



Προγραμματισμός Διαχείρισης Συστημάτων ΙΙ

Μάθημα 8ο
Δικτύωση TCP/IP



Μιχαηλίδης Παναγιώτης

Περιεχόμενα

- Δικτύωση TCP/IP
 - Τι είναι το TCP/IP;
 - Επίπεδα, διευθύνσεις, NAT
 - Πρωτόκολλα: ARP, DHCP

TCP/IP

- Η πιο κοινή στοίβα πρωτοκόλλων δικτύωσης
- Τυπικά οι δικτυακές εφαρμογές χρησιμοποιούν ένα από τα παρακάτω πρωτόκολλα μεταφοράς:
 - TCP - Transmission Control Protocol
 - UDP - User Datagram Protocol
- Όλη η κυκλοφορία πραγματοποιείται από το IP - Internet Protocol

Πρωτόκολλα

- IP
 - Πακετοστραφής (οι δρομολογητές δεν φροντίζουν τι περιέχει μέσα στα πακέτα)
- TCP
 - Συνδεσιοστρεφής, χειραψία δυο φάσεων, αξιόπιστο
 - Έλεγχος συμφόρησης - επιβραδύνει όταν υπάρχει συμφόρηση, επιταχύνει όταν είναι διαθέσιμοι οι πόροι
 - Ροή ελέγχου - δεν καταβάλλεται ο παραλήπτης
- UDP
 - Αναξιόπιστο, αλλά γρήγορη/εύκολη μεταφορά των ξεχωριστών πακέτων

