
Network
Information
Center
México

# Evolution of DNS services in .MX

# Index

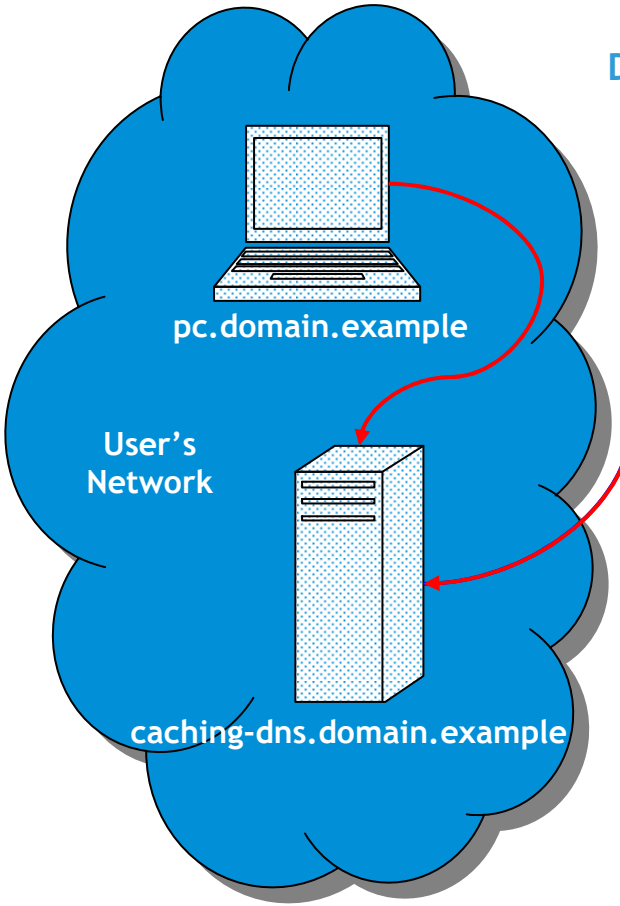
1. In the beginning …
2. Shared Unicast phase 1 and TSIG
3. Dynamic updates and IXFR
4. Shared Unicast phase 2
   a) All four NS RR's in Shared Unicast
   b) Blocking and unblocking of attackers
   c) Diversity
   d) Traffic Engineering
5. What's next …

# In the beginning …

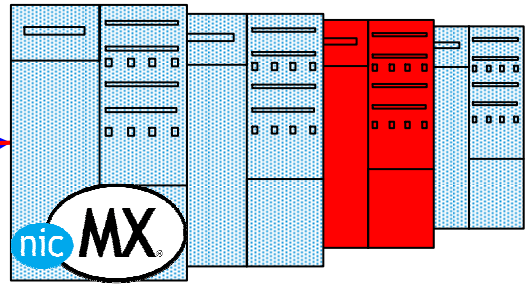
- Sponsored secondaries with other organizations
- Shared Unicast phase 1 (only on one NS RR), all DNS servers operated by NIC Mexico
- TSIG enabled servers
- Dynamic updates and IXFR
- Shared Unicast phase 2 (all four NS RR)

