



# ROOT SERVERS MANAGEMENT AND SECURITY

WSIS African regional meeting

01/29/05

*ALAIN PATRICK AINA*

**aalain@trstech.net**

# What is DNS(1)?



- Addresses are used to locate objects
- Names are easier to remember than numbers
- You would like to get to the address or other objects using a name

**DNS provides a mapping from names to resources of several types.**

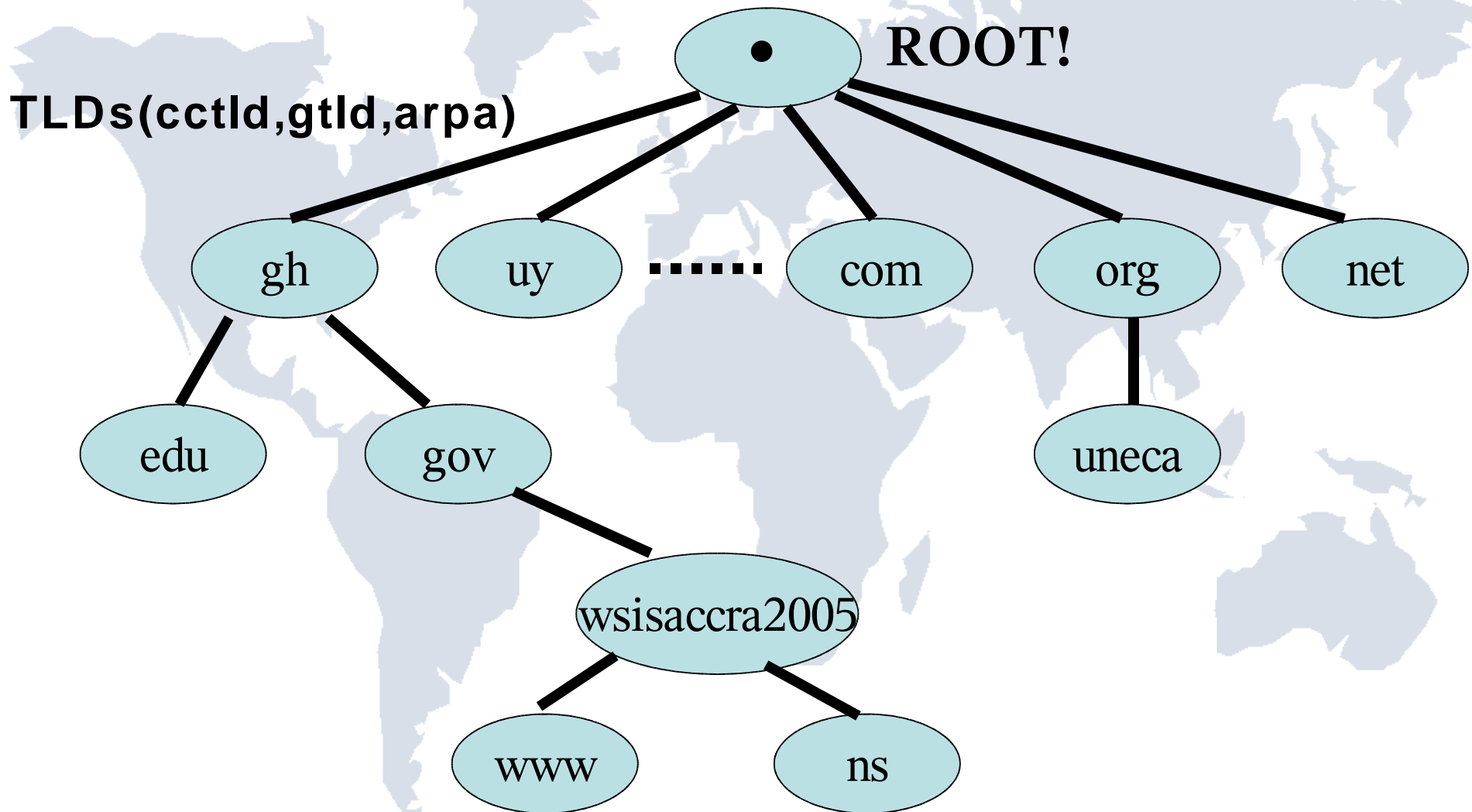
# What is DNS(2)?



