menog
MIDDLE EAST NETWORK OPERATORS GROUP
A forum for network operators in the Middle East

RIPE NCC

Technical & Research Reports and Updates

MENOG 4/RIPE NCC Regional Meeting, Manama, Bahrain, 9 April 2009

Alaa Al-Din (Aladdin) Jawad Kadhem Al-Radhi :
Consultant Engineer and Researcher
Masters CINS "Computer Information Network Security"
DePaul Univeristy Chicago, Illinois USA
PHD Applicant : Internet Researches
alradhi2000@yahoo.ca alaalradhi@hotmail.com
+ 962 796347600

Motto: You can NOT gain ground if you are standing still!

About Me! Passionate / Advocate of All Internet Works, Advances, Researches, Collaborations, etc

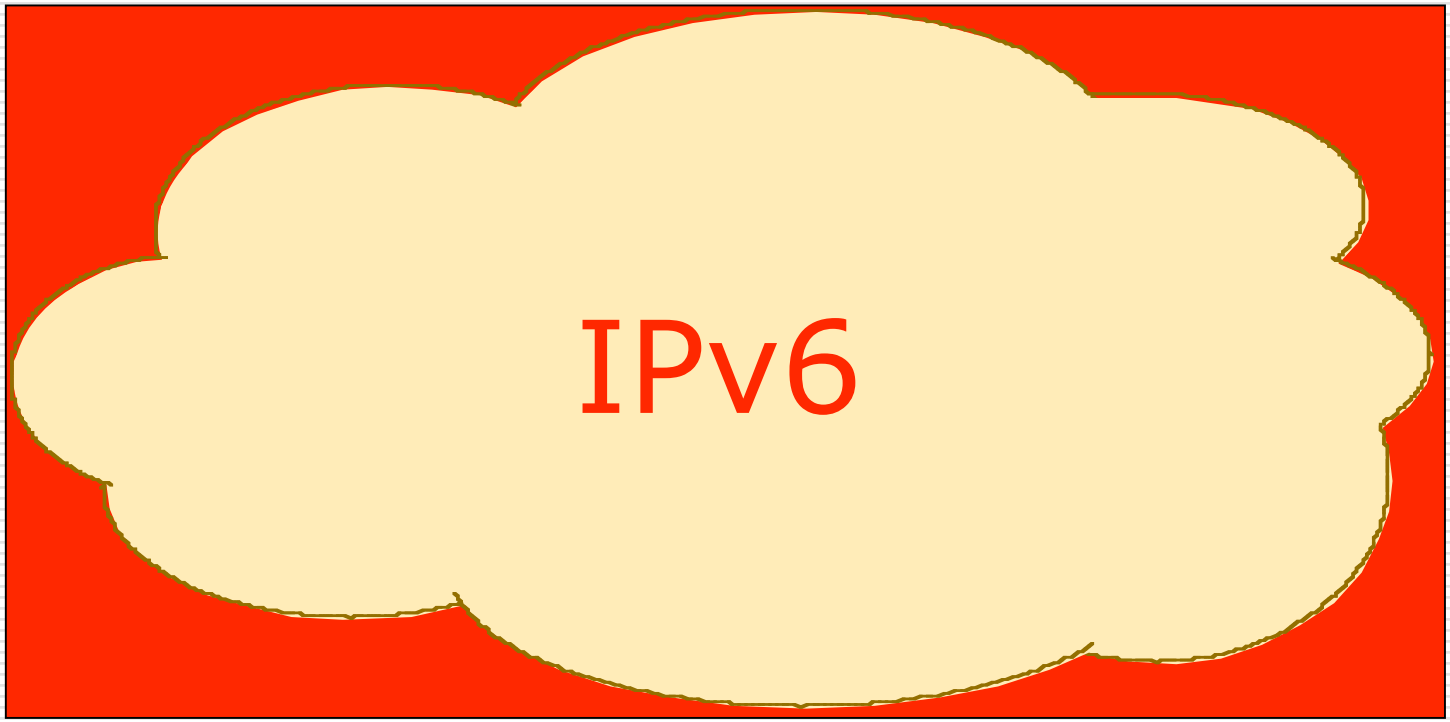
- Advisory Council Member of PIR (Public Interest Registry), www.pir.org
- ICANN "Board of Directors" Nomination Candidate 2009-2011, and Fellow www.icann.org
- AKMS (Arab Knowledge and Management Society) "Board of Trustees" Member, www.akms.org
- ISOC (Internet Society) IGF Ambassador and Global Member www.isoc.org
- ITU Arab Regional Office affiliated Consultant, speaker and presenter www.itu.int
- DIPLO Foundation Internet Governance Fellow www.diplomacy.edu
- DePaul University Security Group, Alumni and International Contact www.depaul.edu
- Member of "Internet 2" www.internet2.edu Middle East Group
- Member of "EUMEDCONNECT 2" www.eumedconnect2.net Middle East Group
- Member of ASIWG " Arabic Script Internationalized Domain Names Work Group www.arabic-script-domains.org
- Member of AOIR "Association Of Internet Researchers" www.aoir.org
- Fellow of RIPE-NCC & MENOG " Middle East Network Operators Group" www.ripe.net and www.menog.net
- Information Share Award Winner 2007-2009 & Member of ASIS&T " American Society for Information Science and Technology" www.asis.org
- Steering Committee Member ACS Arab Computer Society www.arabcomputersociety.org
- Member of EU Communications and Research Association www.ecrea.eu
- Member of IHEOST "Iraq Higher Education Organization for Science & Technology" www.wmin.ac.uk/iraq-he & www.iraqhe.com

Taking Steps Ahead:

IPv6

Internet Security

EREN (Emerging Research & Education Networks)


IPv6

IPv6

IPv6

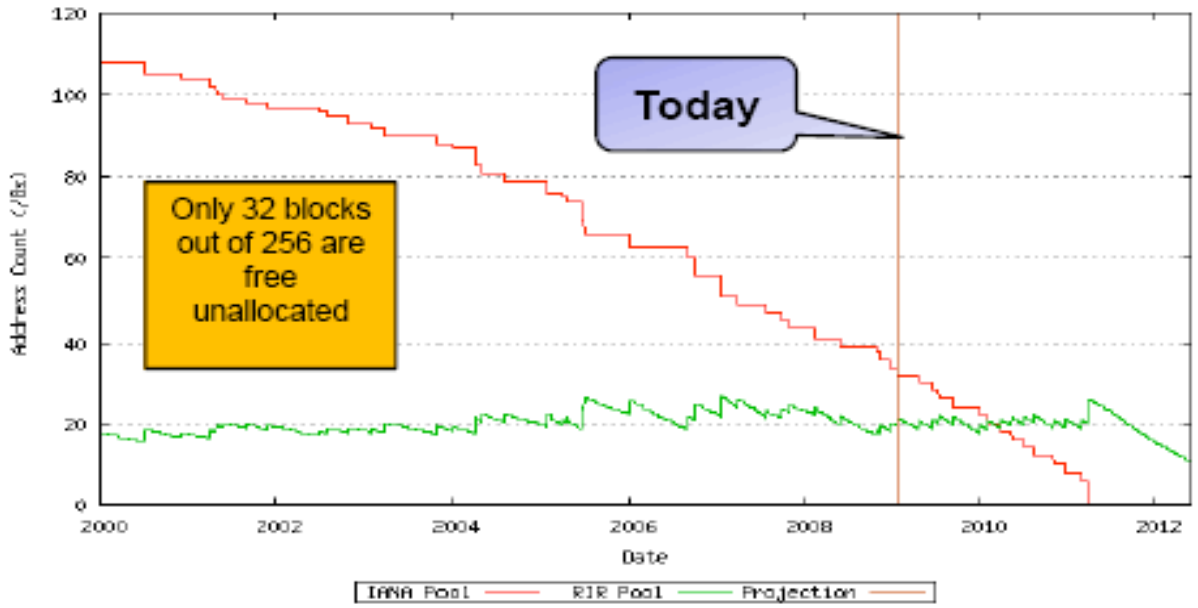
Index:

IPv6

Quick: Why?

IPv6

IPv4 Depletion Predictions at IANA and RIRs



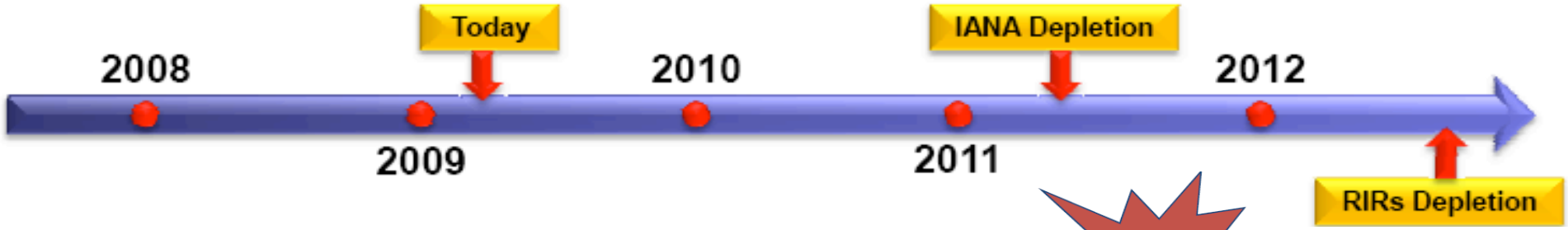
As of January 2009:

Projected Depletion date at IANA: March 2011

Projected Depletion date at RIRs: August 2012

Source
"The IPv4 Address Report"
By Geoff Huston

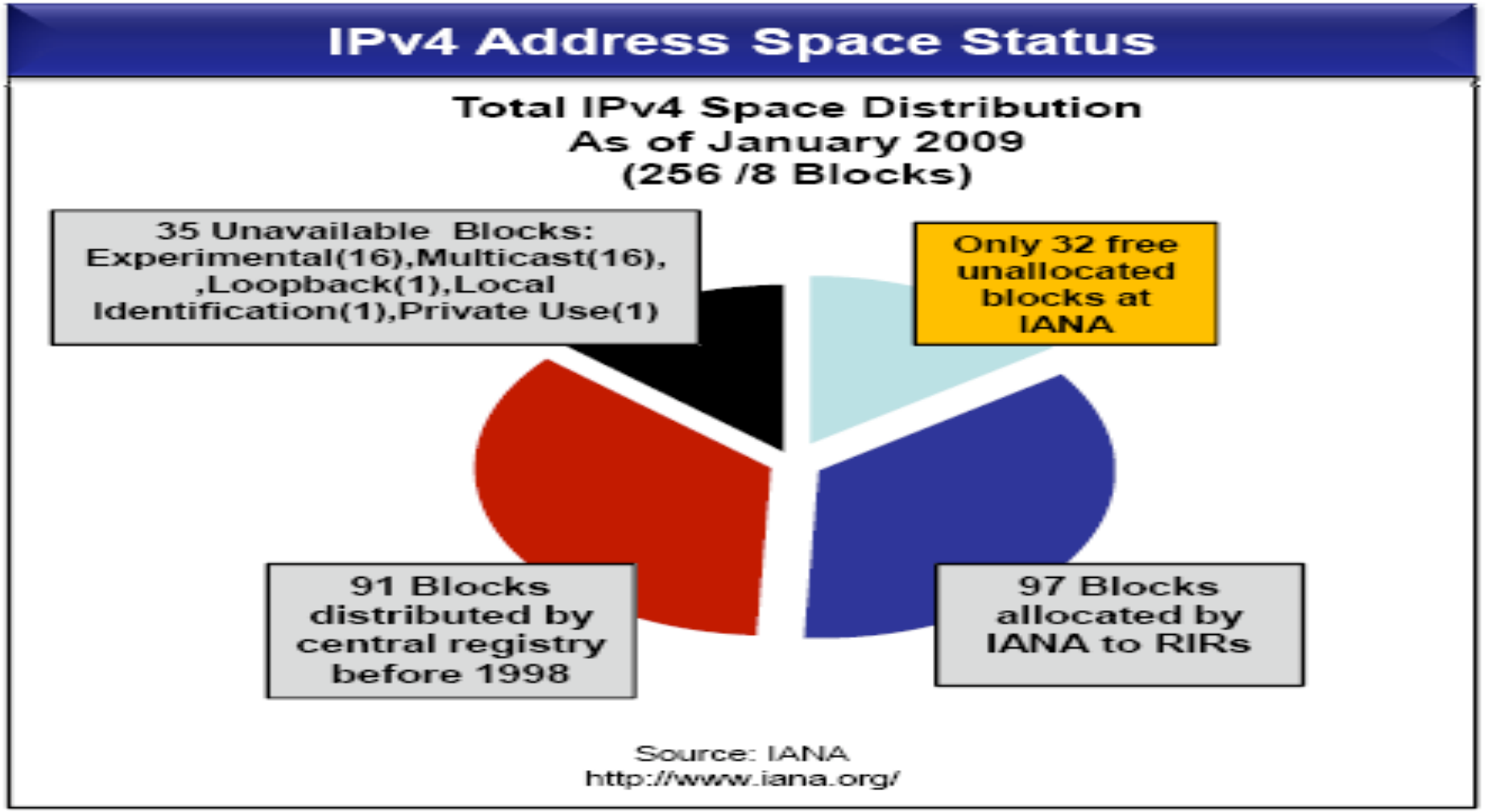
http://www.potaroo.net/tools/ipv4/



IPv4 Run-Out

IPv4 Depletion Assessment

Quick: Why?


