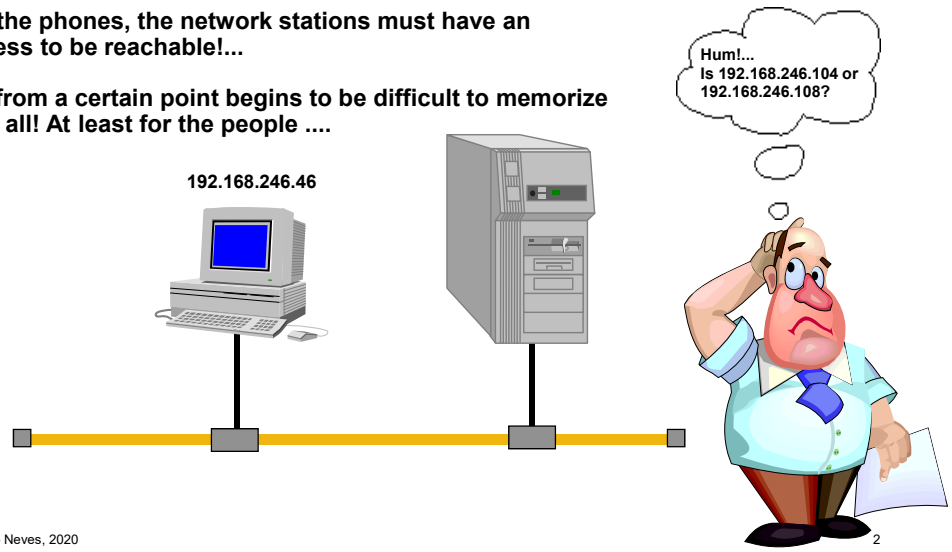
Naming and Addressing
The DNS Service

Joao.Neves@fe.up.pt

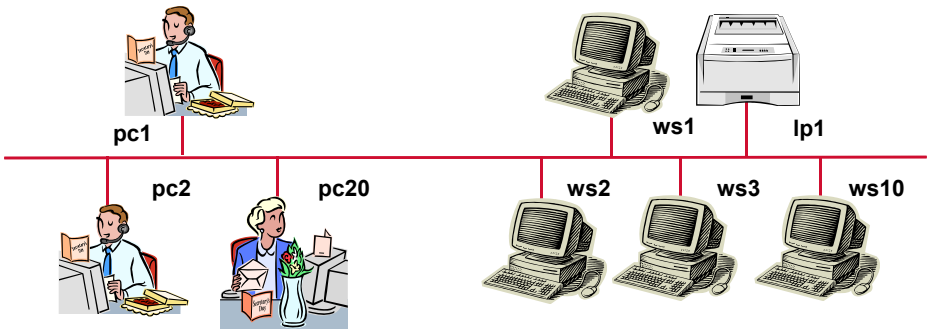
Naming Systems?! ...

Like the phones, the network stations must have an address to be reachable!...

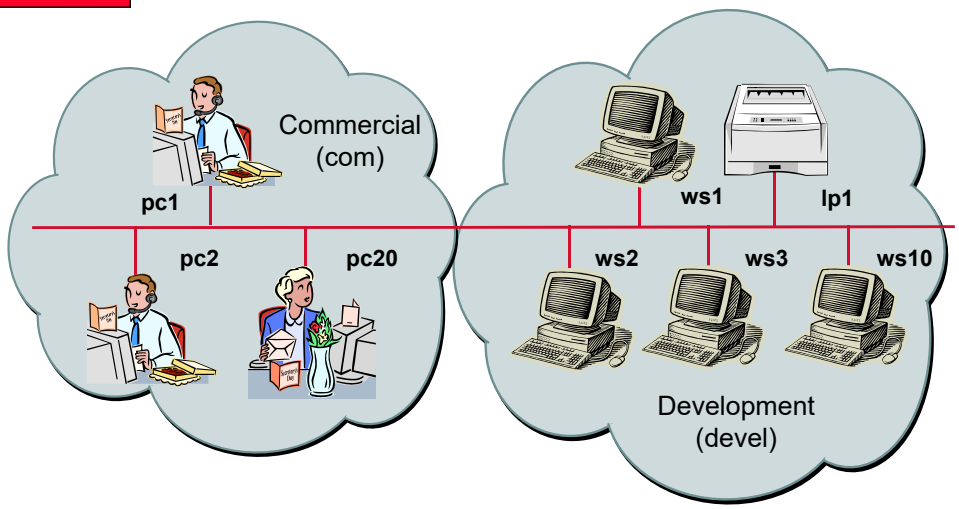
And from a certain point begins to be difficult to memorize them all! At least for the people ....



