω στην απόδοση, στην ασφάλεια, στον χειρισμό και τις ρυθμίσεις και στο κόστος λειτουργίας. Βέβαια μιας και τα εικονικά δίκτυα χρησιμοποιούνται και θα συνεχίσουν να χρησιμοποιούνται για αρκετό καιρό ακόμα χρήσιμες θα ήταν και συγκριτικές μελέτες μεταξύ των αλγορίθμων και μεθόδων που έχουν αναπτυχθεί για τον σχεδιασμό και την διατήρηση τους καθώς και η εξέλιξη αυτών των μεθόδων και αλγορίθμων.

VII. ΑΝΑΦΟΡΕΣ

Benson, T., Akella, A., Maltz, D. (2009). Unraveling the Complexity of Network Management. *Proc. NSDI.*

Jiang, N., Liacheng, S., Zhao, J. (2009). Application of Dynamic Port VLAN Membership with Auxiliary VLAN in Campus Area Network. *9th International Conference on Hybrid Intelligent Systems.*

Jiang, N., Liacheng, S. (2008). Application of MAC-based VLANs for Mobile Office in Campus Area Network. *International Conference on Intelligent Information Hiding and Multimedia Signal Processing.*

Krothapalli, S.D., Yeo, S.A., Yu-Wei E.S., Rao, G. (n.d.). Virtual MAN: A VLAN Management System for Enterprise Networks. *Purdue University.*

McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shencker, S., Turner, J. (2008). OpenFlow: Enabling Innovation in Campus Networks. *ACM SIGCOMM Computer Communication Review.*

Yu, M., Rexford, J., Sun, X., Rao, S., Freamster, N. (2011). A survey of Virtual LAN usage in Campus Networks. *IEEE communications magazine*..

Okayama, K., Yamai, N., Miyashita, T., Kawano, K., Okamoto, T. (2005). A Method of Dynamic Interconnection of VLANs for Large Scale VLAN Environment. *Information and Telecommunication Technologies.*

Prashant, G., Yu-Wei, S., Nan, Z., Sanjay, R. (2007). Characterizing VLAN usage in Operational Network. *ECE Technical Reports, Purdue University.*

Rouiller, S. (n.d.). Virtual LAN Security: weakness and countermeasures. *SANS Institute InfoSec Reading Room.*

Salah, A. (n.d.). Design and Implementation of a Network Security Model using Static VLAN and AAA Server. *University of Mosul, Iraq.*

Seifert, R., Edwards, L. (2008). The All-New Switch Book: The Complete Guide to LAN Switching Technology. *John Wiley & Sons.*

Seifert, R. (1998). Gigabit Ethernet. *Addison –Wesley.*

Shuizhen, X. (2011). Planning, designing and building large-scale network at campus. *ICCRD International Conference.*

Sripanidkulchai, K., Issaeriyapat, C., Meesublak, K. (2008). Inference of Network-wide vlan usage in small enterprise networks. *IEEE Workshop on Automated Network Management*.

Sun, X. (2010). A Systematic Approach for Evolving VLAN Design. *IEEE INFOCOM*.

Tanenbaum, A.S. (1997). Computer Networks. *Prentice-Hall International, Inc.*

Yamasaki, Y., Miyamoto, Y., Yamato, J., Hideaki, G., Hideaki S. (2011). Flexible Access Management System for Campus VLAN Based on OpenFlow. *IPSJ International Symposium On Applications and the Internet.*

VIII. ΗΛΕΚΤΡΟΝΙΚΕΣ ΑΝΑΦΟΡΕΣ

Virtual Lan. (n.d.). Retrieved from http://en.wikipedia.org/wiki/Virtual_LAN

Understanding VLAN trunk protocol. (n.d.). Retrieved from http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094c52.shtml

IEEE 802.1 Q. (n.d.). Retrieved from http://en.wikipedia.org/wiki/IEEE_802.1Q

VLAN information. (n.d.). Retrieved from http://net21.ucdavis.edu/newvlan.htm

Overview of routing between Virtual LANs. (n.d.). Retrieved from www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/switch_c/xcvlan.htm