IPv4 Address Space Status
Total IPv4 Space Distribution
As of January 2009
(256 /8 Blocks)
35 Unavailable Blocks: Experimental(16),Multicast(16), ,Loopback(1),Local Identification(1),Private Use(1)
Only 32 free unallocated blocks at IANA
91 Blocks distributed by central registry before 1998
97 Blocks allocated by IANA to RIRs
Source: IANA
http://www.iana.org/

Quick: Benefits?

IPv6

Impact Metric	Application / Market	General Description: Examples
Cost reductions resulting from increased efficiency	NAT removal	enterprise and application vendors" spending on NAT workarounds accounts for up to 30% of IT related expenditures.
Value of remote access to existing products/services	Increased life expectancy of products	Automobile64 and appliance owners65 could increase the functionality and life expectancy of their products through the use of remote monitoring and support services.
	Service costs	Automotive and appliance owners could decrease service costs through the use of remote monitoring and support services.
Innovation in communications and online products/services	New mobile data services	•Wireless companies could sell new features through expanded network capabilities. •Wireless companies need IPv6 to increase address capacity for peer to peer (P2P) applications.
	Online gaming	Gaming and game console makers could see expanded functionality and thus opportunities for innovative new products

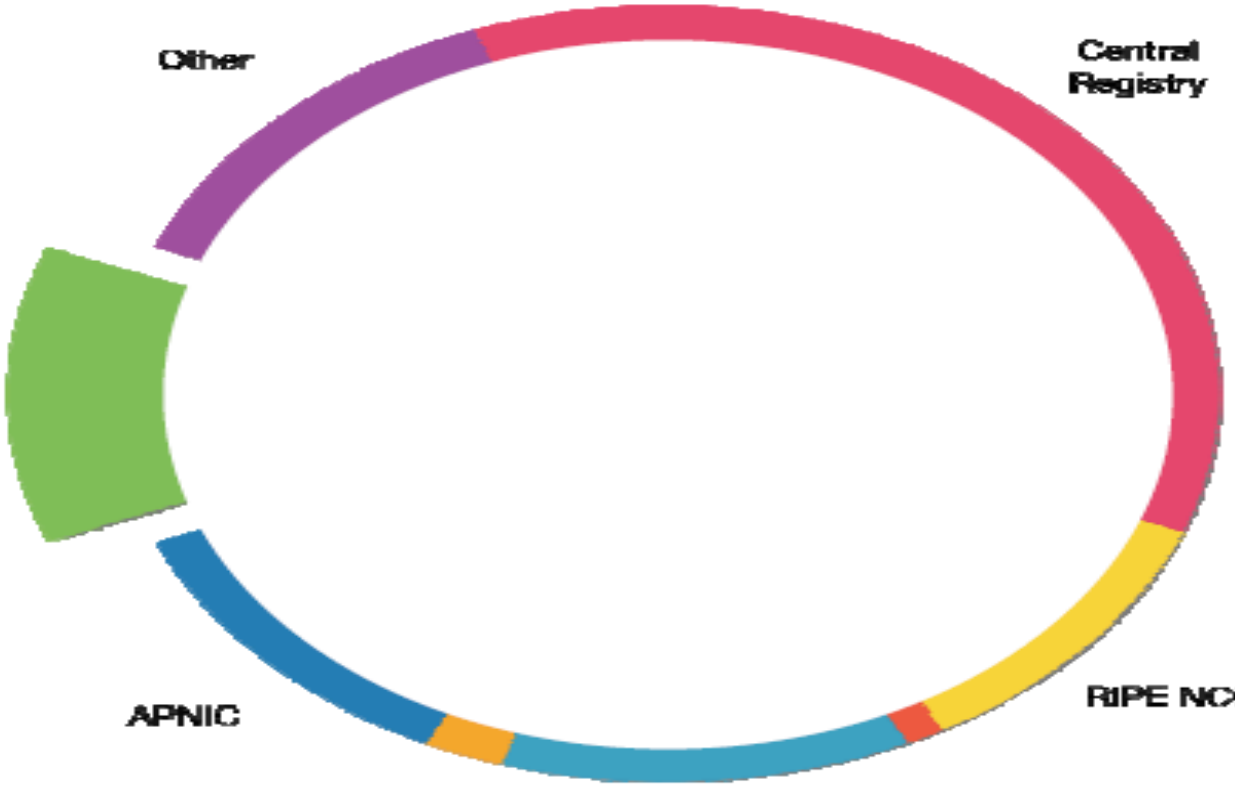
IPv6

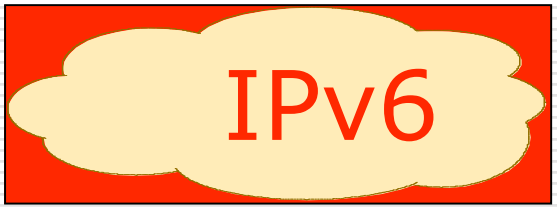
RIPE NCC

IPv6

IPv4 Address Poll NOW:

12%
available





RIPE NCC

IPv6

PDP (Policy Development Process) Issues:

- IPv4 depletion
- Remove any remaining obstacles for IPv6 allocations:
  - IPv6 Allocation criteria altered:
    - No more requirement for assignments to *others*
    - No more requirement for 200 customers
  - New End Site definition:
    - LIRs internal assignments count as End Site
  - LIRs: Plan to make sub-allocations to others or assignments to End Sites
  - IPv6 for End Users
- Get ready for IPv4 endgame
- Sustained IPv4 usage

RIPE NCC

IPv6

Conclusions:

- Increase IPv6 deployment:
  - Easier access to resources
  - Raise awareness
- Get ready for IPv4 endgame:
  - Minimize depletion impact
  - Increased contact with space holders
  - Increased efficiency in usage
  - Enabling usage of allocated but unused space
  - Focus on fairness and responsible stewardship
- Get Involved!
  - Address Policy WG Mailing list
  - http://www.ripe.net/ripe/maillists/archives/address-policy-wg/
  - Policy Announce Mailing List
  - http://www.ripe.net/ripe/maillists/archives/policy-announce/

Regional Highlights: KSA:

WORKSHOP ON THE IPv6 DEVELOPMENT IN SAUDI ARABIA Feb 8 2009

IPv6 Strategy:

Strategic Objectives

- Prepare for the IPv4 exhaustion by supporting IPv6 and ensure stability, business continuity and room for continued growth of the internet in Saudi Arabia
- Ensure a smooth adaption of IPv6 by stakeholders so as to minimize risks
- Raise overall IPv6 awareness nationwide by approaching stakeholders of both the public and private sectors highlighting the necessecity to adopt IPv6

Strategy Implementation Tracks

Infrastructure

- Five (5) Initiatives:
  - IPv6 Addressing
  - IPv6 Commercial Support for Nation Wide Infrastructure
  - .SA ccTLD IPv6 Compliance
  - IPv6 Compliant Internet Filtering
  - IPv6 Lab

Awareness

- Five (5) Initiatives:
  - IPv6 Task Force
  - Outreach Activities
  - International Cooperation
  - IPv6 Training
  - IPv6 Compliant Procurement