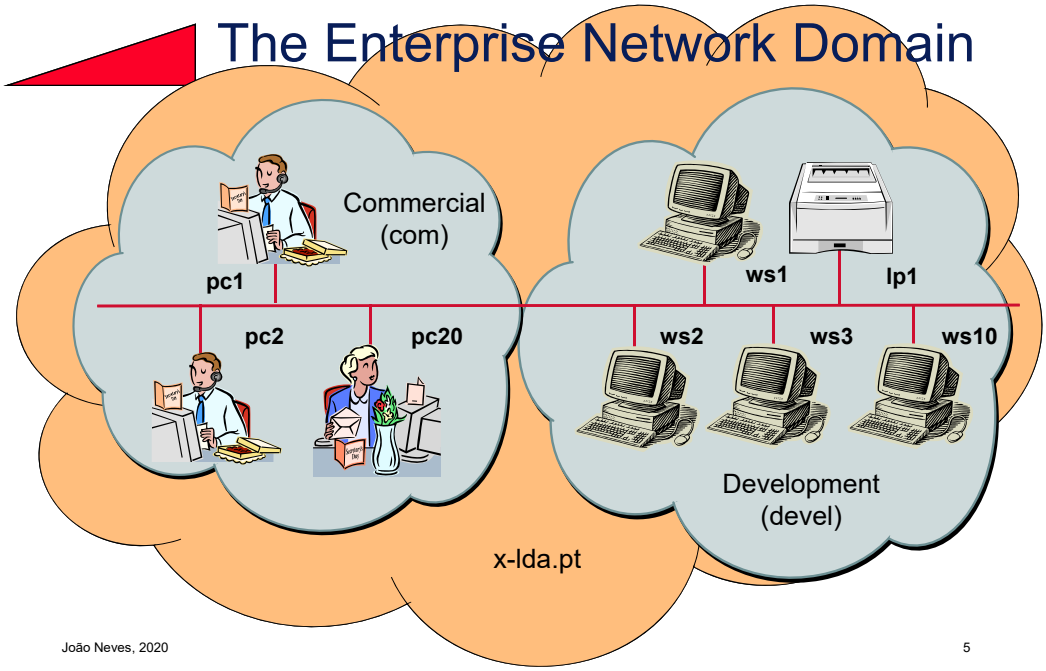
The Enterprise Network



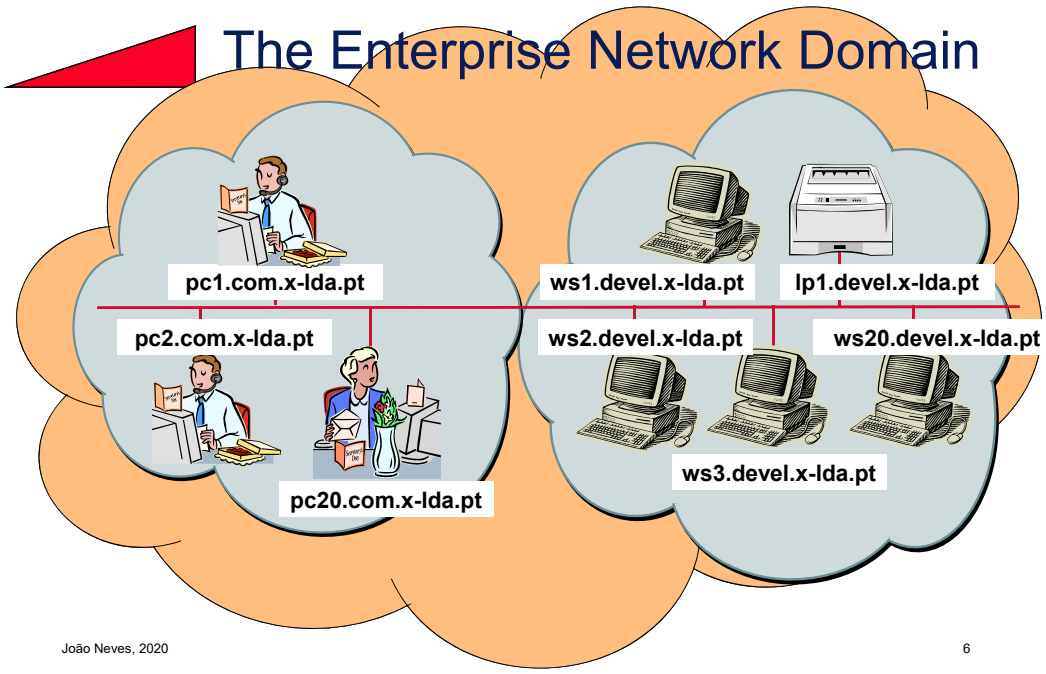
Stations by Department…



The Enterprise Network Domain



The Enterprise Network Domain



The *hosts* file

- The *hosts* is a readable ASCII text file
- Contains the addresses and names of the systems on the network that we want them to be recognized locally
- On Unix operating systems exists in the directory `/etc`

```
#
#       TCP/IP hosts database
#
127.0.0.1        localhost loopback lb
192.35.246.1     animal.inescn.pt animal
192.35.246.7     gonzo.inescn.pt
192.35.246.9     bart.inescn.pt bart
```

disadvantages:
- need to maintain an updated file
- maintain the same version on all machines
- problem of non-existence of all addresses in the file
- the user is required to know the technical details

Domain Name System

The "Domain Name System" (DNS) is the service that translates a domain name into an IP address in its numeric form, and vice versa.

`pc1.com.x-lda.pt` ⟷ `[192.168.9.200]`

Generically, the name of a node in the network will be:

nodarede . subdominio . dominio . dominioprincipal

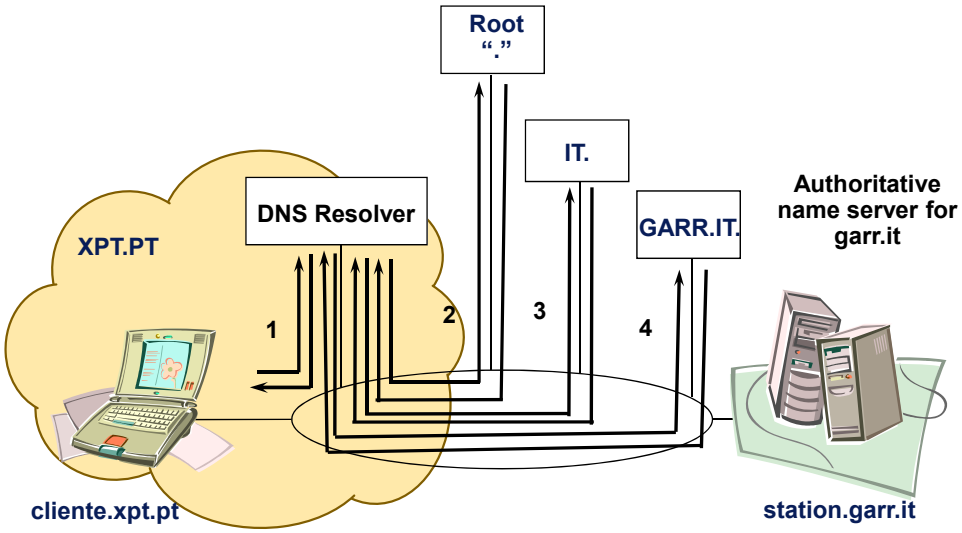
NODAREDE . SUBDOMINIO . DOMINIO. DOMINIOPRINCIPAL

noDarEDe . subDoMIniO . DoMIniO. dominioprinciPAL

Berkeley Internet Name Domain

- In the beginning was maintained centrally, by SRI International Inc, a table with the IP addresses in a file named “hosts;
- In 1983 Paul Mockapetris created the DNS service;
- BIND was one of the first implementations of the DNS service;
- BIND was created with the goal of disseminating the “hosts” file to the network;
- The Unix daemon that implements the BIND is “named”.

DNS Operation



Important Name Servers

- **Root Name Servers**
  - `A.ROOT-SERVERS.NET.`
  - `B.ROOT-SERVERS.NET.`
  - `...`
  - `M.ROOT-SERVERS.NET.`

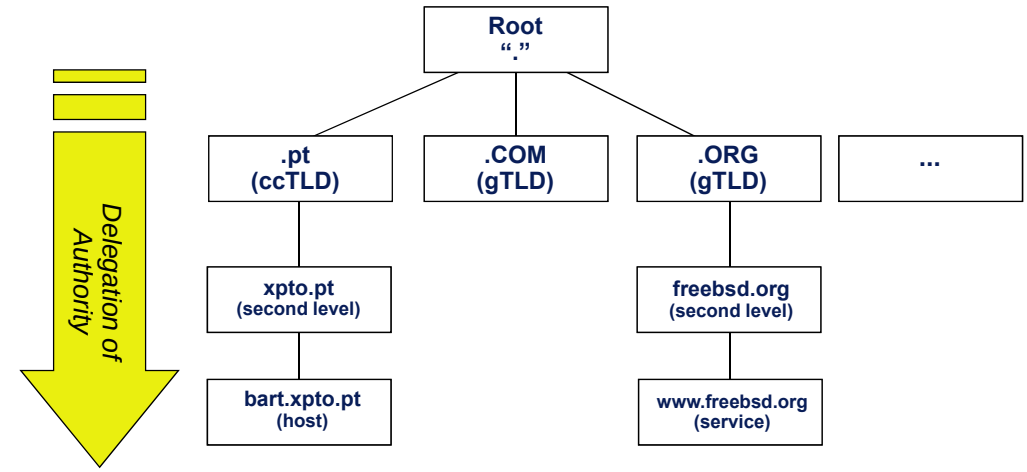
Delegation of Authority

- **Authoritative Name Servers**
  - **Primary/Master Servers**
  - **Secondary/Slave Servers**
- **Non-authoritative Name Servers**
- **DNS Resolver**

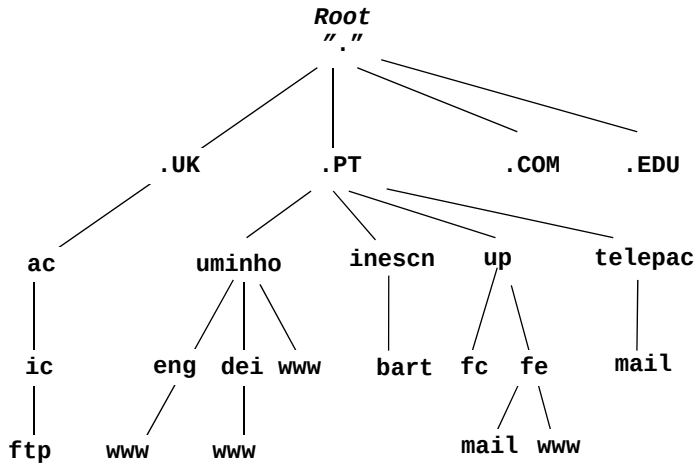
Master & Slaves

- The *master* is the source of map information for a zone.
- The *slave servers* will get updated copies of the *master* maps.
- When a DNS query is made there is no guarantee that the answer will come from the *master*.
- The *slaves servers* do not only work as backup in case of *master* failure! (*As with other directory services*...)
- The *master* and *slave servers* are authoritative for a zone.