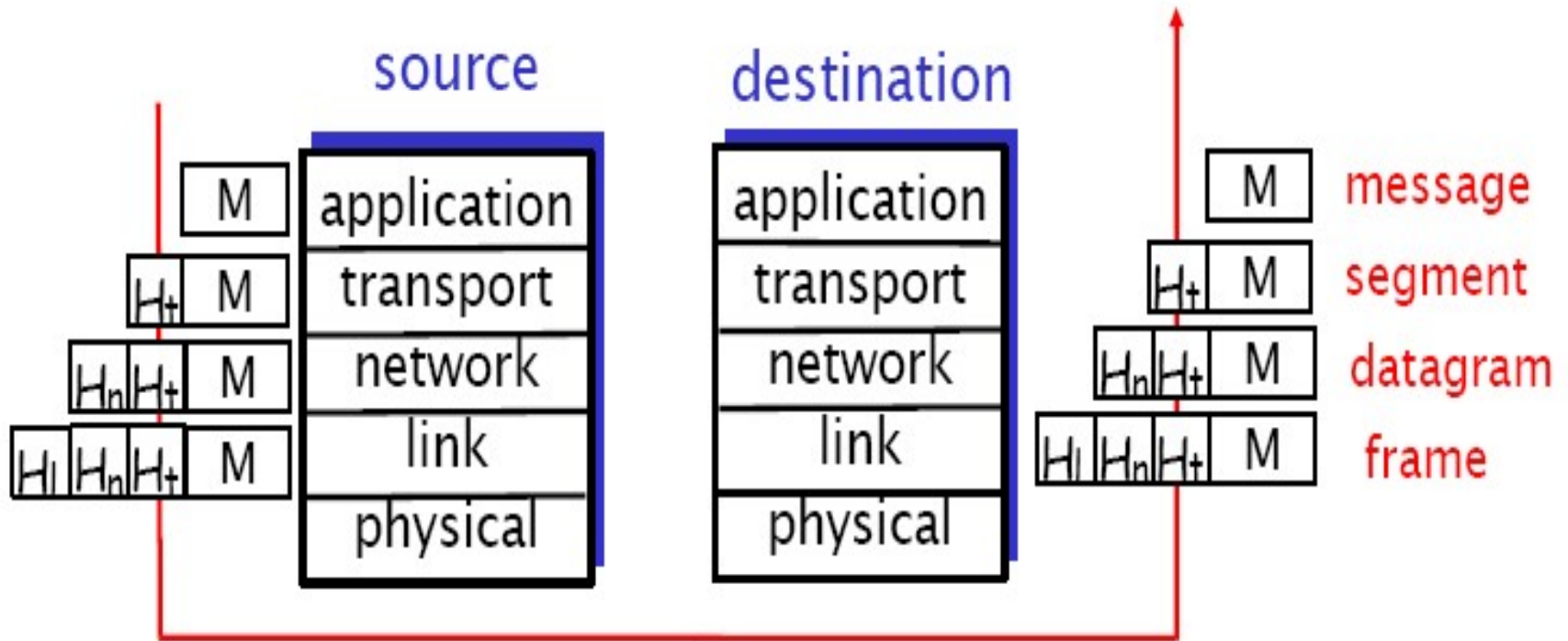
Επίπεδα δικτύων

- Επίπεδο εφαρμογής - εφαρμογές τελικού χρήστη
- Επίπεδο μεταφοράς - παράδοση των δεδομένων ανάμεσα στις εφαρμογές
- Επίπεδο δικτύου - βασική επικοινωνία, διεθυσιοδότηση, δρομολόγηση και πολύπλεξη
- Επίπεδο σύνδεσης - υλικό δικτύων και οδηγόι συσκευών
- Φυσικό επίπεδο - καλώδια ή φυσικά μέσα

Ενθυλάκωση

- Καθώς τα δεδομένα στέλνονται προς τα κάτω διαμέσου της στοίβας, τα δεδομένα ενθυλακώνονται με επικεφαλίδες του κάθε επιπέδου
- Π.χ.
 - Το επίπεδο εφαρμογής στέλνει 100 bytes
 - Το UDP προσθέτει 8 bytes της επικεφαλίδας
 - Το IP προσθέτει 20 bytes
 - Το Ethernet προσθέτει 18 bytes

Επίπεδα + Ενθυλάκωση



Διευθυνσιοδότηση

- Τα διαφορετικά επίπεδα χρησιμοποιούν διαφορετική διευθυνσιοδότηση
 - Το επίπεδο εφαρμογής επιτρέπει στους ανθρώπους να χρησιμοποιούν ονόματα υπολογιστών
 - Το επίπεδο δικτύου (IP) απαιτεί διευθύνσεις IP
 - Το επίπεδο σύνδεσης απαιτεί διευθύνσεις MAC
 - π.χ. Ethernet (48 bits)
 - Τα πρώτα 3 bytes είναι το ID του κατασκευαστή
 - Τα τελευταία 3 bytes είναι ο σειριακός αριθμός
- Οι θύρες αναγνωρίζουν διεργασία ή υπηρεσία σε ένα υπολογιστή
 - Στο αρχείο `/etc/services` περιέχει μια λίστα των δημοφιλών θυρών
 - Θύρες ≤ 1024 είναι δεσμευμένες

Τύπους διευθύνσεων

- Το επίπεδο IP και το επίπεδο σύνδεσης έχουν πολλαπλούς τύπους διευθύνσεων
 - Unicast - ένας υπολογιστής (κάρτα δικτύου)
 - Broadcast - διευθύνσεις που περιλαμβάνουν όλους τους υπολογιστές σε ένα συγκεκριμένο δίκτυο
 - Όλα τα bits του τμήματος διεύθυνσης υπολογιστή είναι 1
 - Multicast - διευθύνσεις που αναγνωρίζουν μια ομάδα υπολογιστών
 - Διευθύνσεις IP με πρώτο byte στο 224-239

Διευθύνσεις IP

- Η διεύθυνση IPv4 έχει 4 bytes (ή 32 bits)
 - Διαχωρίζεται σε δύο τμήματα: δίκτυο και υπολογιστής
 - Αρχικά το διαδίκτυο χρησιμοποιούσε κλάσεις διευθύνσεων IP

