

## Θέμα - IPv6

Του Γιώργου Καργιωτάκη <kargig@void.gr>



Ο Γιώργος εργάζεται σε εταιρεία που φτιάχνει Linux based xDSL routers και ασχολείται με θέματα QoS, VoIP και IPv6 σε Linux!

# IPv6: Ένας θαυμαστός νέος κόσμος!

Ηρθε η ώρα για την αλλαγή. Υποδεχθείτε το καινούργιο Internet!

Όσοι θεωρούν ότι το αρκτικόλεξο IPv6 δεν λέει κάτι, αυτό το άρθρο θα κάνει μία πρώτη εισαγωγή, ώστε σε λίγους μήνες που το IPv6 θα μπει για τα καλά στη ζωή μας να ξέρουν τι έχουν να συναντήσουν. Ο θαυμαστός αυτός νέος κόσμος έχει πολλές ιδιαιτερότητες, καταργεί πράγματα που μέχρι τώρα θεωρούσαμε δεδομένα και φέρνει αρκετά καινούργια.

### Ιστορικά

Θα πρέπει πρώτα όμως να κάνουμε μία αναδρομή στην ιστορία. Το 1981 γεννήθηκε το IPv4 (Internet Protocol, RFC791), το οποίο ήταν η τέταρτη έκδοση του πρωτοκόλλου IP και η μόνη που κατάφερε να διαδοθεί ευρέως. Στο σχεδιασμό του καθορίστηκε το μέγεθός του στα 32bits, γεγονός που περιορίζει τις διαθέσιμες τιμές σε 4.294.967.296 (2<sup>32</sup>). Ανάμεσά τους υπάρχουν κάποιες δεσμευμένες διευθύνσεις για private δίκτυα (~ 18.000.000) και κάποιες άλλες για τις multicast διευθύνσεις (~ 270.000.000), με αποτέλεσμα να περιορίζονται αρκετά οι διαθέσιμες τιμές. Ο τρόπος που παλιότερα γίνονταν η διανομή διευθύνσεων ονομάζεται classful και το μικρότερο εύρος διευθύνσεων που θα μπορούσε να πάρει κάποιος ήταν 256 IP! Το 1993 έγινε αντιληπτό ότι με τον τρόπο που μοίραζαν μέχρι τότε τις διευθύνσεις θα τελείωναν πάρα πολύ γρήγορα, οπότε δημιουργήθηκε το CIDR (Classless Inter-Domain Routing, RFC1518, 1519, 4632) το οποίο έφερε τον όρο του «subnet mask» και πλέον το μικρότερο δυνατό εύρος διευθύνσεων που ορίζεται είναι αυτό της 1 IP (/32). Και αυτό όμως το σύστημα δεν είναι τέλειο. Ένα δίκτυο με subnet mask/24 που αποτελείται από 256 IPs, αν το σπάσει σε 4x/26 δίκτυα τότε χάνονται 8 IPs, 2 για κάθε subnet, το network address και το broadcast. Ομως, με την ανάπτυξη και τη διάδοση του Internet, είναι καθημερινά επιτακτική η ανάγκη για όλο και περισσότερες διευθύνσεις, με αποτέλεσμα στα μέσα

του '90 να γίνει εμφανές ότι το IPv4 ξεμένει από διευθύνσεις με απειλητικούς ρυθμούς για την πορεία του Internet.