DNS Structure



Tree



HOST | Service . [Subdomain.] Domain . TopLevelDomain.

FQDN – *Fully Qualified Domain Name*

Top Level Domains

Top Level Domains (TLDs)

- **ccTLDs** – *Country-code* TLDs
  (ISO country code - ISO 3166)
- **gTLDs** – *generic* TLDs
  - sTLDs – *sponsored* TLDs
  - uTLDs – *unsponsored* TLDs

TLDs

gTLDs

ARPAnet, **.ARPA**, *was divided in:*

- COM
- EDU
- GOV
- INT
- MIL
- NET
- ORG

ccTLDs

Portugal	**PT**
Germany	**DE**
Denmark	**DK**
Spain	**ES**
EUA	**US**
France	**FR**
Hungary	**HU**
United Kingdom	**UK**
Tuvalu	**TV**
Samoa	**WS**
Cocos Islands (Keeling)	**CC**
Vanuatu	**VU**
...	

Source:
`ftp://ftp.ripe.net/iso3166-countrycodes.txt`
`http://www.icann.org/tlds/`

Top Level Domains

Top Level Domains (TLDs)

- **ccTLDs** – *Country-code* TLDs
  (ISO country code - ISO 3166)
- **gTLDs** – *generic* TLDs
  - sTLDs – *sponsored* TLDs
  - uTLDs – *unsponsored* TLDs

sTLDs

gTLDs

ARPAnet, **.ARPA**, *was divided in:*

- COM
- EDU
- GOV
- INT
- MIL
- NET
- ORG

ccTLDs

Portugal	PT
Germany	DE
Denmark	DK
Spain	ES
EUA	US
France	FR
Hungary	HU
United Kingdom	UK
Tuvalu	TV
Samoa	WS
Cocos Islands (Keeling)	CC
Vanuatu	VU
...	

Source:
`ftp://ftp.ripe.net/iso3166-countrycodes.txt`
`http://www.icann.org/tlds/`

Top Level Domains

Top Level Domains (TLDs)

- **ccTLDs** – *Country-code* TLDs
  (ISO country code - ISO 3166)
- **gTLDs** – *generic* TLDs
  - sTLDs – *sponsored* TLDs
  - uTLDs – *unsponsored* TLDs

uTLDs

gTLDs

ARPAnet, **.ARPA**, *was divided in:*

- COM
- EDU
- GOV
- INT
- MIL
- NET
- ORG

ccTLDs

Portugal	PT
Germany	DE
Denmark	DK
Spain	ES
EUA	US
France	FR
Hungary	HU
United Kingdom	UK
Tuvalu	TV
Samoa	WS
Cocos Islands (Keeling)	CC
Vanuatu	VU
...	

Source:
`ftp://ftp.ripe.net/iso3166-countrycodes.txt`
`http://www.icann.org/tlds/`

uTLDs

gTLDs

ARPAnet, **.ARPA**, *was divided in:*

- COM
- EDU
- GOV
- INT
- MIL
- NET
- ORG

ccTLDs

Portugal	PT
Germany	DE
Denmark	DK
Spain	ES
EUA	US
France	FR
Hungary	HU
United Kingdom	UK
Tuvalu	**TV**
Samoa	**WS**
Cocos Islands (Keeling)	**CC**
Vanuatu	**VU**
...	

Source:
`ftp://ftp.ripe.net/iso3166-countrycodes.txt`
`http://www.icann.org/tlds/`

New TLDs

The *Internet Corporation for Assigned Names and Numbers* (ICANN) approved on 16 November 2000 seven new TLDs which have been operational since the end of 2001..

Domain	TLD	Organization
.aero – Aviation Industry	**sTLD**	Société Internationale de Télécommunications Aéronautiques (SITA)
.biz - Business	**uTLD**	NeuLevel, Inc.
.coop - cooperatives	**sTLD**	*Dot Cooperation LLC*
.info – informative	**uTLD**	Afilias Limited
.name - Personal websites and email addresses	**uTLD**	Global Name Registry
.museum - museums	**sTLD**	Museum Domain Management Association
.pro - professionals (example: lawyers, doctors, etc.)	**uTLD**	RegistryPro

New TLDs

- In 2003, ICANN approved the sTLDs: .asia, .cat, .jobs, .mobi, .tel and .travel).
- In 2011-03-18 the gTLD .xxx was approved.

Proposed TLD	Comments Email	Comments Archive	Web Address
.asia	stld-rfp-asia@icann.org	<http://forum.icann.org/lists/stld-rfp-asia/>	www.dotAsia.org
.cat	stld-rfp-cat@icann.org	<http://forum.icann.org/lists/stld-rfp-cat/>	www.puntcat.org
.jobs	stld-rfp-jobs@icann.org	<http://forum.icann.org/lists/stld-rfp-jobs/>	www.shrm.org
.mail	stld-rfp-mail@icann.org	<http://forum.icann.org/lists/stld-rfp-mail/>	www.spamhaus.org
.mobi	stld-rfp-mobi@icann.org	<http://forum.icann.org/lists/stld-rfp-mobi/>	www.mtldinfo.com
.post	stld-rfp-post@icann.org	<http://forum.icann.org/lists/stld-rfp-post/>	www.upu.int
.tel	stld-rfp-tel-telnic@icann.org	<http://forum.icann.org/lists/stld-rfp-tel-telnic/>	www.telname.com
.travel	stld-rfp-travel@icann.org	<http://forum.icann.org/lists/stld-rfp-travel/>	www.ttpc.org
.xxx	stld-rfp-xxx@icann.org	<http://forum.icann.org/lists/stld-rfp-xxx/>	www.iffor.org

http://www.iana.org/domains/root/db/

New TLDs

- In 2011-06-20 was approved the right of groups to create new TLD in any language or script.

iana
Internet Assigned Numbers Authority

http://www.iana.org/domains/root/db/

Root Zone Database

The Root Zone Database represents the delegation details of top-level domains, including gTLDs such as .com, and country-code TLDs such as .uk. As the manager of the DNS root zone, we are responsible for coordinating these delegations in accordance with our policies and procedures.

Much of this data is also available via the WHOIS protocol at whois.iana.org.

DOMAIN	TYPE	TLD MANAGER
.aaa	generic	American Automobile Association, Inc.
.aarp	generic	AARP
.abarth	generic	Fiat Chrysler Automobiles N.V.
.abb	generic	ABB Ltd
.abbott	generic	Abbott Laboratories, Inc.
.abbvie	generic	AbbVie Inc.
.abc	generic	Disney Enterprises, Inc.
.able	generic	Able Inc.
.abogado	generic	Top Level Domain Holdings Limited
.abudhabi	generic	Abu Dhabi Systems and Information Centre
.ac	country-code	Network Information Center (AC Domain Registry) c/o Cable and Wireless (Ascension Island)
.academy	generic	Half Oaks, LLC
.accenture	generic	Accenture plc
.accountant	generic	dot Accountant Limited
.accountants	generic	Knob Town, LLC
.aco	generic	ACO Severin Ahlmann GmbH & Co. KG
.active	generic	Active Network, LLC
.actor	generic	United TLD Holdco Ltd.

Registo em pt.

- Por delegação da IANA, a Fundação para a Computação Científica Nacional (FCCN) foi a entidade responsável pela gestão do domínio TLD ".pt"
- A Associação DNS.PT foi formalmente criada no dia 9 de maio de 2013 e sucedeu à FCCN na responsabilidade pela gestão, registo e manutenção de domínios ".pt"
- Domínios de topo:
  - .PT
  - .COM.PT
  - .EDU.PT
  - .GOV.PT
  - .INT.PT
  - .NET.PT
  - .NOME.PT
  - …
- **`http://www.dns.pt`**

.pt

Regulamento de Registo de Domínios .PT

O Registo de Nomes de Domínio sob .PT obedece às regras jurídicas, técnicas e administrativas constantes das "Regras de Registo de Nomes de Domínio de .pt" com o depósito legal nº376640/14 e cuja vigência iniciou a 16 de Junho de 2014.