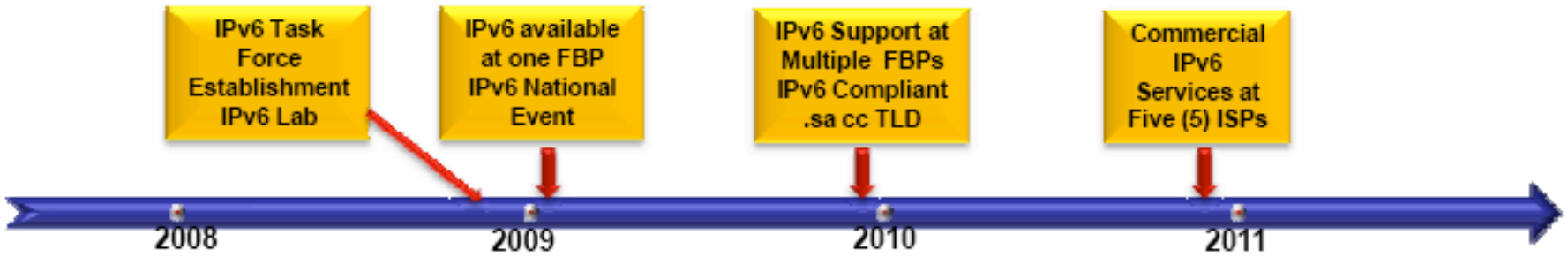
IPv6

Regional Highlights: KSA:

WORKSHOP ON THE IPv6 DEVELOPMENT IN SAUDI ARABIA Feb 8 2009

IPv6 Road Map and Next Steps:

Milestones	Why?	Date	Status
Basic IPv6 Connectivity available at ONE FBPs	Essential and Enough to start offering IPv6 to ISPs and End Users	Early 2009	TBC
IPv6 Task Force Saudi Arabia	Essential to raise awareness and encourage deployment	July 2008	Already Established
Establish an IPv6 Lab	Establish and Disseminate practical IPv6 Experience	15 January 2009	Ready
IPv6 workshop	Raise awareness and encourage the IPv6 deployment	8 February 2009	Today
IPv6 at Multiple FBPs	Important for ISPs and End Users to have more than one Choice	End 2009	TBC
IPv6 Compliant.SA ccTLD Registry	Essential to run IPv6-only hosts or an IPv6-only infrastructure	End 2009	TBC
Commercial IPv6 Services available from Five (5) ISPs	More choices to end users	End 2010	TBC



http://ipv6.org.sa/

IPv6

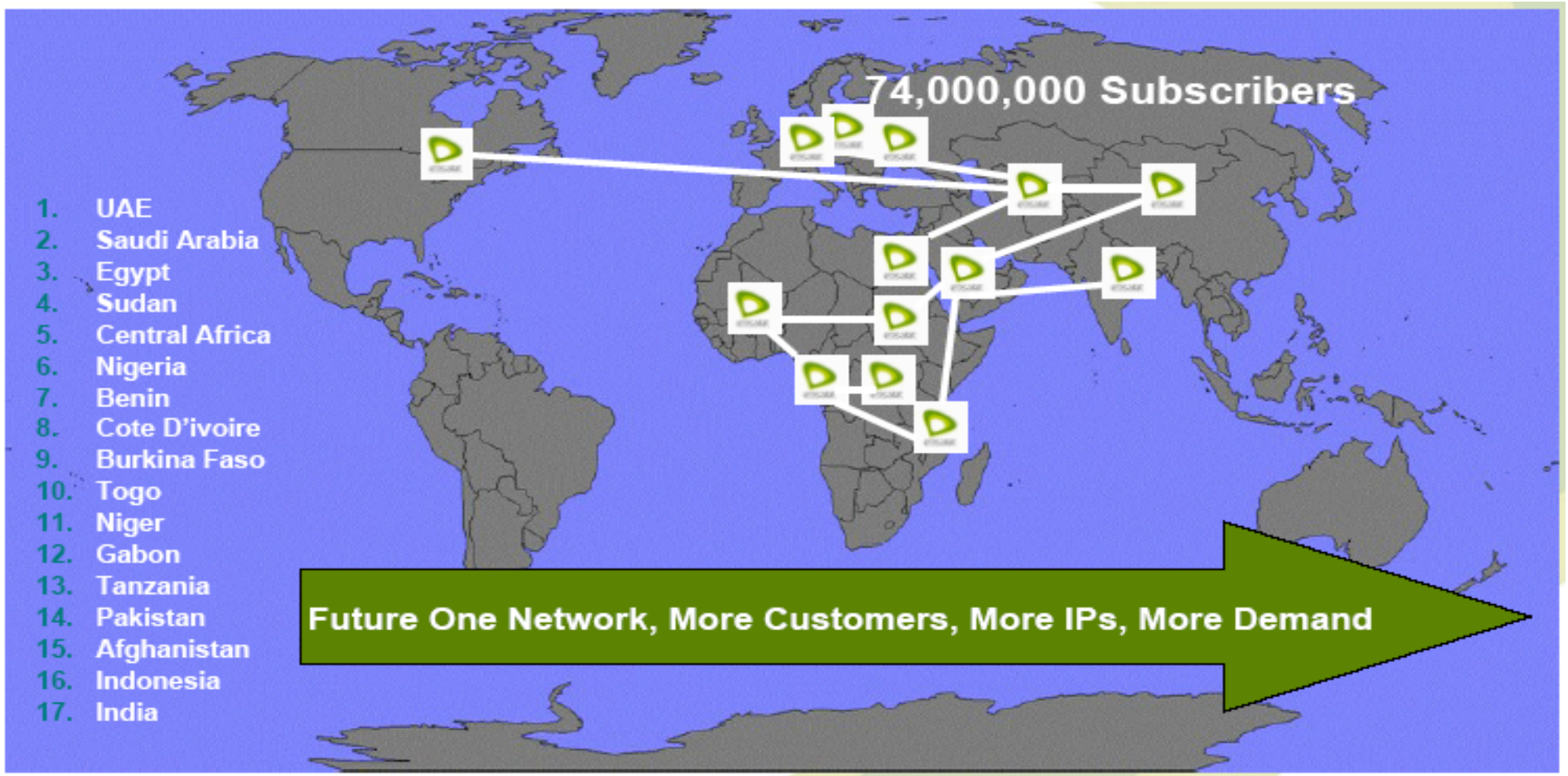
Regional Highlights: UAE:

UAE IPv6 Task Force (Formed in 2005)

IPv6

Regional Highlights: UAE:

Etisalat: Growth & Demands: 17 Countries



IPv6

Regional Highlights: UAE:

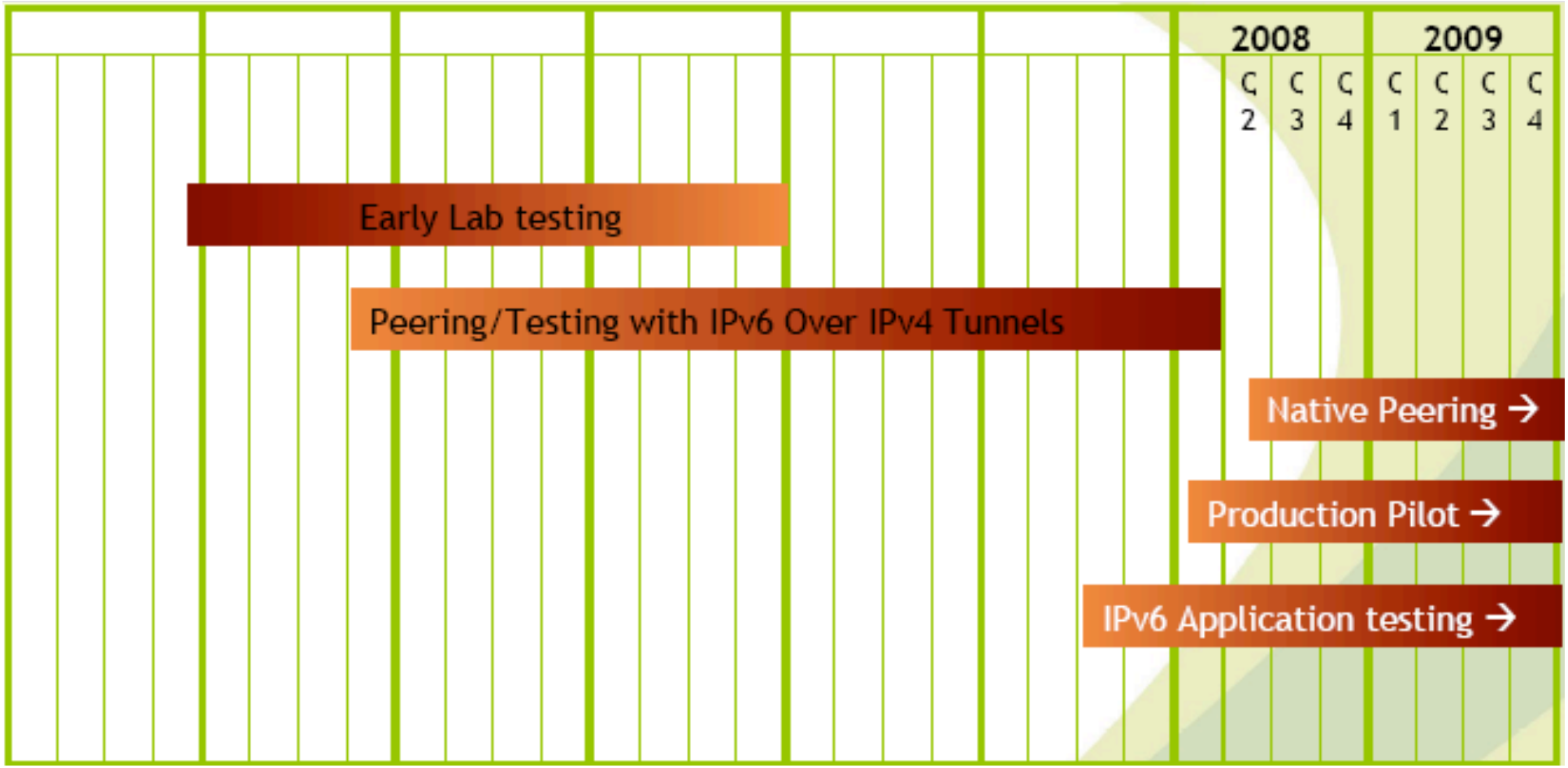
Etisalat: IPv6 History

Form Etisalat IPv6 Task Force & Steering committee	May, 2001	Completed
Test IPv6 with 6Bone (via SPRINTv6)	Oct, 2001	Completed
Obtain Global Unicast IPv6 Addresses from (RIPE NCC)	Oct, 2001	Completed
Building Etisalat Basic IPv6 test network	Feb, 2002	Completed
Building Etisalat IPv6 Systems Infrastructure. (DNS,WEB)	July, 2003	Completed
www.ipv6.ae , Lab.ipv6.ae Publishing.	Oct, 2003	Completed
Verifying networks and services elements IPv6 support.	May, 2004	Completed
Testing with regional ISPs and with EMIX Customers.	N/A	In Progress
IPv6 implementation plan 2007-2011	2007	Yearly
First IPv6 production network (ZBL Network Development & NOC)	Jan, 2008	RFS

IPv6

Regional Highlights: UAE:

Etisalat: IPv6 Roadmap

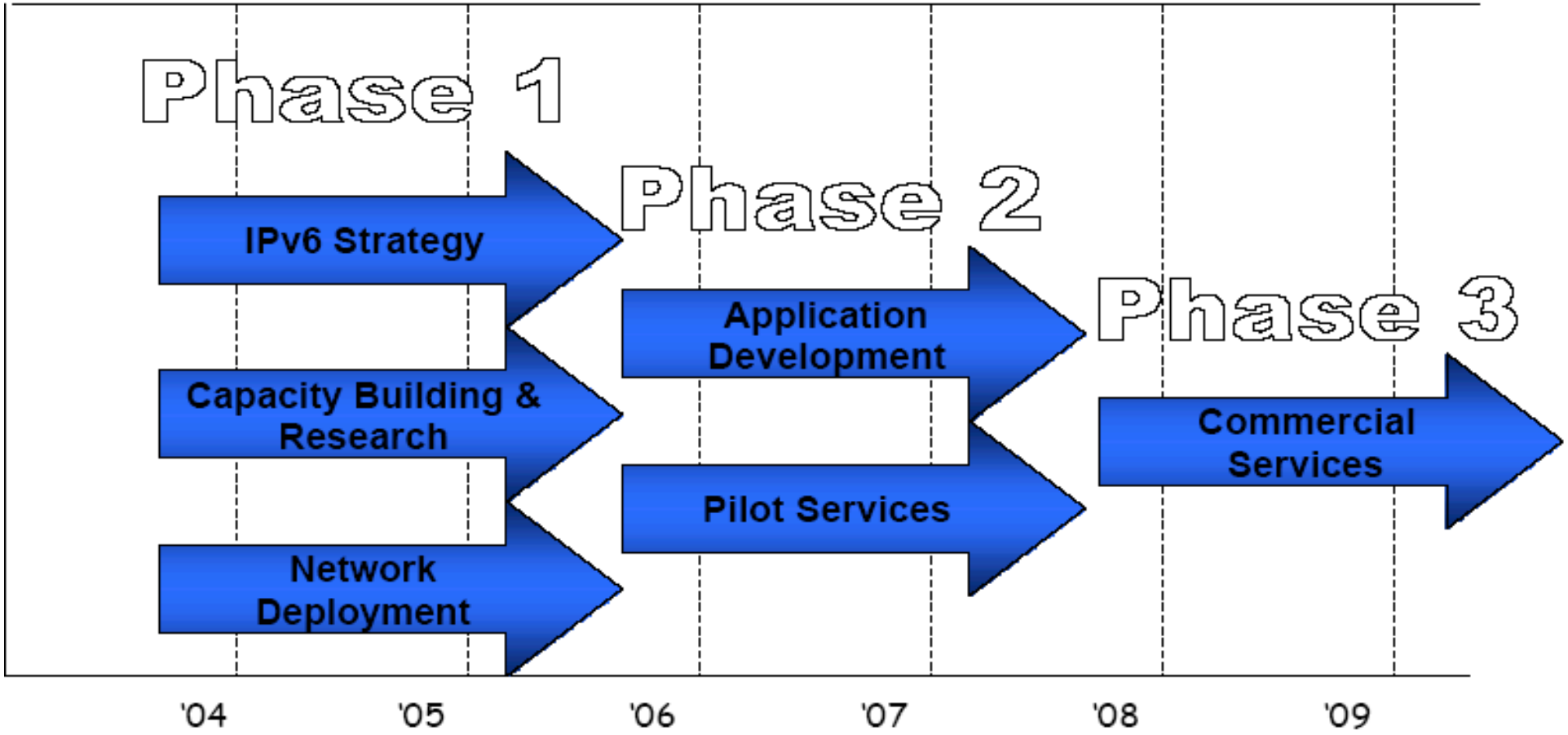


IPv6

Regional Highlights: Egypt:

EGYPT IPv6 TASK FORCE

Egypt IPv6 Task Force (Formed in 2004)



IPv6

Regional Highlights: Egypt:

EGYPT IPv6 TASK FORCE

Egypt IPv6 NREN

EGYPT IPv6 TASK FORCE

The National Research & Education Network

EUN

- Cairo University
- Alexandria University
- Ain Shams University
- Assiut University
- Tanta University
- Mansoura University
- Zagazig University
- Helwan University
- Minia University
- Menofia University
- Suez Canal University
- South Vally University
- Al-Azhar University
- Banha University
- Fayom University
- Bany swief University

2001:4300:2001::/48

ENSTINET

- National institute of Astronomy and Geophysics
- National Authority of Remote Sensing & Space Sciences
- National Research Center & Electronic Research
- National Institute of Measures and Standardizations
- National Telecommunications Institute
- Mobark City for Scientific Research and Applied Technology
- Egyptian Petroleum Research Institute
- Tudoar Belhares Research Institute
- Eye Diesis Research Institute
- Metal deployment Research Institute
- Ministry of Communication and Information Technology

2001:4300:4300::/48

What's Next?

IPv6

- Start Solid steps to form IPv6 Task Force in your country if does NOT exits. You can have assistance from others.
- Participate to WGs, mailing lists, etc: RIPE, IETF, etc
- Read Best global practices to prepare your self.
- You can form a local focus / WG to highlight regional Internet concerns and Q / A.
- Spread the words. Info. should NOT stay ONLY on your HD! "Knowledge" is Power, & "Knowledge Share" is Success.
- Start Awareness Campaigns among your peers.

- Some references, NOT limited to:
  1. www.ipv6.eu
  2. www.ipv6day.org
  3. www.ipv6forum.com
  4. www.ipv6.org
  5. www.ipv6tf.org
  6. www.go6.net
  7. www.ipv6.net
  8. www.Ipv6ready.org

  .....Any Many others!

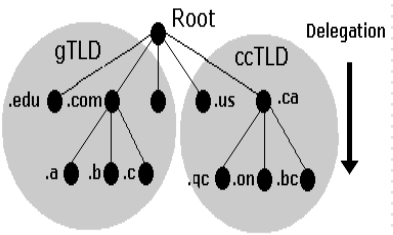

Internet
Security

Index:

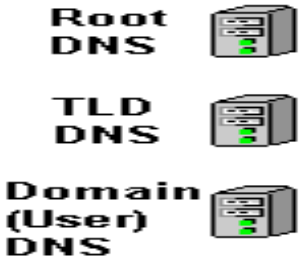
- DNS Domain Name System:
  - Briefing
  - Threats and Attacks
  - "Cache poisoning" Flaw /April 2008
- Internet Hardening: DNSSEC
  - Why?
  - Problems
  - Timeline: 4 Phases
  - Your Organization Strategy?
  - Conclusions & What's Next?
  - New Shots: March 2009

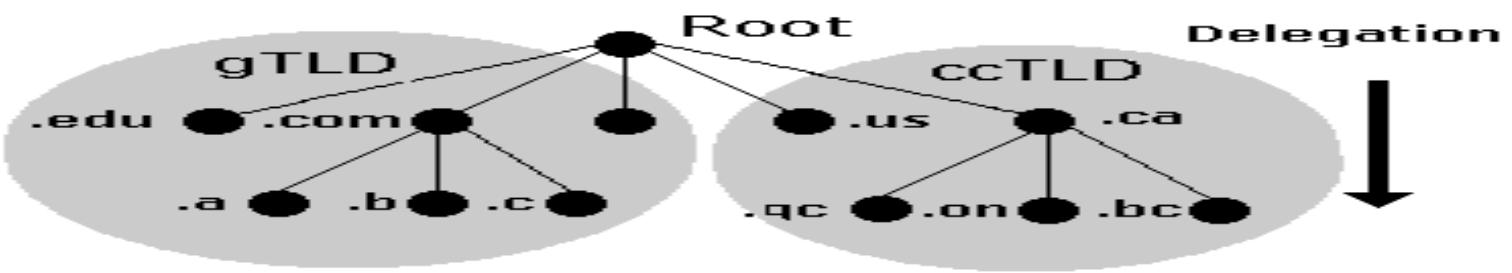
Internet Security

DNS: Briefing



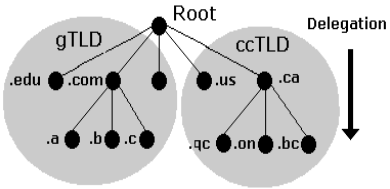
- DNS is one of the basic building blocks of Internet:
  - It converts logical names for resources on the Net to IP
  - Is the Internet directory and phone book
  - Decides if your site can be reached and email delivered
  - Prevents Outages and Provides Redundancy
- DNS have a hierarchical Structure:
  - A Root domain (represented by a single dot "."),
  - A set of TLDs , such as .com or .ca, and
  - Any number of levels under these TLDs.