Ως μία προσωρινή λύση στο γρήγορο ρυθμό εξάντλησης των IPv4 διευθύνσεων εμφανίστηκε το 1996 το NAT (Network Address Translation, RFC1918) μέσω του οποίου πίσω από μία πραγματική διεύθυνση μπορεί να υπάρχουν δίκτυα με private διευθύνσεις και να γίνεται κάποιου είδους μετάφραση/αλλαγή των επικεφαλίδων των πακέτων όταν περνούν προς/από τους NAT gateways. Δυστυχώς, το NAT έχει προβλήματα scalability/απόδοσης, αλλά και σπάει το end-to-end connectivity το οποίο είναι πολύ βασικό στοιχείο για την ελευθερία της επικοινωνίας στο Internet. Το NAT είναι πλέον ο πιο συνηθισμένος τρόπος διασύνδεσης στις σπιτικές μας συνδέσεις. Ο router του σπιτιού μας, που ονομάζεται CPE (Customer-premises equipment), έχει μία πραγματική IP(v4) και από πίσω στο LAN υπάρχουν private διευθύνσεις οι οποίες μέσω NAT καταφέρνουν να συνδεθούν και να επικοινωνήσουν με άλλα μηχανήματα στο Internet. Παρ' όλο, που το NAT εφαρμόζεται σχεδόν παντού, ο ρυθμός εξάντλησης των IPv4 διευθύνσεων συνεχίζει να γίνεται όλο και υψηλότερος, μια που η ευρυζωνικότητα εξαπλώνεται σε όλο και περισσότερες (κυρίως μη Δυτικές) χώρες και αυτή τη στιγμή (Δεκέμβριος 2010) είναι διαθέσιμες λιγότερες από 110.000.000 IPv4 διευθύνσεις. Ο ρυθμός αυτός, όπως φαίνεται στην εικόνα 1, οδηγεί στην πλήρη εξάντληση των διαθέσιμων διευθύνσεων το πολύ στο δεύτερο τρίμηνο του 2011!

Κάποιοι θα έλεγαν ότι η λύση στην εξάντληση των διευθύνσεων του IPv4 θα ήταν να κάνουν οι ISP μας ένα πρώτο NAT (Carrier-Grade NAT) με κάποια από τις private διευθύνσεις και μετά το CPE μας να κάνει ένα δεύτερο NAT με μία διαφορετική private διεύθυνση και όλα θα συνεχίσουν να δουλεύουν μια χαρά. Δυστυχώς, όμως, το μοντέλο αυτό απλώς διπλασιάζει τα



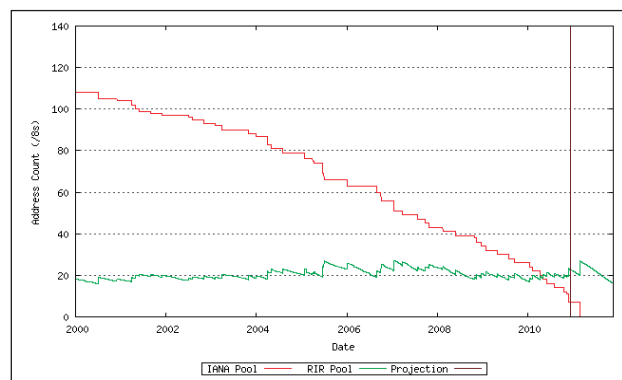
προβλήματα και απομακρύνει το χρήστη από την πραγματική του διεύθυνση, με αποτέλεσμα να είναι πολύ δύσκολο να προσφέρει ο ίδιος υπηρεσίες προς το Internet μέσω της σύνδεσής του. Θα χρειαζόταν αίτημα στον ISP για να γίνει ένα απλό port-forward! Επίσης, τίθενται θέματα network-neutrality και ισότητας των ανθρώπων που θέλουν πρόσβαση στο Internet, μια και οι πλούσιοι θα μπορούν να αγοράζουν πραγματικές IPs, ενώ οι φτωχότεροι θα μένουν με το Carrier-Grade NAT.

### Ο νέος κόσμος και οι αλλαγές που αυτός φέρνει

Ευτυχώς, κάποιοι είχαν προβλέψει ότι θα φτάναμε στην παρούσα κατάσταση ακόμη και με το CIDR και το NAT, οπότε από τις αρχές της δεκαετίας του '90 ξεκίνησε μία προσπάθεια να φτιαχτεί ένα νέο πρωτόκολλο που θα ξεπερνούσε τα προβλήματα διευθυνσιοδότησης -και όχι μόνο- του IPv4. Το 1992 παρουσιάστηκε το IPng, το 1995 παρουσιάστηκε η πρώτη έκδοση του IPv6 (RFC1883) και τον Δεκέμβριο του 1998 έγινε επίσημο (RFC2460). Φυσικά, το εύρος διευθύνσεων αποφασίστηκε να είναι αρκετά μεγαλύτερο του IPv4: από τα 32bit δεν πήγαμε στα 48, ούτε στα 64, πήγαμε κατευθείαν στα 128bit!