Retroceder

- Preâmbulo
- Capítulo I **Condições para o registo de Domínios .PT**
- Capitulo II **Manutenção**
- Capitulo III **Alterações**
- Capitulo IV **Remoções**
- Capitulo V **Responsabilidade**
- Capitulo VI **Arbitragem**
- Capitulo VII **Disposições Finais e Transitórias**
- Anexo **Política WHOIS do Domínio de Topo .PT**

PREÂMBULO

A Associação DNS.PT é a entidade responsável pela gestão, registo e manutenção do administrativamente, à Fundação para a Computação Científica Nacional, FCCN, no final esta entidade que geriu o ccTLD .pt nos passados 25 anos. A Associação DNS.PT sucedeu, e obrigações até então por esta prosseguidos no âmbito da delegação efetuada pela IANA de Junho de 1988, (RFC 1032, 1033, 1034 e 1591) e, em particular, na responsabilidade pe sob o ccTLD (country code Top Level Domain) .pt, domínio de topo correspondente a Port inserta no Decreto-Lei 55/2013, de 17 de abril.

A Associação DNS.PT é uma associação privada sem fins lucrativos e tem como fundad Tecnologia, IP (FCT), Associação do Comércio Eletrónico e Publicidade Interativa (ACEP Consumidor (DECO) e o representante designado pela IANA – Internet Assigned Numbers A ccTLD.pt.

A Associação tem como escopo a gestão, operação e manutenção do registo do domi cumprindo para o efeito a lei, os princípios da transparência e publicidade, os respetiv nacionais e internacionais a nível técnico, administrativo e estratégico que lhe sejam apli Associação estão cometidas outras competências de cariz mais operacional onde se de espaço de endereços Internet sob .pt com elevados padrões de eficácia, transparência e pu política de resolução extrajudicial de conflitos com recurso ao ARBITRARE - Centro de Arbi de Domínio e Firmas e Denominações, como Centro especializado com competência para a de domínio, (www.arbitrare.pt); a atuação de acordo com as boas práticas internacionais a do serviço DNS; e a manutenção da certificação pela norma ISO9001.

Fonte:
`https://www.dns.pt/pt/dominios-2/regras-de-dominios/preambulo/`

Marcas e Nomes em pt.

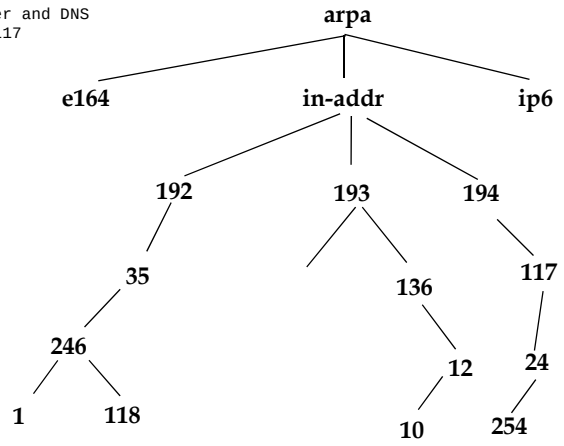
Instituto Nacional da Propriedade Industrial
(Ministério da Justiça)

- Em Portugal, só o INPI é que pode atribuir direitos de exclusividade sobre marcas e outros sinais utilizados no comércio.
- Disponibiliza uma ferramenta que agrega, num interface comum, as Bases de Dados do INPI e as Bases de Dados de Nomes de Domínio ".PT", permitindo a consulta da existência de determinada marca/domínio em simultâneo

https://justica.gov.pt/registos/propriedade-industrial/marca

Reverse Mapping Tree

RFC 2916 - E.164 number and DNS
Obsoleted by: 6116, 6117



RFC3172, BCP0052
Management Guidelines & Operational Requirements for the Address and Routing Parameter Area Domain ("arpa")

Domain Name System

- DNS is a service that works according to the hierarchical client-server flow model.
- The *nameserver* is a program that accesses the hosts database and answers the questions of the other programs.
- The *resolver* is a set of routines that are “called” by user programs; generates questions to the server, processes the server's responses, and returns the requested information.
- Port 53 is reserved for DNS, with UDP and TCP transport.

Resolver Routines...

```
RESOLVER(3)              OpenBSD Programmer's Manual              RESOLVER(3)

NAME
     res_query, res_search, res_mkquery, res_send, res_init, dn_comp,
     dn_expand - resolver routines


SYNOPSIS
     #include <sys/types.h>
     #include <netinet/in.h>
     #include <arpa/nameser.h>
     #include <resolv.h>

     int
     res_query(char *dname, int class, int type, u_char *answer, int anslen);

     int
     res_search(char *dname, int class, int type, u_char *answer, int anslen);

     dn_comp(char *exp_dn, char *comp_dn, int length, char **dnptrs,
             char **lastdnptr);

     int
     dn_expand(u_char *msg, u_char *eomorig, u_char *comp_dn, u_char *exp_dn,
             int length);

DESCRIPTION
     These routines are used for making, sending, and interpreting query and
     reply messages with Internet domain name servers.

     Global configuration and state information that is used by the resolver
     routines is kept in the structure  res. Most of the values have reason-
```

[...]

/etc/resolv.conf

```
domain        xpt.pt
nameserver    194.115.29.9
nameserver    194.37.24.1
nameserver    192.39.26.1
```

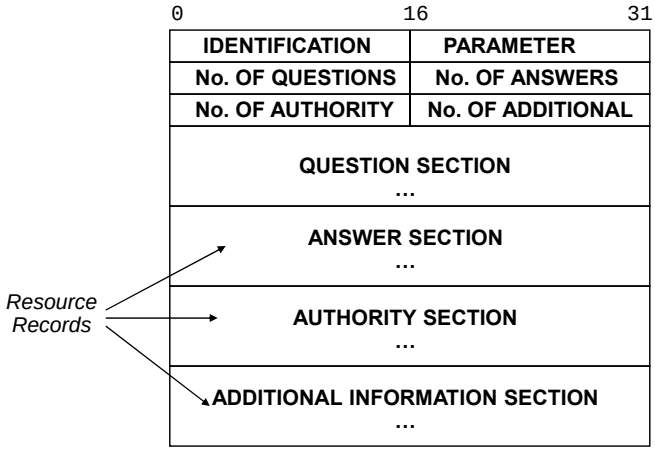
Other configuration options

search To search in a list of domains instead of just one

sortlist It allows to sort the addresses returned by the routine gethostbyname

options Possible: debug, ndots:n

DNS Message format



bit of PARAMETER field

0 Operation:
- 0 Query
- 1 Answer

1-4 Query Type:
- 0 Standard
- 1 Inverse
- 2 Completion 1 (Obsol.)
- 3 Completion 2 (Obsol.)

5 Set if answer authoritative

6 Set if message truncated

7 Set if recursion desired

8 Set if recursion available

9-11 Reserved

12-15 Response Code:
- 0 No error
- 1 Format error in query
- 2 Server failure
- 3 Name does not exist
- ....