Κλάση	1ο byte	Δομή	Σχόλια
A	1-126	Δ.Υ.Υ.Υ	Πολύ αρχικά δίκτυα
B	128-191	Δ.Δ.Υ.Υ	Μεγάλες τοποθεσίες
C	192-223	Δ.Δ.Δ.Υ	Μικρότερες τοποθεσίες
D	224-239		Διευθύνσεις multicast
E	240-255		Πειραματικό

– 128.180.2.57

- Κλάση B (128.180), υπολογιστή (2.57)

Διευθύνσεις κλάσης A

- Το τμήμα δίκτυο είναι τα πρώτα 8 bits
- Το τμήμα υπολογιστή είναι τα τελευταία 24 bits
- Οι διευθύνσεις IP κυμαίνονται από 1.x.x.x έως 126.x.x.x
- Αριθμός δικτύων < 128 (2^7)
- Μέγιστος αριθμός υπολογιστών ανά δίκτυο: 16777216 (2^{24})

Διευθύνσεις κλάσης B

- Το τμήμα δίκτυο είναι τα πρώτα 16 bits
- Το τμήμα υπολογιστή είναι τα τελευταία 16 bits
- Οι διευθύνσεις IP κυμαίνονται από 128.x.x.x έως 191.x.x.x
- Αριθμός δικτύων < 16384 (2^{14})
- Μέγιστος αριθμός υπολογιστών ανά δίκτυο: 65536 (2^{16})

Διευθύνσεις κλάσης C

- Το τμήμα δίκτυο είναι τα πρώτα 24 bits
- Το τμήμα υπολογιστή είναι τα τελευταία 8 bits
- Οι διευθύνσεις IP κυμαίνονται από 192.x.x.x έως 223.x.x.x
- Αριθμός δικτύων < 2097152 (2^{21})
- Μέγιστος αριθμός υπολογιστών ανά δίκτυο: 256 (2^8)

Διευθύνσεις κλάσης D

- Διεύθυνση πολυεκπομπής
- Δεν υπάρχει τμήμα δίκτυο
- Η διεύθυνση πολυεκπομπής είναι τα τελευταία 28 bits
- Οι διευθύνσεις IP κυμαίνονται από 224.x.x.x έως 239.x.x.x
- Αριθμός ομάδων πολυεκπομπής $< 268435456 (2^{28})$

Υποδικτύωση

- Τα ξεχωριστά δίκτυα είναι συχνά πολύ μικρότερα από τα μεγέθη των κλάσεων
- Η υποδίκτυωση επιτρέπει το σπάσιμο μιας διανομής σε πολλαπλά μικρότερα δίκτυα
- Ένας οργανισμός μπορεί χωρίζει την κλάση B σε πολλά μικρότερα δίκτυα, όπως
 - 128.180.5.*, 128.180.98.*, 128.180.14.*

CIDR

- Classless Inter-Domain Routing
 - Επιτρέπει για μικρότερες δικτυακές διευθύνσεις από την κλάση - απόλυτες κλάσεις δικτύου
 - Απαιτεί το πεδίο μήκος π.χ. 128.160.0.0/16
 - Συλλέγει μικρότερα δίκτυα σε ένα μεγάλο δίκτυο
 - $192.200.254.0 + 192.200.255.0 = 192.200.254.0/23$
 - Μπορεί να διανείμει τμήματα των διευθύνσεων της κλάσης A και B
 - Συλλογικά δίκτυα μειώνουν το μέγεθος του πίνακα δρομολόγησης