Ετσι, οι διαθέσιμες διευθύνσεις είναι  $2^{128}$  ή  $3.4 \cdot 10^{38}$  ή 340.282.366.920.938.463.463.374.607.431.768.211.456! Ενώ μία IPv4 διεύθυνση αποτελείται από τέσσερις ομάδες των 8bit ( $2^8=256$ ) αποτελούμενο από δεκαδικούς αριθμούς που χωρίζονται με τελεία (.), μία IPv6 διεύθυνση αποτελείται από οκτώ ομάδες των 16bit ( $2^{16}=65536$ ) που γράφονται με δεκαεξαδικούς αριθμούς και χωρίζονται με άνω κάτω τελεία (:). Ετσι, μία IPv4 διεύθυνση μπορεί να είναι η 167.112.22.8, ενώ μία IPv6 η 2001:3f2:55:1a3b:1200:af10:210:98. Υπάρχουν δύο κανόνες συντόμευσης των διευθύνσεων: α) μηδενικά που προηγούνται σε μία ομάδα μπορούν να απαλειφθούν και β) αν υπάρχουν συνεχόμενες ομάδες από μηδενικά σε μία IPv6 διεύθυνση, τότε αυτά αντικαθίσταται από "::". Για παράδειγμα, η 2001:abcd:cafe:0000:0000:0000:5 μπορεί να γραφτεί ως 2001:abcd:cafe::5. Επίσης, είναι πολύ διαφορετικές οι επικεφαλίδες των πακέτων στο IPv6, ώστε να ελαχιστοποιείται η κατεργασία τους από τους routers. Όπως είναι εύκολα αντιληπτό, τα δύο πρωτόκολλα δεν είναι συμβατά μεταξύ τους και έτσι ένα μηχάνημα που έχει μόνο IPv4 διεύθυνση δεν μπορεί να «μιλήσει» με κάποιο άλλο που έχει μόνο IPv6 διεύθυνση. Αναγκαστικά, λοιπόν, θα πρέπει να υπάρξουν κάποιοι μηχανισμοί μετάβασης από το ένα πρωτόκολλο στο άλλο. Λόγω της πολυπλοκότητας και του μεγέθους των IPv6 διευθύνσεων είναι πάρα πολύ σημαντική η σωστή χρήση του DNS. Η αναγωγή ενός ονόματος σε μία IPv4 διεύθυνση γίνεται μέσω του «A record», ενώ στο IPv6 μέσω του AAAA (quad A) record. Για το reverse lookup, αντί του domain in-addr.arpa υπάρχει πλέον το ip6.arpa. Στο σχεδιασμό του IPv6 είχε εισαχθεί για πρώτη φορά η έννοια του IPsec, το οποίο στην πορεία ενσωματώθηκε και στο IPv4. Μεγάλη, επίσης, σημασία έχει δοθεί στο IP Mobility, το οποίο περιγράφει ένα τρόπο κατά τον οποίο συσκευές μπορούν να μετακινούνται μεταξύ δικτύων, κρατώντας όμως την IP τους.

Την εμφάνισή τους όμως κάνουν και νέοι τύποι διευθύνσεων, καθώς και η έννοια του scope (πεδίο εφαρμογής) μίας διεύθυνσης. Ένας DHCP client στο IPv4 όταν δεν παίρνει απάντηση, κάνει ανάθεση μίας IP στο εύρος 169.254.0.0/16. Με την ανάθεση αυτής της διεύθυνσης είναι δυνατόν να επικοινωνήσει κανείς με τα υπόλοιπα μηχανήματα ενός LAN. Η αντίστοιχη περιοχή στο IPv6 είναι η ff80::/10 και οι διευθύνσεις αυτές ονομάζονται link-local και δεν είναι routable προς το Internet. Κάθε interface στον IPv6 κόσμο παίρνει μία link-local διεύθυνση και μέσω αυτής μπορεί και επικοινωνεί με το



**Χρονοδιάγραμμα εξάντλησης των IPv4 διευθύνσεων.**

υπόλοιπο τοπικό δίκτυο. Η loopback διεύθυνση στο IPv4 είναι η 127.0.0.1, ενώ στο IPv6 η ::1. Η loopback διεύθυνση και η link-local έχουν scope «link-local». Η αντίστοιχη περιοχή των private διευθύνσεων του IPv4 στο IPv6 είναι η fc00::/7 και ονομάζονται ULA (Unique Local Addresses, RFC4193). Ο τεράστιος αυτός χώρος των διευθύνσεων δημιουργήθηκε με σκοπό οι private διευθύνσεις σε κάθε LAN να είναι μοναδικές, παρ' όλο που δεν πρέπει να είναι routable στο Internet. Σε κάθε private LAN, δηλαδή, θα δημιουργείται μέσω ενός αλγορίθμου ένα ψευδο-τυχαίο subnet μέσα στο fc00::/7, το οποίο θα είναι σχεδόν μοναδικό στον κόσμο για κάθε LAN. Τέλος υπάρχουν οι «κανονικές» διευθύνσεις οι οποίες μαζί με τις ULA έχουν «global» scope.