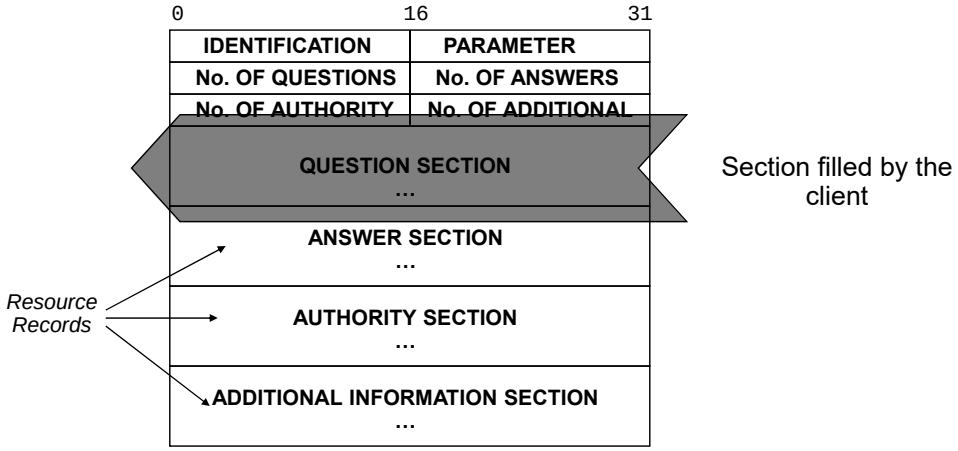
DNS Common Response Codes

Bits 12-15 of PARAMETER field

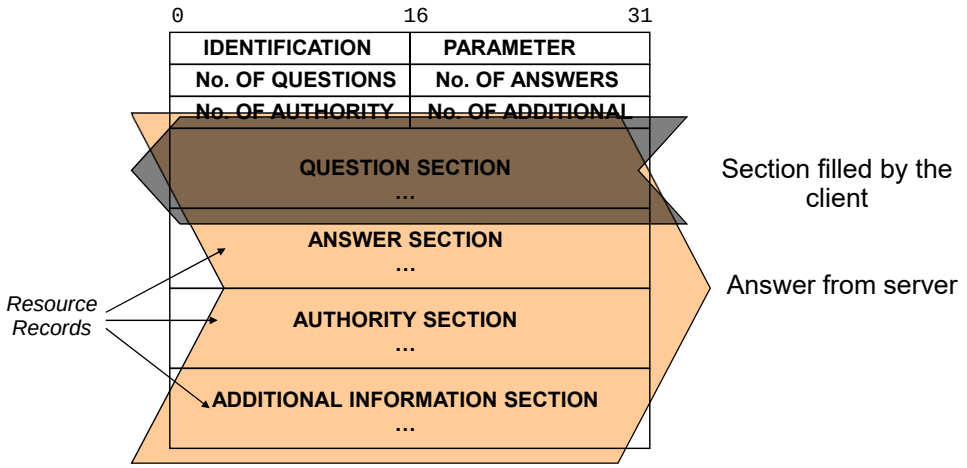
- `NoError:` *"All is fine"* (`RCODE:0`)
- `FormErr:` *"You sent me garbage"*
- `ServFail:` *"I made a mistake" or "I could not validate DNSSEC"*
- `NXDomain:` *"The queried name does not exist"*
- `NotImp:` *"I do not know about that OPCODE"*
- `Refused:` *"I won't do what you tell me"*
- … `RCODE:11`

`http://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-6`

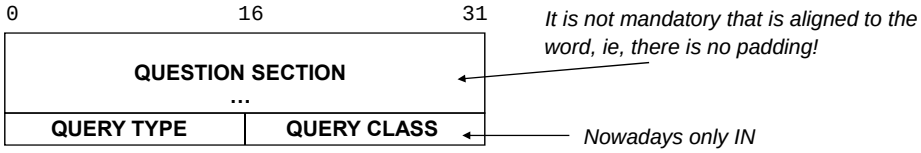
DNS Message format



DNS Message format

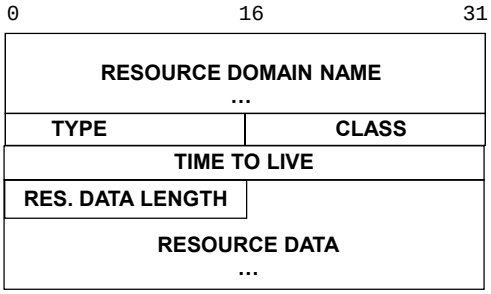


DNS Message format

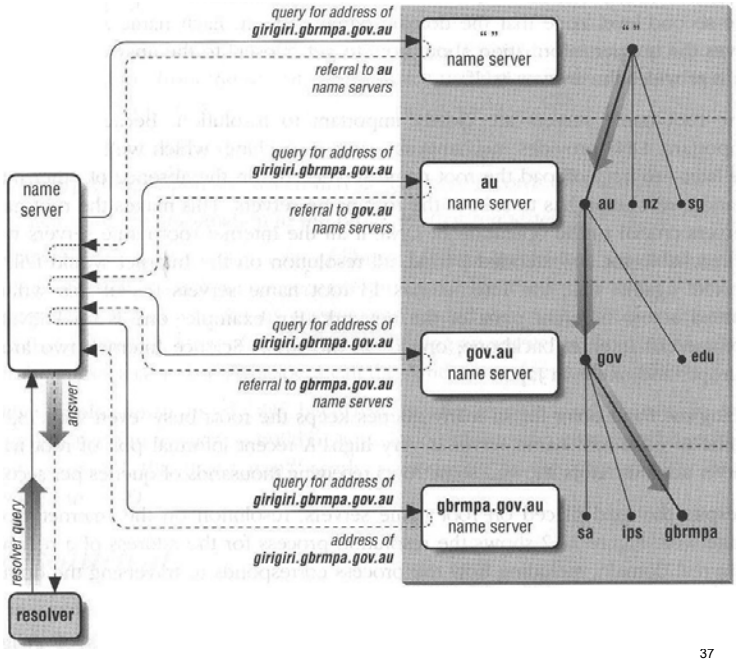


Resource Records:

- ANSWER SECTION
- AUTHORITY SECTION
- ADDITIONAL INFORMATIONSECTION



Names Resolution



dig

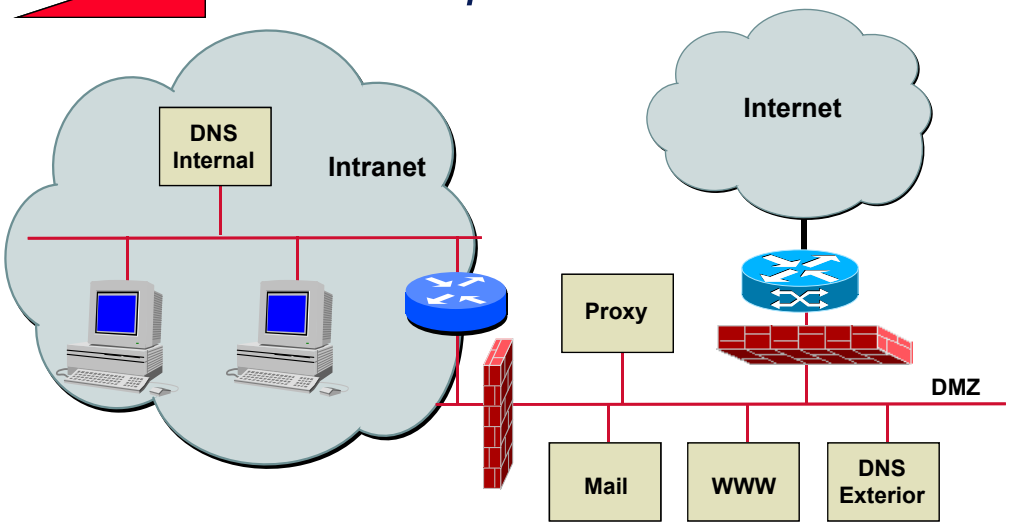
```
jneves@homer(6)$ dig +trace uga-buga.xpto.net
; <<>> DiG 9.2.1 <<>> +trace uga-buga.xpto.net
;; global options:  printcmd
.                       148339  IN      NS      L.ROOT-SERVERS.NET.
[...]
.                       148339  IN      NS      J.ROOT-SERVERS.NET.
.                       148339  IN      NS      K.ROOT-SERVERS.NET.
;; Received 260 bytes from 194.117.24.1#53(194.117.24.1) in 25 ms

net.                    172800  IN      NS      A.GTLD-SERVERS.net.
[...]
net.                    172800  IN      NS      K.GTLD-SERVERS.net.
net.                    172800  IN      NS      E.GTLD-SERVERS.net.
net.                    172800  IN      NS      M.GTLD-SERVERS.net.
;; Received 464 bytes from 198.32.64.12#53(L.ROOT-SERVERS.NET) in 223 ms

xpto.net.               172800  IN      NS      ns.webtt.biz.
xpto.net.               172800  IN      NS      ns2.webtt.biz.
;; Received 79 bytes from 192.5.6.30#53(A.GTLD-SERVERS.net) in 171 ms

uga-buga.xpto.net.      86400   IN      A       64.239.29.225
xpto.net.               259200  IN      NS      ns.xpto.net.
xpto.net.               259200  IN      NS      ns2.xpto.net.
;; Received 118 bytes from 64.239.29.225#53(ns.webtt.biz) in 135 ms
```