Internet Security

DNS: Briefing



- Tells machines where to go when you:
  - Type in a web address
  - Send an email

User

ISP

Name Server Operators

Resolver

Am I online?
Where should I go to get my answer?
- My local Internet Service Provider

Cache

Do I already have the answer?
- Send the answer back to resolver

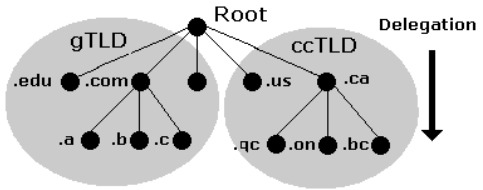
Else, contact Domain Name Server

Name Server

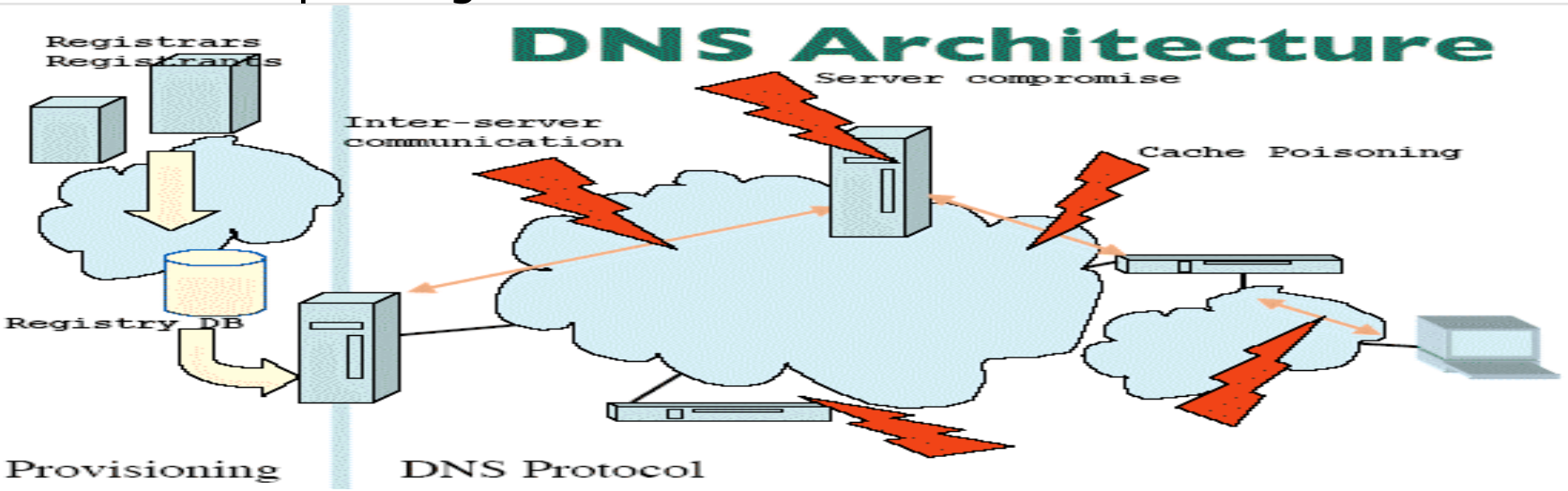
Find the IP address
Send it back

Internet Security

DNS: Threats & Attacks



- The original DNS is NOT secure. Vulnerabilities help Attackers to intercept DNS by faking network packets or gaining access to servers on network to corrupt and destroy information.
  - Forgery: DNS data being returned to your ISP can be forged, especially easy on a wireless network, so you are transported where you did NOT mean to go
  - Poisoning: DNS data can be modified, causes your ISP cache to have valid but wrong information on where to go
  - Eavesdropping: Can intercept your DNS data and just "listen" before passing on



Internet Security

DNS Flaw: "Cache poisoning" of April 08

Discovered by Dan Kaminsky

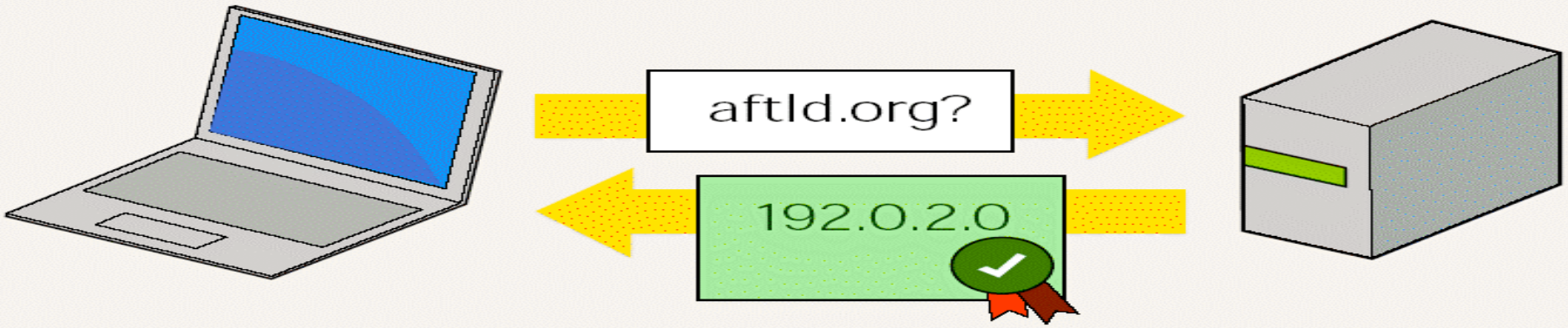
- Transaction IDs (which are supposed to prevent attackers from assigning their own IP address to any domain) are ineffective as security measures. An attacker could flood a DNS server with multiple varied requests for a domain, such as 1.foo.com, 2.foo.com. As transaction IDs can only be a No. between 0 and 65535, and the attacker can launch multiple requests, then the attacker could spoof a domain by matching ID through chance.
- Once this domain is spoofed, the attacker can flood a Name-Server with spoofed replies to poison its cache for the domain being attacked: for e.g. foo.com. Requests for foo.com would direct a user to a site of the attacker's choosing.
- This vulnerability can be exploited by using multiple vectors of attack. Web browsers can be forced to look up what the attacker wants, as links, images and ads can cause a DNS look-up. Mail-Servers will look up what an attacker wants when performing functions such as a spam check, or when trying to deliver a newsletter, or email response.
- Dan Kaminsky warned that it is also possible to pollute TLD: .com, .net and .org.

Internet Security

Internet Hardening DNSSEC: Why?