Δεν τελειώνουν όμως εδώ οι διαφορές του IPv6 με το IPv4. Για αρχή, αλλάζει εντελώς ο τρόπος που αποκτάμε διευθύνσεις στο LAN μας με την εισαγωγή του SLAAC (StateLess Address AutoConfiguration) μέσω ICMPv6 μηνυμάτων πάνω από τις link-local διευθύνσεις. Ο συνηθισμένος τρόπος απόδοσης διευθύνσεων σε ένα LAN στην εποχή του IPv4 είναι το DHCP. Αυτό, στο IPv6 αλλάζει και πλέον οι routers στέλνουν ένα multicast Router Advertisement (RA) με τα πρώτα 64bit (prefix)

### Προβλήματα με ρυθμίσεις IPv6 σε Dual Stack

Στην περίπτωση που δεν υπάρχει σωστή συνδεσιμότητα με τον IPv6 κόσμο, δηλαδή, αν έχει φορτωθεί το IPv6 module, έχουν δηλωθεί IPv6 διευθύνσεις και routing το οποίο γίνεται μέσω πάρα πολύ αργού tunnel προς το Internet, τότε είναι σίγουρο ότι θα παρατηρηθούν μεγάλες δικτυακές δυσλειτουργίες. Αυτό συμβαίνει γιατί οι διευθύνσεις IPv6 έχουν «προτεραιότητα» έναντι των IPv4 όταν συνυπάρχουν και τα δύο πρωτόκολλα, οπότε το πρώτο DNS query που γίνεται για να μεταφραστεί ένα hostname είναι το AAAA record. Αν ο DNS server απαντήσει με μία IPv6 διεύθυνση τότε η σύνδεση θα δοκιμαστεί να γίνει πάνω από IPv6, και αν το upstream IPv6 link είναι αργό θα υπάρχουν σημαντικές καθυστερήσεις. Ιδιαίτερο πρόβλημα εμφανίζεται στους browsers επειδή για κάθε διεύθυνση/σύνδεσμο που χρειάζεται να επισκεφτούν γίνεται πρώτα το AAAA record query. Αν πάρουν απάντηση, προσπαθούν να συνδεθούν μέχρι να υπάρξει timeout (>20sec), οπότε και δοκιμάζουν A record query για την ύπαρξη IPv4. Ο Firefox έχει ρύθμιση για την απενεργοποίηση του AAAA lookup μέσω του about:config -> network.dns.disableIPv6. Αν η τιμή γίνει true τότε σταματά να ψάχνει για AAAA records και ρωτά άμεσα για A records..

## Θέμα - IPv6

μίας διεύθυνσης και τα υπόλοιπα 64bit τα συμπληρώνει ο client που λαμβάνει τα RA. Για αρχή, ο client χρησιμοποιώντας μία παραλλαγή της mac διεύθυνσης της κάρτας δικτύου που λέγεται EUI64, δημιουργεί τη link-local διεύθυνσή του. Έπειτα, κάνει ένα Duplicate Address Detection (DAD) για να διαπιστώσει αν τη διεύθυνση που πήρε τη χρησιμοποιεί κάποιος άλλος στο LAN. Αν όλα είναι εντάξει, τότε στέλνει ένα Router Solicitation μήνυμα, λαμβάνει το prefix και σε συνδυασμό με το EUI64 δημιουργεί την global διεύθυνση. Ένας router μπορεί να στείλει πολλά prefixes και οι clients να δημιουργήσουν διευθύνσεις για καθένα από αυτά τα prefixes.