Split DNS



Maps Propagation

Mechanisms for detecting the change of zone maps:

- ***Polling -*** periodically the secondary consult the S0A record and if it has been changed, initiate the transfer of the zone.
- ***Notification*** - whenever the S0A record is changed, the primary notifies the secondary (not all servers support ...). Notify [RFC1996]

Transfer of zone maps:

- ***Total*** - the secondary asks the primary to download the map (includes all records in the zone).
- ***Incremental*** - the secondary asks the primary to transfer the records that have been modified (not supported by all servers).Incremental transfer (IXFR) [RFC1995]

Server Configuration

- **`named.conf`**
  - **Declaration of domains:**
    - » **Primary Server | *Master***
    - » **Secondary Server | *Slave***
- Root (“.”) Cache – when you *boot* the server it knows nothing, just where is the *root*
- Maps of zones – multiple records
- Access control information, zone transfer authorization (AXFR), file / directory identification

named.conf

```
options {
        //bind data file to boot a name server.
        //
        directory       "/var/named";
        pid-file        "/var/run/named.pid";
        //
        //who is authorized to axfr
        allow-transfer   {
                192.35.246.1;  194.117.24.1; 194.117.30.3; 192.35.246.9;
                146.193.0.1; 193.136.62.3; 193.136.0.1;193.136.0.3;
         };
};
zone “xpto.pt" in {
        type master;
        file "prime/xpto.pt";
};
zone “x-lda.pt" in {
        type slave;
        file "sec/x-lda.pt";
        masters { 194.79.69.129; };
};
```

named.root / root.cache / named-cache

```
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.cache
;           on server           FTP.INTERNIC.NET
;       -OR-                    RS.INTERNIC.NET
;
;       last update:     March 13, 2019
;       related version of root zone:     2019031302
;
; FORMERLY NS.INTERNIC.NET
;
.                        3600000      NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.      3600000      AAAA  2001:503:ba3e::2:30
;
```


https://www.internic.net/domain/named.root

named.root / root.cache / named-cache

```
; FORMERLY NS.INTERNIC.NET
.                        3600000      NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.      3600000      AAAA  2001:503:ba3e::2:30
;
[…]
; FORMERLY NIC.NORDU.NET
;
.                        3600000      NS    I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.      3600000      A     192.36.148.17
I.ROOT-SERVERS.NET.      3600000      AAAA  2001:7fe::53
;
[…]
; housed in Japan, operated by WIDE
;
.                        3600000      NS    M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.      3600000      A     202.12.27.33
M.ROOT-SERVERS.NET.      3600000      AAAA  2001:DC3::35
; End of File
```

Map of Zone – Resource Records

- SOA
- NS
- A
- PTR
- CNAME
- HINFO
- TXT
- MX
- MB
- MG
- MINFO
- MR
- WKS
- AFSDB
- ISDN
- RP
- .....

SOA and NS records

```
;
@       IN      SOA     ns.inescn.pt. joao\.neves.inescn.pt. (
                        2020031817    ; Serial
                        28800         ; Refresh - 8 hours
                        7200          ; Retry - 2 hours
                        604800        ; Expire - 7 days
                        86400 )       ; Minimum TTL - 24 hours
        IN      NS      ns.inescn.pt.
        IN      NS      ns2.inescn.pt.
        IN      NS      ns3.inescn.pt.
        IN      NS      inesc.inesc.pt.
        IN      NS      ciup1.ncc.up.pt.
;
        IN      A               192.35.246.9
[...]
```

SOA and NS records

```
;
@       IN      SOA     ns.inescn.pt. joao\.neves.inescn.pt. (
                        2020031817    ; Serial
                        28800         ; Refresh - 8 hours
                        7200          ; Retry - 2 hours
                        604800        ; Expire - 7 days
                        86400 )       ; Minimum TTL - 24 hours
        IN      NS      ns.inescn.pt.
        IN      NS      ns2.inescn.pt.
        IN      NS      ns3.inescn.pt.
        IN      NS      inesc.inesc.pt.
        IN      NS      ciup1.ncc.up.pt.
;
        IN      A               192.35.246
[...]
```

- **Declaration of Master;**
- **Declaration of a domain authority;**
- **There can only be one per domain;**
- **Control of queries and cache of other servers.**

SOA and NS records

```
;
@       IN      SOA     ns.inescn.pt. joao\.neves.inescn.pt. (
                        2020031817    ; Serial
                        28800         ; Refresh - 8 hours
                        7200          ; Retry - 2 hours
                        604800        ; Expire - 7 days
                        86400 )       ; Minimum TTL - 24 hours
        IN      NS      ns.inescn.pt.
        IN      NS      ns2.inescn.pt.
        IN      NS      ns3.inescn.pt.
        IN      NS      inesc.inesc.pt.
        IN      NS      ciup1.ncc.up.pt.
;
        IN      A               192.35.246.9
[...]
```

RFC1912

SOA and NS records

```
;
@       IN      SOA     ns.inescn.pt. joao\.neves.inescn.pt. (
                        2020031817    ; Serial
                        28800         ; Refresh - 8 hours
                        7200          ; Retry - 2 hours
                        604800        ; Expire - 7 days
                        86400 )       ; Minimum TTL - 24 hours
                        ns.inescn.pt.
                        ns2.inescn.pt.
                NS      ns3.inescn.pt.
        IN      NS      inesc.inesc.pt.
        IN      NS      ciup1.ncc.up.pt.
;
        IN      A               192.35.246.9
[...]
```

Attention to the implications of the size of the maps of zones and the frequency of updates...

MX, A, CNAME records

```
@       IN      SOA     ns.inescn.pt. jneves.inescn.pt. (
                        2019051714    ; Serial
                        28800         ; Refresh - 8 hours
                        7200          ; Retry - 2 hours
                        604800        ; Expire - 7 days
                        86400 )       ; Minimum TTL - 24 hours
        IN      NS      ns.inescn.pt.
[...]
        IN      MX      10      animal.inescn.pt.
        IN      MX      20      correio.inescn.pt.
        IN      MX      100     mail2.ip.pt.
;
animal  IN      A               192.35.246.1
ns      IN      A               192.35.246.1
        IN      MX      20      animal.inescn.pt.
        IN      MX      10      correio.inescn.pt.
        IN      MX      100     mail2.ip.pt.
ntp0    IN      CNAME           animal.inescn.pt.
proxy   IN      A               192.35.246.1
proxy   IN      A               192.35.246.5
```