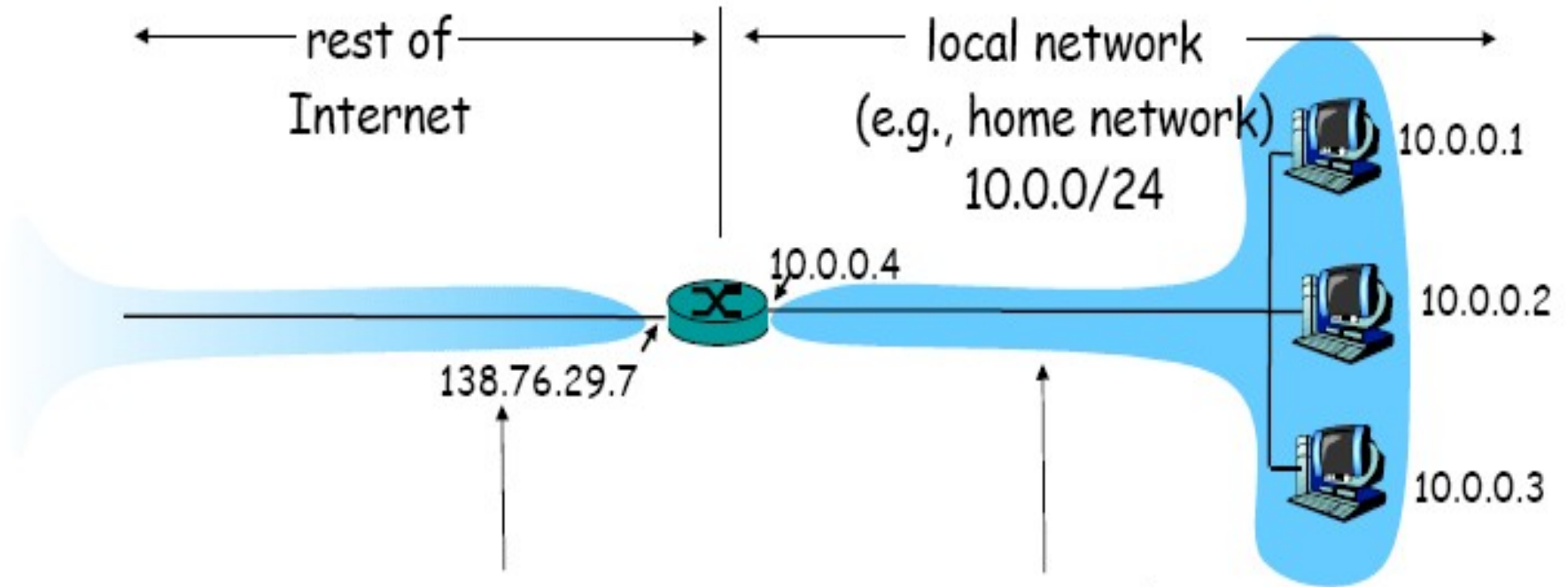
Έλλειψη διευθύνσεων

- Πριν CIDR υπήρχαν αρκετές διευθύνσεις
 - Οι κλάσεις B ήταν από το 1995
 - Οι πίνακες δρομολογητών ήταν πλημμυρισμένες
- CIDR + NAT + όνομα βασισμένη στο εικονικό υπολογιστή επιβραδύνει την διανομή IP
- IPv6 λύνει το πρόβλημα αυτό (διευθύνσεις 16 bytes)

NAT

- Network Address Translation
 - Ο δρομολογητής λαμβάνει τα πακέτα, αντικαθιστά τις εσωτερικές δικτυακές διευθύνσεις και θύρες με εξωτερικές ορατές διευθύνσεις και θύρες
 - Διατηρεί απεικόνιση έτσι ώστε τα εξωτερικά πακέτα να κατευθύνονται στο κατάλληλο εσωτερικό υπολογιστή
 - Τυπικά χρησιμοποιεί μια δημόσια διεύθυνση IP, πολλές θύρες αλλά μπορεί (θεωρητικά) να απεικονίσει αφηρημένα θύρες/υπολογιστές
 - Ενσωματωμένη σε πολλούς δρομολογητές, Linux