Δυστυχώς, το SLAAC δεν προσφέρει το πλήθος των πληροφοριών που περιέχεται μέσα σε ένα μήνυμα DHCP, οπότε στην πορεία δημιουργήθηκε και το DHCPv6, το οποίο λειτουργεί με παρόμοιο τρόπο με αυτόν του κλασικού DHCP. Και για να γίνουν τα πράγματα ακόμη πιο... μπερδεμένα, σε έναν οικιακό χρήστη το πιθανότερο είναι ότι το CPE του θα πρέπει να υποστηρίζει και SLAAC και DHCPv6. Για παράδειγμα, μέχρι τώρα η τυπική διαδικασία σύνδεσης ενός CPE στο Internet είναι να κάνει το CPE ένα PPP connection με τον ISP, να πάρει μία IPv4 διεύθυνση στο PPP interface και έπειτα, μέσω DHCP, να μοιράσει private διευθύνσεις στο LAN, κάνοντας NAT με την public IPv4 διεύθυνση του PPP interface του router. Το σενάριο διευθυνσιο-

**Για όποιον θέλει να διαβάσει περισσότερα πράγματα σχετικά με το IPv6 υπάρχει ένα βιβλίο που παρέχεται δωρεάν με άδεια Creative Commons: <http://goo.gl/4iaon>.**

δότησης στον κόσμο του IPv6 όμως είναι αρκετά διαφορετικό. Ο router μέσω PPP συνδέεται με τον ISP και το PPP interface παίρνει μία link-local IPv6 διεύθυνση. Έπειτα, υπάρχει δυνατότητα πάνω από το link-local interface να γίνει λήψη των RA του ISP, ώστε να αποκτήσει και global IPv6 διεύθυνση στο PPP. Στη συνέχεια, ξεκινά η διαδικασία του «prefix-delegation» από το DHCPv6 client του CPE που παίρνει από τον DHCPv6 server του ISP ένα prefix (συνήθως /64 ή /56), μαζί με άλλες πληροφορίες όπως DNS, NTP, SIP κ.λπ. servers. Στη συνέχεια, το CPE αναμεταδίδει το prefix αυτό ως RA στο LAN και οι clients/PC συνθέτουν την IPv6 διεύθυνσή τους παίρνοντας ως πρώτα 64bits το prefix και τα άλλα 64bits από το EUI64 τους. Έχοντας οι clients πλέον global IPv6 διεύθυνση μπορούν να βγουν στο IPv6 Internet. Στον IPv4 κόσμο μέχρι τώρα μέσω του PPP γίνονταν ανάθεση μίας μοναδικής IP σε κάθε CPE, στον κόσμο του IPv6 όμως ένα /64 αντιστοιχεί σε  $2^{64}$  = 18.446.744.073.709.552.000 διαθέσιμες IPs! Αριθμός ολόκληρου του IPv4 Internet στο τετράγωνο για κάθε user ξεχωριστά!

### Μετάβαση στο νέο κόσμο

Δυστυχώς το θέμα της μετάβασης από τον κόσμο του IPv4 στο IPv6 θυμίζει το πρόβλημα της κότας και του αυγού. Οι ISPs λένε ότι δεν υπάρχουν αρκετά services στο Internet που να προσφέρουν υπηρεσίες σε IPv6 ώστε να επενδύσουν και να ξεκινήσουν να προσφέρουν IPv6 στους χρήστες τους. Από την άλλη, οι ιδιοκτήτες των υπηρεσιών υποστηρίζουν ότι δεν υπάρχουν αρκετοί χρήστες IPv6 ώστε να κάνουν αυτοί τη μετάβαση των υπηρεσιών τους σε IPv6. Η αλήθεια βρίσκεται φυσικά κάπου στη μέση, και πλέον όλοι έχουν αργήσει τόσο πολύ να ξεκινήσουν τη μετάβαση, ώστε βρίσκονται με την πλάτη στον τοίχο, λόγω της έλλειψης IPv4 διευθύνσεων. Φυσικά, ο ερχομός του IPv6 δεν σημαίνει πως θα εξαφανιστεί το IPv4 μέσα σε μία νύχτα. Οι πιο αισιόδοξες προβλέψεις μιλούν για 2 έως 3 χρόνια μετάβα-

σης, ενώ οι πιο απαισιόδοξες ακόμα και για 10 έως 15 χρόνια, έως ότου εξαλειφθεί εντελώς το περιεχόμενο που θα παρέχεται πάνω από IPv4.