MX, A, CNAME records

```
@       IN      SOA     ns.inescn.pt. jneves.inescn.pt. (
                        2019051714    ; Serial
                        28800         ; Refresh - 8 hours
                        7200          ; Retry - 2 hours
                        604800        ; Expire - 7 days
                        86400 )       ; Minimum TTL - 24 hours
        IN      NS      ns.inescn.pt.
[...]
        IN      MX      10      animal.inescn.pt.
        IN      MX      20      correio.inescn.pt.
        IN      MX      100     mail2.ip.pt.
;
animal  IN      A               192.35.246.1
ns      IN      A               192.35.246.1
        IN      MX      20      animal.inescn.pt.
        IN      MX      10      correio.inescn.pt.
        IN      MX      100     mail2.ip.pt.
ntp0    IN      CNAME           animal.inescn.pt.
proxy   IN      A               192.35.246.1
proxy   IN      A               192.35.246.5
```


MX, A, CNAME records

```
@       IN      SOA     ns.inescn.pt. jneves.inescn.pt. (
                        2019051714    ; Serial
                        28800         ; Refresh - 8 hours
                        7200          ; Retry - 2 hours
                        604800        ; Expire - 7 days
                        86400 )       ; Minimum TTL - 24 hours
        IN      NS      ns.inescn.pt.
[...]
        IN      MX      10      animal.inescn.pt.
        IN      MX      20      correio.inescn.pt.
        IN      MX      100     mail2.ip.pt.
;
animal  IN      A               192.35.246.1
ns      IN      A               192.35.246.1
        IN      MX      20      animal.inescn.pt.
        IN      MX      10      correio.inescn.pt.
        IN      MX      100     mail2.ip.pt.
ntp0    IN      CNAME           animal.inescn.pt.
proxy   IN      A               192.35.246.1
proxy   IN      A               192.35.246.5
```

PTR record

```
; Description:  Reverse mapping for 246.35.192.in-addr.arpa.
;
@       IN      SOA     ns.inescn.pt. joao\.neves.inescn.pt. (
                        2019051713        ; Serial
                        28800           ; Refresh - 8 hours
                        7200            ; Retry - 2 hours
                        604800          ; Expire - 7 days
                        86400 )         ; Minimum TTL - 24 hours
        IN      NS      ns.inescn.pt.
        IN      NS      ns2.inescn.pt.
        IN      NS      ns3.inescn.pt.
        IN      NS      inesc.inesc.pt.
        IN      NS      ciup1.ncc.up.pt.
;
0.246.35.192.in-addr.arpa.      IN      PTR     inescn.pt.
1.246.35.192.in-addr.arpa.      IN      PTR     animal.inescn.pt.
5.246.35.192.in-addr.arpa.      IN      PTR     lula.inescn.pt.
9.246.35.192.in-addr.arpa.      IN      PTR     bart.inescn.pt.
```

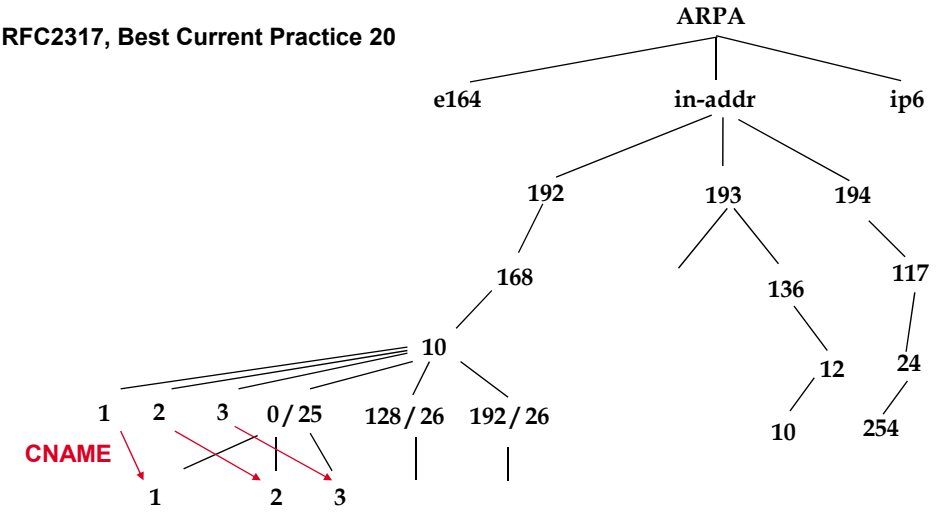

Classless Problem…

```
;    Reverse mapping for:
;                  192.168.10/25         Company A
;                  192.168.10.128/26     Company B
;                  192.168.10.192/26     Company C
;

$ORIGIN 10.168.192.in-addr.arpa.
;
1      IN      PTR     host1.A.dominio.
2      IN      PTR     host2.A.dominio.
3      IN      PTR     host3.A.dominio.
;
129    IN      PTR     host1.B.dominio.
130    IN      PTR     host2.B.dominio.
131    IN      PTR     host3.B.dominio.
;
193    IN      PTR     host1.C.dominio.
194    IN      PTR     host2.C.dominio.
195    IN      PTR     host3.C.dominio.
```

Classless IN-ADDR.ARPA delegation

RFC2317, Best Current Practice 20



Classless Problem…

```
$ORIGIN 10.168.192.in-addr.arpa.
@       IN      SOA     ns.my.domain.  Hostmaster.my.domain. (...)
;...
; [0 – 127] / 25
0/25            NS      ns.A.dominio.
0/25            NS      ns2.A.dominio.
;
1               CNAME   1.0/25.10.168.192.in-addr.arpa.
2               CNAME   2.0/25.10.168.192.in-addr.arpa.
3               CNAME   3.0/25.10.168.192.in-addr.arpa.
; [128 - 191] / 26
128/26          NS      ns.B.dominio.
128/26          NS      ns2.B.dominio.
;
129             CNAME   129.128/26.10.168.192.in-addr.arpa.
130             CNAME   130.128/26.10.168.192.in-addr.arpa.
131             CNAME   131.128/26.10.168.192.in-addr.arpa.
;....
```

Classless Problem…

```
$ORIGIN 0/25.10.168.192.in-addr.arpa.
@       IN      SOA     ns.A.dominio.  Hostmaster.A.dominio. (...)
                NS      ns.A.dominio.
                NS      ns2.A.dominio.
;
1               PTR     host1.A.dominio.
2               PTR     host2.A.dominio.
3               PTR     host3.A.dominio.

$ORIGIN 128/26.10.168.192.in-addr.arpa.
@       IN      SOA     ns.B.dominio.  Hostmaster.B.dominio. (...)
                NS      ns.B.dominio.
                NS      ns2.B.dominio.
;
129             PTR     host1.B.dominio.
130             PTR     host2.B.dominio.
131             PTR     host3.B.dominio.
```


The CHAOSNET Class.....

```
root@hostA# dig txt chaos version.bind.

; <<>> DiG 9.2.1rc2 <<>> any chaos version.bind.
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14739
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; ANSWER SECTION:
version.bind.           0       CH      TXT     "9.2.1rc2"

;; Query time: 2 msec

[...]

root@hostB# dig txt chaos version.bind.

;;...
;; ANSWER SECTION:
version.bind.           0       CH      TXT     "Compadri, na sei!..."

;; Query time: 2 msec
;; SERVER: 192.35.246.1#53(192.35.246.1)
;; WHEN: Wed Oct 29 15:49:03 2003
;; MSG SIZE  rcvd: 63
```

DNSSEC

- Domain Name System Security Extensions (DNSSEC)
- Recently vulnerabilities in the DNS were discovered that allow an attacker to hijack this process of looking some one up or looking a site up on the Internet using their name;
- DNSSEC is the act of adding special signatures to the root, TLD, and authoritative *nameservers* for a zone to establish a chain of trust;
- DNSSEC enabled zones ensure that the answer to a DNS query has not been tampered with.