NAT: Network Address Translation



Ειδικές διευθύνσεις

- 127.0.0.1
 - Διεύθυνση βρόχου επιστροφής
 - Απλοποιεί τον προγραμματισμό δικτυακών εφαρμογών
 - Το αντίστοιχο όνομα της διεύθυνσης επιστροφής είναι το localhost
- 0.0.0.0
 - Διεύθυνση δικτύου
 - Απλοποιεί τους πίνακες δρομολόγησης για αναφορά σε ολόκληρα δίκτυα
- Μια διεύθυνση με 1 σε όλα τα bits στο τμήμα υπολογιστή λέγεται διεύθυνση εκπομπής

Ιδιωτικές διευθύνσεις

- Ενώ η NAT μπορεί να προστατεύει τις εσωτερικές διευθύνσεις από το να είναι ορατές στις επικεφαλίδες IP, δεν είναι τέλειο
 - Μερικές εφαρμογές θα κωδικοποιούν τις διευθύνσεις σε δεδομένα
 - Τι θα γίνει αν θέλουμε πραγματικά να συνδεθούμε με ένα εξωτερικό υπολογιστή που έχει διεύθυνση IP ίδια με ένα εσωτερικό υπολογιστή;
- Οι περισσότεροι χρησιμοποιούν ιδιωτικό χώρο διευθύνσεων (unroutable)

Κλάση IP	Από	Προς	Διάστημα CIDR
A	10.0.0.0	10.255.255.255	10.0.0.0/8
B	172.16.0.0	172.31.255.255	172.16.0.0/12
C	192.168.0.0	192.168.255.255	192.168.0.0/16

ARP: Address Resolution Protocol

- Αφού προσδιοριστεί η δρομολόγηση ενός πακέτου, πρέπει να μεταδοθεί στην επόμενη πύλη ή υπολογιστή του τοπικού δικτύου
- Οι μεταδόσεις LAN χρησιμοποιούν διευθύνσεις LAN
- Το ARP χρησιμοποιείται για να αποκαλύψει την διεύθυνση υλικού της διεύθυνσης IP στόχου
- Το ARP στέλνει μια εκπομπή LAN ζητώντας ποιος υπολογιστής έχει την επιθυμητή διεύθυνση IP. Ο ιδιοκτήτης ανταποκρίνεται με ένα μήνυμα Unicast που περιέχει την απάντηση
 - Τα αποτελέσματα αποθηκεύονται κρυφά σε ένα πίνακα

Δείγμα πίνακα ARP

```
% arp -a
```

```
Net to Media Table: IPv4
```

Device	IP Address	Mask	Flags	Phys Addr
eri0	proxima	255.255.255.255		08:00:20:86:2f:72
eri0	genie-plab	255.255.255.255		08:00:20:80:83:c4
eri0	128.180.123.254	255.255.255.255		00:d0:02:13:44:00
eri0	ariel	255.255.255.255	SP	00:03:ba:27:95:90
eri0	dhcp123-114	255.255.255.255		00:0c:6e:94:15:de

Δρομολόγηση

- Δρομολογητές και πίνακας δρομολόγησης
- Οι δρομολογητές μετακινούν τα πακέτα από δίκτυο σε δίκτυο
 - Τα πακέτα που προορίζονται στο ίδιο τοπικό δίκτυο αποστέλονται άμεσα στον υπολογιστή προορισμού
 - Τα πακέτα που προορίζονται σε διαφορετικό δίκτυο, τότε προωθούνται σε ένα υπολογιστή πύλης ή δρομολογητής
 - Οι δρομολογητές βρίσκονται σε περισσότερα από ένα δίκτυο
 - Οι αποφάσεις δρομολόγησης λαμβάνονται με βάση τη διεύθυνση δικτύου
 - Το τμήμα δικτύου προσδιορίζεται με την εφαρμογή της μάσκας δικτύου
 - Οι δρομολογητές χρησιμοποιούν τον πίνακα δρομολόγηση για αναζήτηση δρομολογίων σε άλλα δίκτυα