Το λειτουργικό που είναι πιο έτοιμο να υποδεχτεί αυτόν το νέο κόσμο δεν είναι άλλο παρά το αγαπημένο μας Linux. Αυτή τη στιγμή, είναι το μοναδικό λειτουργικό που μπορεί να υποστηρίξει σε kernel και user-space SLAAC μαζί με RDNSS (Recursive DNS Server) extensions, καθώς και DHCPv6 εγγενώς. Ο πιο απλός τρόπος για να ξεκινήσει κάποιος να ασχολείται με τον κόσμο του IPv6 είναι, σε ένα μηχάνημα που ήδη έχει κάποια ή κάποιες IPv4 διευθύνσεις, να φορτώσει το IPv6 module (οι περισσότερες διανομές το κάνουν ήδη αυτόματα) και να προσθέσει κάποια global IPv6 διεύθυνση, εκτός της link-local. Η κατάσταση στην οποία ένα μηχάνημα χρησιμοποιεί και IPv4 και IPv6 διευθύνσεις ονομάζεται Dual-Stack. Όταν ο κόσμος αποκτήσει native IPv6 συνδέσεις προς το Internet οι περισσότεροι (αν όχι όλοι) οι υπολογιστές μας θα χρησιμοποιούν για κάποια χρόνια το dual stack, ώστε να έχουν πρόσβαση στον IPv4 και στον IPv6 κόσμο ταυτόχρονα. Μία υβριδική κατάσταση Dual-Stack, την οποία υποστηρίζουν κάποια σύγχρονα λειτουργικά, είναι αυτή στην οποία χρησιμοποιούνται οι λεγόμενες IPv4-mapped IPv6 διευθύνσεις, στις οποίες τα πρώτα 80bit είναι μηδενικά, τα επόμενα 16bit είναι 1, ενώ τα υπόλοιπα 32bit αποτελούνται από την IPv4 διεύθυνση. Ένα παράδειγμα είναι μία διεύθυνση της μορφής ::ffff:123.56.12.90.

Ένας δεύτερος τρόπος σύνδεσης είναι να χρησιμοποιηθεί κάποιος από τους διαθέσιμους μηχανισμούς tunneling. Μέσω αυτών των μηχανισμών μπορεί κανείς να ενθυλακώσει IPv6 πακέτα μέσα σε IPv4 μέχρι αυτά να φτάσουν σε ένα gateway το οποίο μιλά και τα δύο πρωτόκολλα, και το οποίο αφαιρεί την ενθυλάκωση ώστε το IPv6 πακέτο να προχωρήσει στον προορισμό του. Αντίστοιχη διαδρομή θα ακολουθήσει το πακέτο και στην επιστροφή του στο αρχικό μηχάνημα. Υπάρχουν πολλοί διαφορετικοί μηχανισμοί για tunneling που χωρίζονται κυρίως σε δύο υποκατηγορίες: σε αυτά που τα άκρα τους ορίζονται αυτοματοποιημένα, και σε εκείνα που χρειάζονται ρύθμιση από το χρήστη. Ο πιο διαδεδομένος μηχανισμός αυτοματοποιημένου tunneling είναι το 6to4. Για τα 6to4 tunnels υπάρχει ένα δεσμευμένο εύρος διευθύνσεων, το 2002::/16 και μία anycast IPv4 διεύθυνση, η 192.88.99.1. Όταν κάποιο μηχάνημα έχοντας μία IPv4 διεύθυνση θέλει να συνδεθεί μέσω 6to4 στο IPv6, τότε δημιουργεί ένα tunnel με το 192.88.99.1., ενώ ταυτόχρονα παίρνει μία IPv6 διεύθυνση που τα πρώτα του 16bit είναι το 2002, τα επόμενα 32bit είναι η IPv4 διεύθυνσή του μετασχηματισμένη σε δεκαεξαδικό, προστίθενται 16bit για subnet και ακολουθούν τα 64bit για το host. Για τη διεύθυνση 195.200.35.4 η αντίστοιχη 6to4 είναι η: 2002:C3C8:2304::/48. Η μετεξέλιξη του 6to4 ονομάζεται 6rd (Rapid Deployment) και έχει σχεδιαστεί με τέτοιο τρόπο ώστε οι ISPs να έχουν μεγαλύτερο έλεγχο των πελατών που συνδέονται στους 6to4 relay gateways. Η διαφορά τους έγκειται στο ότι το IPv4 άκρο δεν χρειάζεται να είναι το anycast 192.88.99.1, αλλά ορίζεται από κάθε ISP. Επίσης, το IPv6 subnet το ορίζει ο κάθε ISP από αυτό που του έχει ανατεθεί. Από εκεί και πέρα, υπάρχουν διάφοροι μη αυτόματοι μηχανισμοί tunneling που παρέχονται από υπηρεσίες στο Internet, όπως το sixxs.org, το he.net, το gogo6.com κ.λπ. Στις περιπτώσεις αυτές κάποιος χρειάζεται να κάνει register ένα account, να του αποδοθεί ένα IPv6 prefix και έπειτα ξεκινά είτε κάποιο dedicated client είτε δίνει εντολές μέσω γραμμής εντολών και δημιουργείται ένα tunnel προς κάποιους 6-to-4 relays, ώστε έχει πρόσβαση στον IPv6 κόσμο.