DNSSEC

To facilitate signature validation, DNSSEC adds new DNS records:

- **RRSIG** - Contains a cryptographic signature, zone-signing key
- **DNSKEY** - Contains a public signing key
- **DS** - Delegation signer record; contains the hash of a DNSKEY record
- **NSEC** and **NSEC3** - For explicit denial-of-existence of a DNS record
- **CDNSKEY** and **CDS** - For a child zone requesting updates to DS record(s) in the parent zone.

EDNS

- EDNS standard (RFC 2671, 1999; updated by RFC 6891, 2013)
  - “Extension Mechanisms for DNS (EDNS(0))”
- DNS software vendors added various workarounds for broken servers
- Broken servers:
  - Does not respond at all
  - Respond with non-FORMERR error code
- DNS Servers cope with that by asking without EDNS

EDNS

- DNS query timeouts
  - query with EDNS → timeout
  - an EDNS problem or packet loss?
  - retries, latency for users
- Known offenders
  - Obsolete DNS software
  - too strict firewall

EDNS

- 2019 (E)DNS flag day
  - https://dnsflagday.net
  - February 2019
  - DNS servers which do not respond at all to EDNS queries will be treated as dead

DNS Management

RFC1912: Common DNS Operational and Configuration Errors

Som

- Ev me
- Ea *ers*
- Pu
- Av , www, ntp, po
- Att]”
- Th YMMDDnn
- Th e accepted for ma

DNS Management

RFC1912: Common DNS Operational and Configuration Errors

Some Recommendations:

- Every Internet-reachable host should have a name
- Each domain must have at least two *nameservers*
- Put *secondary servers* on external networks
- Avoid CNAME's, use them only for services (ftp, www, ntp, pop, etc ...) and never declare a CNAME as NS
- Attention to special characters "`( )<>@,;:\".[]`"
- The recommended syntax for the *Serial* is YYYYMMDDnn
- The wildcard "*" in an MX RR causes email to be accepted for machines that do not exist ….

Typical Maintenance problems

- Typing errors
  (pressed the next key…)
- Inserting comments using the character "#"
  (so which is it??? It's the ";")
- Incorrect update of *Serial* counter
  (the new value is less than or equal to the previous one)
- Incoherent information on zone maps and "reverse", make sure your PTR and A records match
  (update only one of the maps; the IP address is not coincident on both maps)
- Forgetting the "point" at the end
  (ceases to be a FQDN; external NS inaccessible; unknown MX; names with double referenced domain)

Next Steps...

Internationalized Domain Names (IDN)

- Arabic (Arabic) يونيكود
- Arabic (Persian) یونی‌کُد
- Armenian Յունիկոդ
- Bengali য়ুনিকোড
- Cyrillic (Russian) Юникод
- Devanagari (Hindi) यूनिकोड
- Georgian უნიკოდი
- Greek Γιούνικοντ
- Gujarati યૂનિકોડ
- Gurmukhi ਯੂਨਿਕੋਡ
- Han (Chinese) 统一码 統一碼 万国码 萬國碼
- Hangul 유니코드
- Hebrew יוניקוד
- Hiragana ゆにこおど
- Khmer អ្នធីគោដ
- Malayalam യൂനികോഡ്
- Syriac ܝܘܢܝܩܘܕ
- Tamil யூனிகோட்
- Thai ยูนีโคด

What are IDN?

An Internationalized Domain Name (IDN) uses a particular encoding and format to allow a wider range of scripts to represent domain names. Until late 2009**, **Top-Level Domains** were restricted to only the Latin letters a to z without accents or symbols. After 2009, IDN TLDs were introduced in other scripts including Arabic, Chinese and Cyrillic scripts.

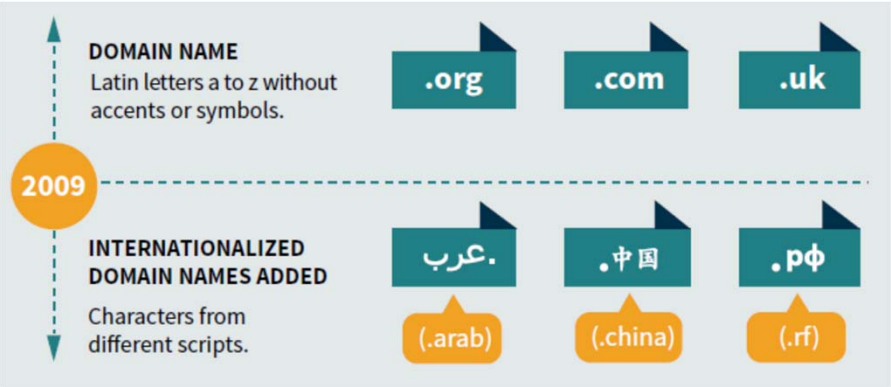
IDN TLDs can be either ccTLDs or gTLDs.

Internationalized Domain Names

Domain names with non-Latin characters or Latin characters beyond letters (a to z) digits (0 to 9) and hyphen (-), as allowed by relevant protocols.

Source:
https://www.icann.org/sites/default/files/assets/idn-access-domain-names-03sep15-en.pdf

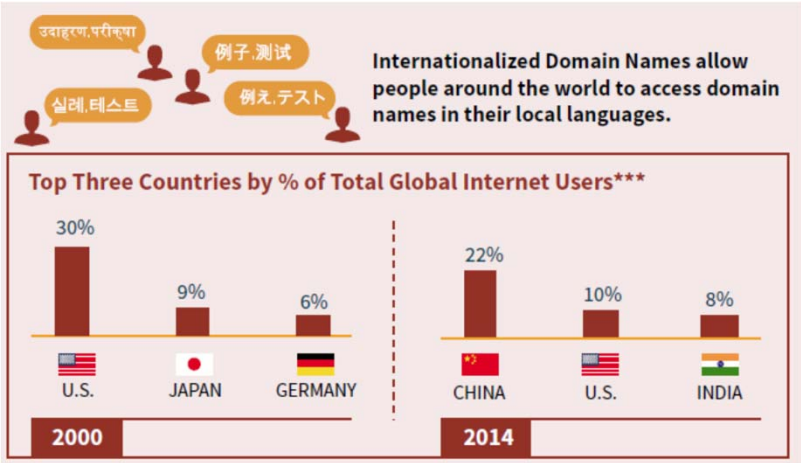
What has changed with TLD?



.рф is the Cyrillic ccTLD for the Russian Federation

Source:
`https://www.icann.org/sites/default/files/assets/idn-access-domain-names-03sep15-en.pdf`

Why IDN?



Source:
`https://www.icann.org/sites/default/files/assets/idn-access-domain-names-03sep15-en.pdf`

IDN

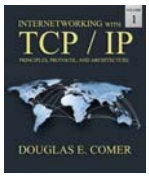
Internationalized Domain Names (IDN)

- RFC´s 3490, 3491, 3492 (*Proposed Standard*)
- Guidelines for the Implementation of Internationalized Domain Names
  `http://www.icann.org/general/idn-guidelines-20jun03.htm`
- **`http://www.icann.org/topics/idn.html`**

DNS Server Software

- Internet Systems Consortium (BIND)
- CZ.NIC (Knot Resolver)
- NLNetLabs (Unbound)
- PowerDNS (PowerDNS Recursor)

DNS: further reading



Comer, Douglas E.
Internetworking with TCP/IP (VOL I)
Pearson, 6th Edition (2014)
ISBN-10: 0-13-608530-X
ISBN-13: 978-0-13-608530-0

Albitz, Paul & Liu, Cricket, "*DNS and BIND"***,**
4th ed., O´Reilly & Associates, Inc., 2001
ISBN 0-596-00158-4

- **Mockapetris, P.,** *Domain Names Concepts and Facilities,* STD 13, RFC1034, USC/Information Sciences Institute, November 1987.
- **Mockapetris, P.,** *Domain Names Implementation and Specification*, STD 13, RFC1035, USC/Information Sciences Institute, November 1987.
- **Barr, D.,** *Common DNS Operational and Configuration Errors*, RFC1912, February 1996.