- A lookup mechanism for translating objects into other objects
- A globally distributed, loosely coherent, scalable, reliable, dynamic database
- Comprised of three components
  - A “name space”
  - Servers making that name space available
  - Resolvers (clients) which query the servers about the name space

**A key component of the Internet infrastructure**

# What is DNS(3)?

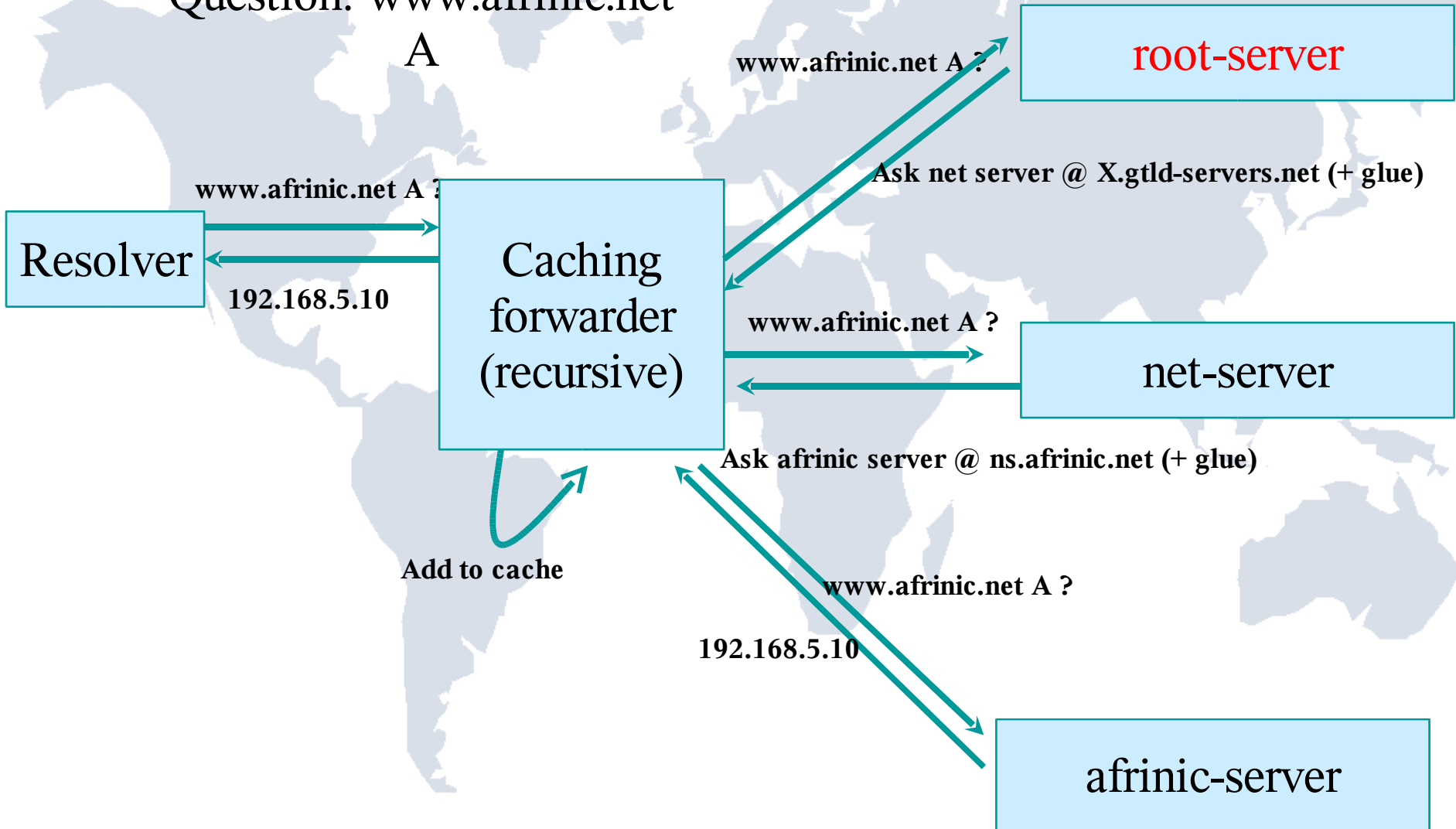


The DNS Tree

# How it works?

Question: www.afrinic.net

A



# Root servers(1)

- Assure the « universal resolvability » to the Internet users
  - Provide the critical first step in resolving unique names and addresses
- Currently limited to 13 distinct entries in the list
  - a.root-servers.net,...,m.root-servers.net
  - Geographical and topologically distributed
  - Running on different variants of Unix operating system
  - Operated by 12 different professional engineering groups
- More than 13 servers
  - Anycast DNS