### Σύνδεση στον IPv6 κόσμο



Ο πιο εύκολος τρόπος σύνδεσης στο IPv6 για κάποιον που δεν έχει native IPv6 πρόσβαση, αλλά διαθέτει μία δημόσια IPv4 διεύθυνση στο μηχάνημά του είναι να χρησιμοποιήσει το 6to4. Στην περίπτωση που υπάρχει NAT τότε πρέπει είτε να γίνει προώθηση του protocol 41 (ipn6) προς το μηχάνημα που θα ξεκινήσει το tunnel είτε να χρησιμοποιηθεί κάποιος ειδικός client, π.χ., AICCU για το sixxs.net. (Για να αποκτήσει κάποιο LAN μηχάνημα μία δημόσια IPv4 διεύθυνση θα πρέπει να είναι αυτό το οποίο θα κάνει την PPP σύνδεση. Η διαδικασία είναι αρκετά απλή, αρκεί το CPE να υποστηρίζει bridge mode-RFC1483). Για να δημιουργηθεί ένα 6to4 tunnel σε μηχάνημα με δημόσια IPv4 (έστω 56.123.123.21) χρειάζεται να μετατραπεί πρώτα η v4 διεύθυνση σε hex και να προστεθεί ύστερα από το prefix 2002:

```
# printf "2002:%02x%02x:%02x%02x::1\n" `echo
56.123.123.21 | tr . '\`
2002:387b:7b15::1
```

Επειτα, πρέπει να δημιουργηθεί το tunnel (θα πρέπει να υπάρχει εγκατεστημένο το πακέτο iproute):

```
# ip tunnel add tun6to4 mode sit remote any local
56.123.123.21
# ip link set dev tun6to4 mtu 1472 up
Na αποδοθεί η 6to4 διεύθυνση
# ip -6 addr add 2002:387b:7b15::1/16 dev tun6to4
Τέλος, να μπου κανόνες για routing
# ip -6 route add ::0 via ::192.88.99.1 dev tun6to4 met-
ric 10
```

```
# ip -f inet6 addr
```

Αν όλα λειτουργήσαν σωστά:

```
# ping6 www.ntua.gr
PING www.ntua.gr(achilles.noc.ntua.gr) 56 data bytes
64 bytes from achilles.noc.ntua.gr: icmp_seq=1 ttl=61
time=
84.5 ms
64 bytes from achilles.noc.ntua.gr: icmp_seq=2 ttl=61
time=84.9 ms
```

Μέσω ενός browser μπορεί κανείς πλέον να επισκεφθεί IPv6 διευθύνσεις, π.χ., <http://ipn6.google.com>. Αν κάποιος επιθυμεί να έχει πρόσβαση μέσω IP σε μία IPv6 υπηρεσία, τότε πρέπει να κλείσει την IP στο url μέσα σε "[ ]". Για παράδειγμα: [http://\[2001:648:2000:de::210\]](http://[2001:648:2000:de::210]). Αυτό χρειάζεται για να ξεχωρίζει η IPv6 διεύθυνση από την πόρτα πρόσβασης, η οποία πάλι δηλώνεται με ":" μετά το κλείσιμο της αγκύλης.

