DNS architectures
Agenda

- Introduction
- DNS Architecture Master-Slave
- DNS Architecture Multi-Masters
- DNS Architecture Stealth
- State-of-the-art Stealth DNS SMART Architecture
Why different DNS architectures?

- Originally, DNS protocol was based on a Master-Slave architecture
- Network infrastructures are more and more complex
- There is an increase need of protection mechanisms against external attacks
- In some cases, the standard architecture is not enough
DNS Master-Slave architecture
Master-Slave Principles

- The DNS Master-Slave architecture relies on the DNS transaction type called zone transfer Full (AXFR RFC 1035) or incremental (IXFR RFC 1995)

- One server is authoritative for a zone. It is the value defined in the SOA RR MNAME field

- All zones list the name servers that are members of the architecture as NS

- The DNS master is authorized to notify slave zones and answer to AXFR or IXFR DNS transactions
Master-Slave Principles

Zone mycompany.com
SOA masterdns
NS masterdns
NS slavedns1
NS slavedns2

NS update

masterdns

Zone mycompany.com
SOA masterdns
NS masterdns
NS slavedns1
NS slavedns2

slavedns1

slavedns2

Zone mycompany.com
SOA masterdns
NS masterdns
NS slavedns1
NS slavedns2
Master-Slave pros

- Only one server has to be updated
- The DNS protocol itself is used to update slave zones
  - No additional script needed
- Easier to configure and maintain
Master-Slave cons

- Administrators will not be able to locally update the DNS servers, when the master is down

- In the case of a public DNS, the identity of the DNS master is known
Master-Slave usage

- This is the first DNS architecture created and the most deployed
- This is a standard DNS architecture
DNS Multi-Masters architecture
Multi-Masters Principles

- The DNS Multi-masters architecture relies on the SOA RR MNAME field (RFC 1035).

- Each DNS server will list itself as MNAME.

- All zones list the name servers that are members of the architecture as NS.
Multi-Masters Principles

Zone mycompany.com
SOA masterdns1
NS masterdns1
NS masterdns2
NS masterdns3

Zone mycompany.com
SOA masterdns2
NS masterdns1
NS masterdns2
NS masterdns3

Zone mycompany.com
SOA masterdns3
NS masterdns1
NS masterdns2
NS masterdns3
Multi-Masters pros

- NS updates can be locally done on the servers, ensuring an up-to-date DNS even when the WAN/MPLS link is down.
Multi-Masters cons

- Complexity: a dedicated tool or a set of maintained scripts is necessary to replicate in real time all modifications on all servers

- Increase of the communication latency
Multi-Masters usage

- The Multi-Masters architecture is mainly used on Microsoft Active Directory infrastructures.

- Any domain controller can send or receive updates of information stored in Active Directory.
DNS Stealth architecture
Stealth Principles

- The DNS Stealth architecture is a Master-Slave architecture where the DNS Master is hidden from DNS clients.

- One Slave server is chosen to be the Pseudo Master. This pseudo master will be the NS configure as MNAME of the SOA.

- All zones list the SLAVE and Pseudo Master name servers that are members of the architecture as NS. **BUT NOT THE HIDDEN MASTER**

- The DNS master is authorized to notify slave zone and answer to AXFR or IXFR DNS transactions from slaves members of the Stealth architecture.
Stealth Principles

Zone mycompany.com
SOA pseudomasterdns
NS pseudomaster
NS slavedns

Zone mycompany.com
SOA pseudomasterdns
NS pseudomaster
NS slavedns

NS update

Pseudo Master

Slave DNS
Stealth pros

- Only one server has to be updated

- The DNS protocol itself is used to update slave zones

- The identity of the DNS master Hidden is only known by the administrator

- It is not mandatory to have a public IP as DNS Master Hidden
Stealth cons

- Administrators will not be able to locally update the DNS servers when the master is down.

- The DNS hidden is not supposed to resolve DNS client queries.

- This architecture is complex and a dedicated tool is necessary to deploy it properly.
Stealth usage

- The Stealth architecture is mainly used on Public DNS architectures

- It is a relevant architecture when data is critical and needs specific protection mechanisms.
The SmartArchitecture
Ease of Deployment

- Automate DNS architecture deployment
  - Library of SmartArchitecture DNS templates
  - Automated configuration of all DNS servers according to selected SmartArchitecture
  - Best practices enforcement

- DNS Stealth: State of the Art Internet DNS architecture
  - Most secure Internet DNS architecture

A DNS slave server is published to DNS clients as the Master DNS server

DNS Pseudo Master (Slave)

Hidden DNS master

DNS Master server is hidden to DNS clients behind firewalls

DNS Slave server
SmartArchitectures: Automated Architecture Deployment

**Step 1**
Select your Architecture

1. [Diagram of step 1 selection]
2. [Diagram of step 1 selection]
3. [Diagram of step 1 selection]
4. [Diagram of step 1 selection]

**Step 2**
Import your Data

Management of the SmartArchitecture as one “Virtual server”

**Step 3**
Insert your Servers

- DNS Slave
- Hidden DNS Slave
- Pseudo Master

**Done!**
Your Architecture is Deployed and Operating

Management appliance configures all servers automatically
SmartArchitecture: Move to Architecture Management!

- Reduce Complexity: Manage Architectures rather than servers
- Automate your Deployment and Management
- Best practices enforcement

Diagram:
- DHCP Star Failover
- DNS Master-Slave
- DHCP Split Scope
- Global Architecture Management
- DNS Multi-Master
- DNS Stealth
IP addressing plan management

Network services engines: DNS-DHCP-NTP-TFTP

Multi-vendor DNS&DHCP services management
  - Microsoft – ISC – Cisco – SOLIDServer™

Active IP address Tracking with IPLocator module

Built-in work flow

Unified system management
  - Integrated zero admin database
  - Hardened OS with embedded stateful firewall
  - Easiness of upgrade, backup and disaster recovery management
Please feel free to contact us for more information or a presentation of EfficientIP solutions:
By email: info@efficientip.com
Or via our website: www.efficientip.com