Παραμετροποίηση δικτύου

- Προσθήκη ενός υπολογιστή σε ένα LAN
 - Ανάθεση μιας μοναδικής διεύθυνσης IP και όνομα υπολογιστή (ανά κάρτα)
 - Θέτουμε τον υπολογιστή να παραμετροποιήσει τις κάρτες δικτύου κατά τον χρόνο εκκίνησης
 - Θέτουμε την εξ ορισμού δρομολόγηση
 - Αναφορά σε ένα διακομιστή ονομάτων DNS
- Αρχεία
 - `/etc/sysconfig/network-scripts/ifcfg-eth0`
 - Όνομα υπολογιστή, εξ ορισμού δρομ, διεύθυνση IP, μάσκα δικτύου, εκπομπή
- Το DHCP θα μπορούσε να κάνει όλα αυτά αυτόματα

Απεικόνιση ονομάτων σε διευθύνσεις IP

- Τρεις επιλογές: /etc/hosts, NIS, DNS
- Απλούστερη: /etc/hosts

```
% more /etc/hosts
```

```
#
```

```
# Internet host table
```

```
#
```

```
127.0.0.1 localhost
```

```
128.180.120.15 proxima
```

```
128.180.120.9 mailhost
```

```
128.180.120.103 ariel # Added by DHCP
```

- Δουλεύει όταν το NIS ή DNS είναι διάσπαση
 - π.χ. στο χρόνο εκκίνησης

ifconfig

- Παραμετροποίηση κάρτα δικτύου με `ifconfig`
 - `ifconfig eth0 128.138.240.1 netmask 255.255.255.0`
`up`
 - Εμφάνιση configuration π.χ. για Linux
 - `ifconfig -a`

Αρχεία παραμετροποίησης RH/Fedora

- `/etc/sysconfig/network`
 - Όνομα υπολογιστή, εξ ορισμού πύλη (GATEWAY)
- `/etc/sysconfig/static-routes`
 - Στατικές δρομολ
- `/etc/resolv.conf`
 - Αναφορές σε διακομιστές ονομάτων
- `/etc/sysconfig/network-scripts/ifcfg-XXXX`
 - Διεύθυνση IP, μάσκα δικτύου, διεύθυνσης εκπομπής ανά κάρτα
 - π.χ., `eth0`, `eth1`, `lo`
- Χρήση `ifup` και `ifdown` για να αλλάξουμε την κατάσταση της κάρτας ή χρήση `/etc/init.d/network`

DHCP

- Dynamic Host Configuration Protocol
- Οι πελάτες ενοικιάζουν την παραμετροποίηση δικτύου από το διακομιστή
 - Διευθύνσεις IP και μάσκες δικτύου
 - Πύλες
 - Διακομιστές ονομάτων DNS
 - Syslog υπολογιστών
 - Διακομιστές X, διακομιστές proxy
 - και περισσότερα

Πως λειτουργεί το DHCP;

- Ο πελάτης στέλνει ένα μήνυμα "Who am I?"
- Ο τοπικός διακομιστής DHCP απαντά με ενοικίαση παραμετροποίηση δικτύου
- Όταν η ενοικίαση λήγει, ο πελάτης ανανεώνει την ενοικίαση
 - Ο διακομιστής DHCP πρέπει να κρατά πληροφορίες ενοικίασης

Παραμετροποίηση dhcpd

```
#dhcpd.conf
```

```
#
```

```
option subnet-mask 255.255.255.0;
```

```
default-lease-time 600;
```

```
max-lease-time 7200;
```

```
subnet 192.168.1.0 netmask 255.255.255.0 {
```

```
    range 192.168.1.51 192.168.1.60;
```

```
    option broadcast-address 192.168.1.255;
```

```
    option routers gw.synack.net;
```

```
}
```

```
subnet 209.180.251.0 netmask 255.255.255.0 {
```

```
}
```

```
host gandalf {
```

```
    hardware ethernet 08:00:07:12:34:56;
```

```
    fixed-address gandalf.synack.net;
```