Το επόμενο βήμα είναι να λειτουργήσει κάποιος ως IPv6 gateway για τα υπόλοιπα μηχανήματα του LAN του και να μπορεί να τους μοιράζει IPs μέσω RA. Αυτό μπορεί να γίνει εγκαθιστώντας το πακέτο radvd και ενεργοποιώντας το forwarding για IPv6.

```
# echo net.ipv6.conf.all.forwarding = 1 >> /etc/sysctl.conf
# sysctl -p
```

Για το παραπάνω παράδειγμα με την PPP σύνδεση (ppp0) και το LAN πίσω από την eth1, ένα τυπικό config file για radvd θα ήταν:

```
interface eth1 {
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    AdvSendAdvert on;
    prefix 0:0:0:1::/64 {
        AdvOnLink on;
        AdvAutonomous on;
        AdvValidLifetime 86400;
        AdvPreferredLifetime 86400;
        Base6to4Interface ppp0;
```

```
AdvRouterAddr on;
```

```
};
```

```
};
```

Για σύνδεση πίσω από NAT, όπως αναφέρθηκε και παραπάνω, είναι προτιμότερη η χρήση ενός client. Για σύνδεση στο sixxs.net χρειάζεται απλώς ένα account, η εγκατάσταση του πακέτου aiccu, καθώς και ένα config όπως το παρακάτω:

```
username demo-user-gr
password demo-pass-gr
ipv6_interface sixxs
protocol tic
server tic.sixxs.net
#tunnel_id TXXXXX
verbose false
daemonize true
automatic true
requireetis false
makebeats true
behindnat true
```

Είναι σημαντικό να θυμόμαστε ότι στον κόσμο του IPv6 κάθε μηχάνημα έχει μία ή παραπάνω δημόσιες IPs, άρα ακόμη και τα μηχανήματα στο «LAN» είναι προσβάσιμα από τον έξω κόσμο. Για να αποφύγουμε δυσάρεστες εκπλήξεις, καλό είναι να εφαρμόσουμε κάποιους κανόνες firewalling σε κάθε μηχανήμα μέσω της IPv6 έκδοσης των iptables που ονομάζονται ip6tables. Προσοχή μόνο στα ICMPv6 μηνύματα, τα οποία είναι πάρα πολύ σημαντικά για τη λειτουργία του IPv6 και δεν θα πρέπει να κόβονται ή τουλάχιστον να κόβονται συγκεκριμένα μηνύματα πάρα πολύ προσεκτικά, αλλιώς ενδέχεται να υπάρχουν σοβαρά προβλήματα. Από εκεί και πέρα, ο κόσμος του IPv6 είναι ανοιχτός για εξερεύνηση!

## Προς το μέλλον

Κάθε μέρα όλο και περισσότερα services αρχίζουν και υποστηρίζουν IPv6 και ήδη οι μεγάλοι πάροχοι πληροφοριών όπως το Google (<http://ipn6.google.com>) και το Facebook (<http://www.v6.facebook.com>) είναι αρκετά έτοιμοι. Αν και στο εξωτερικό υπάρχουν αρκετοί πάροχοι που ήδη προσφέρουν στους πελάτες τους native IPv6 συνδέσεις για χρόνια, στην Ελλάδα δεν υπάρχει κάτι επίσημο ακόμα. Ομως κάποιοι Έλληνες πάροχοι βρίσκονται σε στάδιο προετοιμασίας και δοκιμών και δεν αποκλείεται μέσα στους επόμενους μήνες να αρχίσει κάποιο πιλοτικό πρόγραμμα για όσους έχουν τερματικό εξοπλισμό που υποστηρίζει IPv6. Πιλοτική υλοποίηση έχει γίνει επίσης και στο πλαίσιο του φοιτητικού DSL (Δίοδος). Η μετάβαση στον κόσμο του IPv6 είναι αναπόφευκτη, όσο νωρίτερα αρχίσει η χρήση του τόσο μεγαλύτερη θα είναι η εξοικείωση και τόσο πιο έτοιμος μπορεί να αισθάνεται κάποιος για τη μέρα του IPv4 Apocalypse που πλησιάζει!

## Σύνδεσμοι:

- [1] <http://www.ipv6actnow.org/>
- [2] <http://bgp.potaroo.net/v6/v6rpt.html>
- [3] <http://www.potaroo.net/tools/ipv4/index.html>
- [4] <http://ipn6.he.net/statistics/>
- [5] <http://www.sixxs.net/>
- [6] <http://www.6deploy.eu/>
- [7] <http://www.ipv6-taskforce.gr/>
- [8] <http://ipn6.otenet.gr>