# Shared Unicast phase 1

# The DNS is not redundant by itself



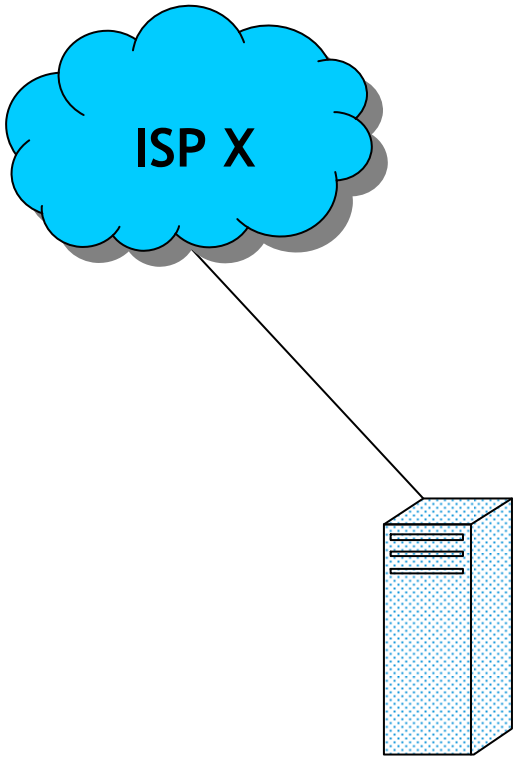

DNS servers for .MX before July 2003




**1/N %** approximately the level of impact on the TLD for every DNS server that stops answering queries

**25%** in the case of .MX before July 2003

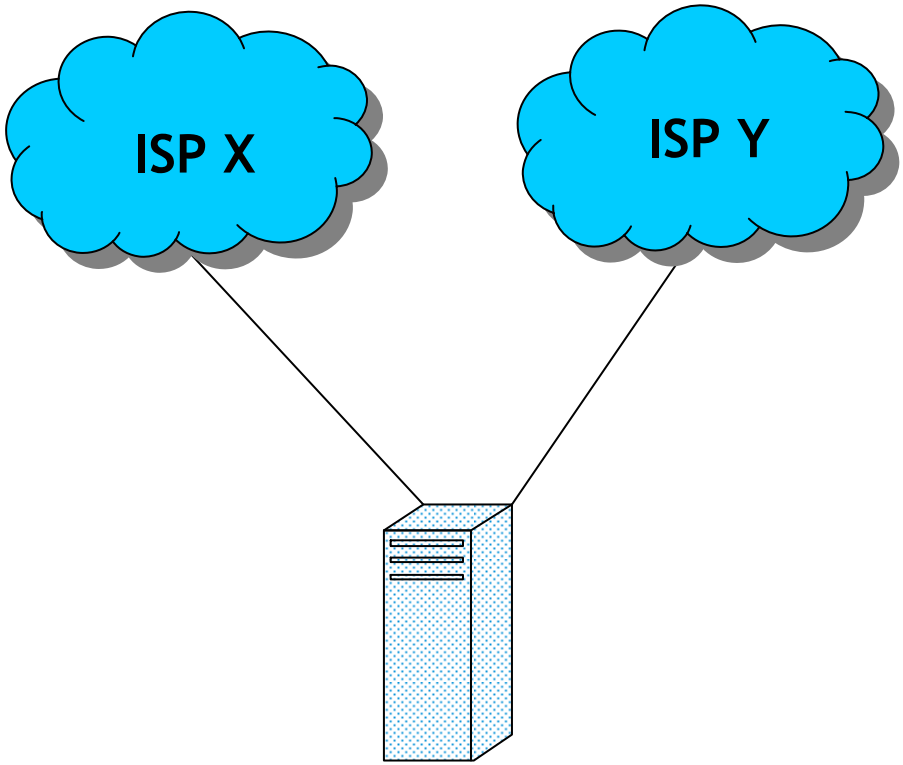
# Single-homed server




**dns.domain.example**

**192.0.2.1**

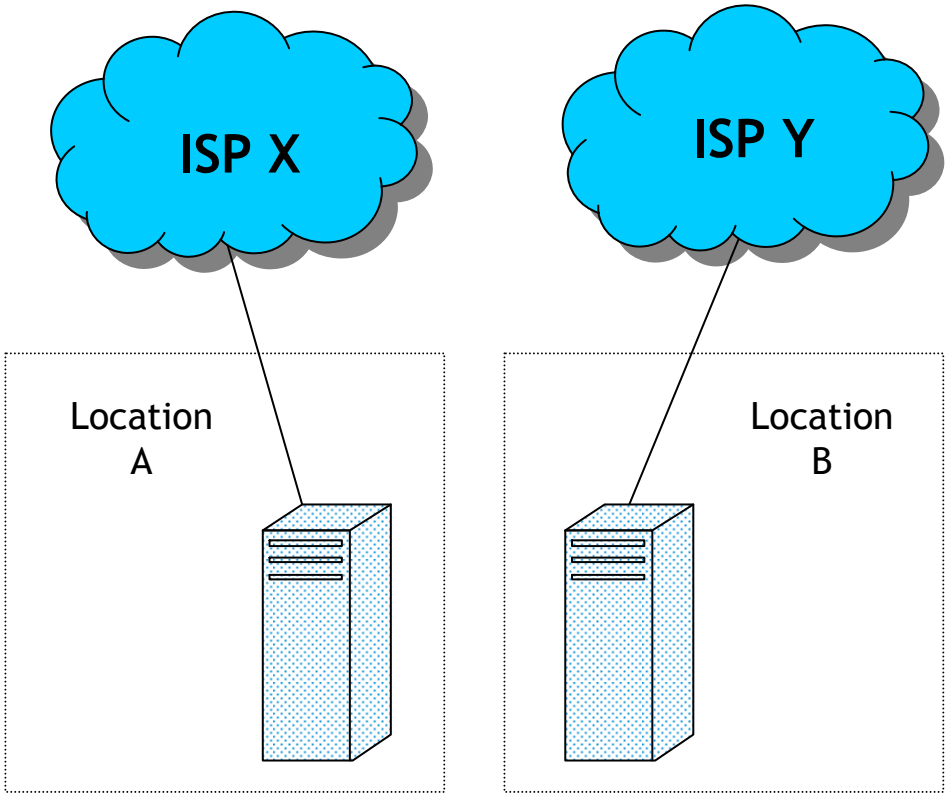
# Multihomed server




**dns.domain.example**

**192.0.2.1**

# Server with Shared Unicast IP




**dns.domain.example**

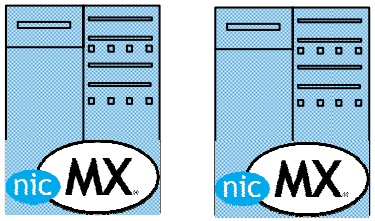
**192.0.2.1**

# Shared Unicast phase 1

DNS servers for .MX, SLD's and IR for the NIR at July 2003

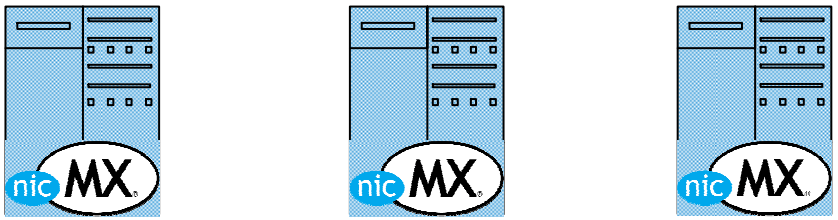
- Local mirror in one entity, Shared Unicast in the other, with 3 physical global nodes
- Implemented TSIG

**ns.nic.mx**



Monterrey, MX
Triara

**yacateuctli.nic.mx**



Monterrey, MX
Avantel

México City, MX
Alestra

San Jose, US
Verio


# Dynamic Updates

# Dynamic Updates

- Implemented, since January 2004
- Every update, deletion or creation goes immediately to the DNS stealth master
- By IXFR the changes go to the secondaries
- The user does not have to wait more than a few seconds, normally, to see her/his domain online

# Shared Unicast phase 2

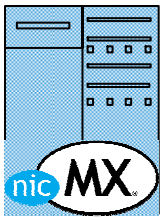
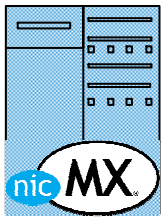
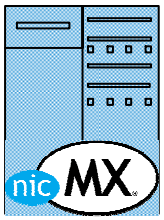
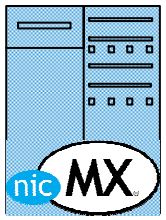
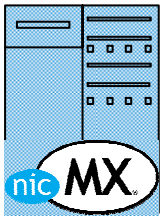
# Shared Unicast phase 2

DNS servers for .MX, SLD's and IR for the NIR at July 2005

Shared Unicast in all the servers with 4 entities (BTW, we changed the hostnames for several reasons):

**a.ns.mx**
**b.ns.mx**
**c.ns.mx**
**d.ns.mx**

On 5 physical global nodes:

**Monterrey, MX**
**Triara**

**Monterrey, MX**
**Avantel**

**México City, MX**
**Alestra**

**San Jose, US**
**Verio**

**San Francisco, US**
**ISC**

# Blocking and unblocking of attackers

- Monitoring the number of queries based on source IP