# Root servers(2)



Root server operators distribution

# Root servers(3)

Server	Operator	Locations
A	VeriSign Global Registry Services	Dulles VA
B	Information Sciences Institute	Marina Del Rey CA
C	Cogent Communications	Hemdon VA; Los Angeles; New York City; Chicago
D	University of Maryland	College Park MD
E	NASA Ames Research Center	Mountain View CA
F	Internet Systems Consortium, Inc.	Ottawa; Palo Alto; San Jose CA; New York City; San Francisco; Madrid; Hong Kong; Los Angeles; Rome; Auckland; Sao Paulo; Beijing; Seoul; Moscow; Taipei; Dubai; Toronto; Monterrey; Lisbon; Johannesburg; Tel Aviv; Jakarta; Munich; Osaka; Prague
G	U.S. DOD Network Information Center	Vienna VA
H	U.S. Army Research Lab	Aberdeen MD
I	Autonomica/NORDUnet	Stockholm; Helsinki; Milan; London; Geneva; Amsterdam; Oslo; Bangkok; Hong Kong; Brussels; Frankfurt; Ankara; Bucharest; Chicago; Washington DC; Tokyo; Kuala Lumpur
J	VeriSign Global Registry Services	Dulles VA (2 locations); Mountain View CA; Seattle WA; Amsterdam; Atlanta GA; Los Angeles CA; Miami; Stockholm; London; Tokyo; Seoul; Singapore; Sterling VA (2 locations, standby)
K	Reseaux IP Europeens – Network Coordination Centre	London (UK); Amsterdam (NL); Frankfurt (DE); Athens (GR); Doha (QA); Milan (IT); Reykjavik (IS); Helsinki (FI); Geneva (CH); Poznan (PL); Budapest (HU)
L	Internet Corporation for Assigned Names and Numbers	Los Angeles
M	WIDE Project	Tokyo; Seoul (KR); Paris (FR)

Root servers distribution(12/16/04) : One instance of F.root-servers.net in johannesbourg

# Root zone



- The information itself (only TLDs delegation and glue data)
- Created by IANA, distributed to root-servers by Veri-sign
  - After authenticity and technical consistency checks
  - Reviewed and audited by DoC
  - Available at [ftp.internic.net/domain](ftp://ftp.internic.net/domain)

# Root servers operators(1)



- 12 different professional engineering groups
  - Diverse organisational structure
  - Diverse operational history
  - Diverse hardware and software
- Focused on
  - Reliability, and stability of the service
  - Accessibility to all the Internet users
  - Technical cooperation
  - Professionalism

# Root servers operators(2)



- Communication procedures
  - Normal operation
    - Regular Meetings(IETF.....), mailing list, normal phone
  - Special situation
    - Encrypted e-mail, private telephone number, conference telephone bridges
- Operation based on RFC2870
  - “Root Name Server Operational Requirements”

# Root servers operators(3)

- Coordination within ICANN
  - RSSAC
- No formal contract with ICANN
- Data publishers, not authors or editors
- Present in different technical forums and meetings
  - IETF, APNIC, ARIN, RIPE, NANOG, AFNOG

# Root servers system security(1)



- Physically protected
- Tested operational procedures
  - Root zone file integrity, authenticity and validity
  - Permanent infrastructure to respond to emergency
    - Phone bridge, mailing lists, exchange of secure credentials.....
- Experienced, professional and trusted staff
- Careful operational evaluation of technical suggested modifications

# Root servers system security(2)



- Major operational threat is DDOS
  - Defense :
    - Anycast
    - Overprovisioning
    - Law enforcement

# Responses to an evolving Internet



- IPv6 glue possible for TLDs in root zone
- Increasing robustness and responsiveness as well as resilience with wide deployment of distributed anycast
- Analysis of impact of new uses and protocols on the services
  - IPV6
    - AAAA records for the root servers
  - DNSSEC
    - Signing root zone
    - Root key management, Key rollover, etc...

# Useful links



- ICANN RSSAC
  - <http://www.icann.org/committees/dns-root/>
- Root Name Servers
  - <http://www.root-servers.org>
- IANA
  - <http://www.iana.org>.
- ICANN SSAC
  - <http://www.icann.org/committees/security>



Questions ?