- Automatic blocking on firewall on DNS server
- Exponentially growing time of blocking on attackers: 5, 10, 20, 40, 60 minutes
- A memory of 3 hours of misbehavior

# Diversity on:

- **Operating Systems**: FreeBSD 4, Linux 2.6, OpenBSD 3.7, Solaris 9
- **Hardware architectures**: AMD64, Intel x86, Sparc
- **DNS implementations**: BIND 8.4, BIND 9.2, ANS 2.3
- **Firewalls**: IPFW2, IPF, PF, IPtables
- **BGP implementations**: Quagga, OpenBGP, Cisco IOS
- **Carriers** covering ~90% of Mexico's Internet: Alestra, Avantel and Telmex plus Verio and ISC

# Traffic engineering

- Different physical nodes are "seen" from one point on the Internet
- We turned off some entities on some nodes; but every entity is on, in at least, 3 nodes; also taking care of the diversity
- In case of problems on a node, the off entities can be manually turned on for taking over the load

# Other features

- Full control of DNS system
- 7x24 contract for all the IDC's, except one
- Easy to include one more server to the pool, there is no need to request IANA updates, anymore (unless we decide to include another entity)
- Redundant remote access on all servers: SSH, KVM over Internet or analog PSTN modem
- Memory file system for zone storage

# What's next …

# What's next …

- IPv6 support on the Registry applications
- Detailed statistics on DNS queries
- Secondary for other ccTLD's in Shared Unicast
- IPv6 transport … soon
- DNSsec … later
- IRIS … later
- ENUM … maybe
- IDN's … not for some time

# Statistics on DNS queries

- More than 150 millions of DNS queries per day.
- Have or will have reports on number of queries:
  - Type of queries (A, NS, PTR, etc.)
  - Per source (ISP, country/zone)
  - Existent domains
  - Non existent domains

# Thank you

**Francisco Arias**

**farias@nic.mx**