DNSSEC

- Confirm the integrity of the information i.e. proof the data has NOT been modified in transit from the DNS zone publisher (the registry) to the end-user
- Authenticate the source of the information: providing something like a "seal of origin", that can be verified. DNS response is only considered correct if the attached signature can be verified. Each domain has a unique signature
- Provide: Defense layers: Multiple defense rings in physical secured systems and Multiple layers in the networking world



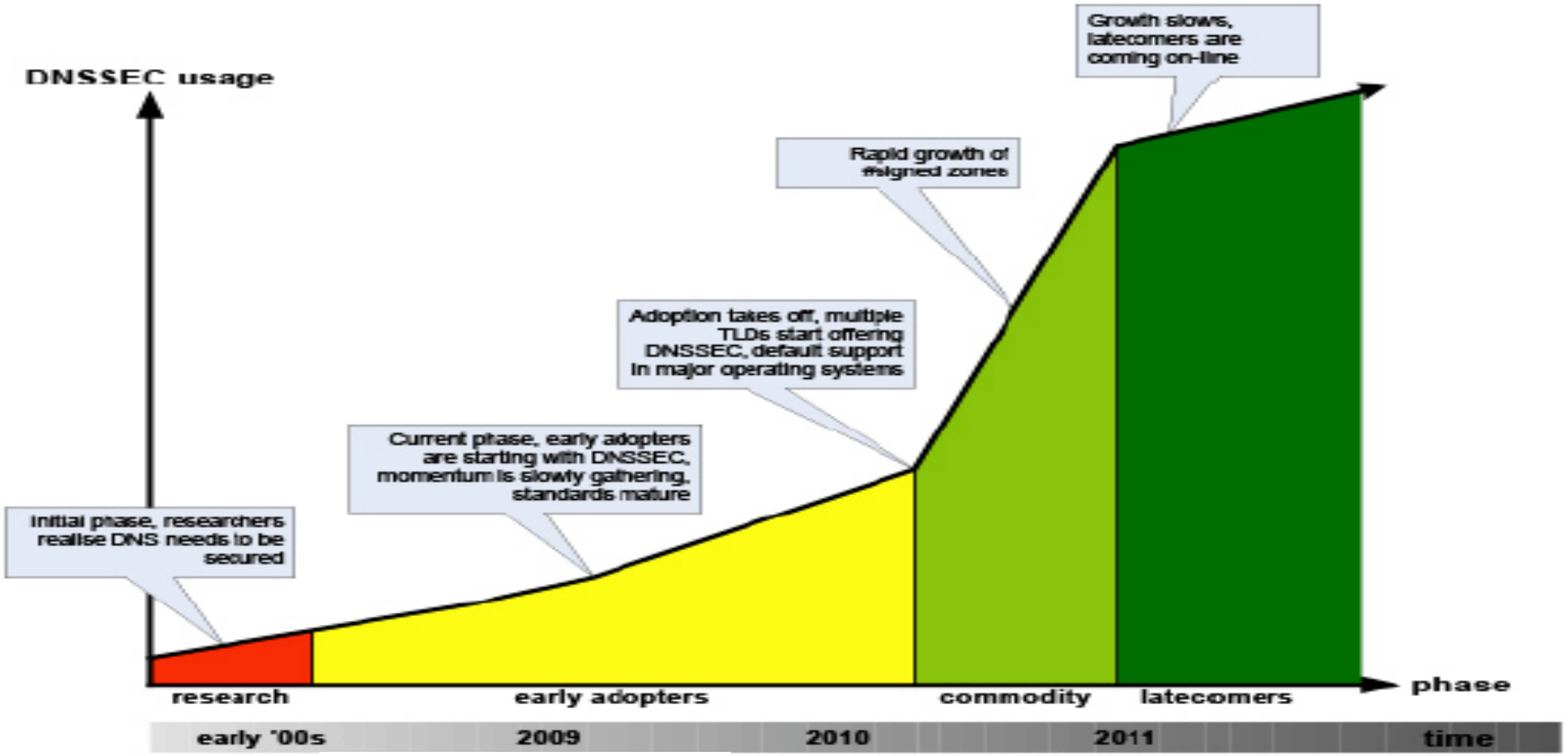
Internet Hardening
DNSSEC: Problems

- Complex to implement.
- A lot of debate about the "Root Sign" .
- DNSSEC zone files are very big, and hence loading the network & slowing the Internet operations as believed.
- When vulnerabilities are found in DESSEC, the large record sizes would aid any DoS attacks.
- The public/private keys used with DNSSEC can be hacked with time. So keys should be changed regularly to reduce compromise risk. Hence Data Confidentiality is NOT provided.
- Authentication is based on the root keys being known. It will be difficult to regularly change the root keys without impacting the DNSSEC structure.
- Currently, DNSSEC has a "bootstrap problem"; i.e. people typically ONLY deploy a technology if they receive an immediate benefit. To address these challenges, significant effort is ongoing to deploy DNSSEC globally as the Internet is so vital

Internet Security

Internet Hardening
DNSSEC: Timeline: 4 Phases

1. Research 2. Early Adopters 3. Commodity 4. Late Comers



Internet Security

Internet Hardening
DNSSEC: Your Organization Strategy?

1. When to Start?

- Sooner or later! Recommended:
- Phase 2: Early Adopters: Universities, research institutions, ISPs, banks and some top-level registrar
- Phase 3: Commodity: All Organizations even those who do NOT have their own domain names
- Phase 4: Late Comers: NOT recommended as you will be likely susceptible to attacks!

2. What to Start With?

- Enabling DNSSEC on all recursive caching Name-Servers
- Signing the zones on the authoritative Name-Servers
- Update or replace your Resolvers to validate DNSSEC information from zones already DNSSEC enabled. Many (commercially) available Resolvers already support DNSSEC
- Once the Resolver infrastructure is in place, you can start signing your zones and publishing the DNSSEC enabled zones on your primary name servers.

Internet Hardening
DNSSEC: Conclusions & What's Next?

- DNSSEC provides trust in DNS responses. NOT everybody has to participate at once to make DNSSEC work . DNSSEC design allows starting anywhere within the DNS hierarchy. Organizations can start now, without waiting for others. The more organizations adopt DNSSEC, the stronger it becomes.
- Although DNSSEC is complex, there is NO other option in the long run.
- Managing DNSSEC is different from managing DNS. DNSSEC is becoming easier every day. Appliances are already starting to appear on the market (including open source initiatives such as OpenDNSSEC). Tooling is also maturing quickly, rapidly making it easier to automate many of the harder tasks in DNSSEC. And recently third parties have started offering hosted DNSSEC.
- To make the Internet safer, DNSSEC should be adopted by everyone. Thus, organizations must start deploying it. Implementing DNSSEC will enable an organization to secure its own domain, and to validate DNS data from others.
- Get Involved! Prepare: Download: Pilot: Educate: Deploy:

Internet Hardening
DNSSEC: New Shots: March 2009

- Dot-GOV is first signed gTLD, making it the first operationally active DNSSEC signed zone. For more details please look at www.dotgov.gov/dnssecinfo.aspx
- Internet 2 JointTechs on DNSSEC. Look at presentations at www.events.internet2.edu/speakers/speakers.php?go=people&id=80
- Microsoft published DNSSEC deployment guides:
- http://www.microsoft.com/downloads/details.aspx?FamilyID=7a005a14-f740-4689-8c43-9952b5c3d36f&DisplayLang=en
- DNSSEC will be explained in Black Hat event in Amsterdam, Netherlands 14-15 April 2009. Stay tuned! https://www.blackhat.com/html/bh-europe-09/train-bh-eu-09-pw-pn-DNSSEC.html

EREN

(Emerging Research & Education Networks)

EREN

Index:

- Quick Facts:
  - Why Needed?
- Some Highlights:
  - Internet 2
  - EUMEDCONNECT 2
- What's Next?

Why Needed?

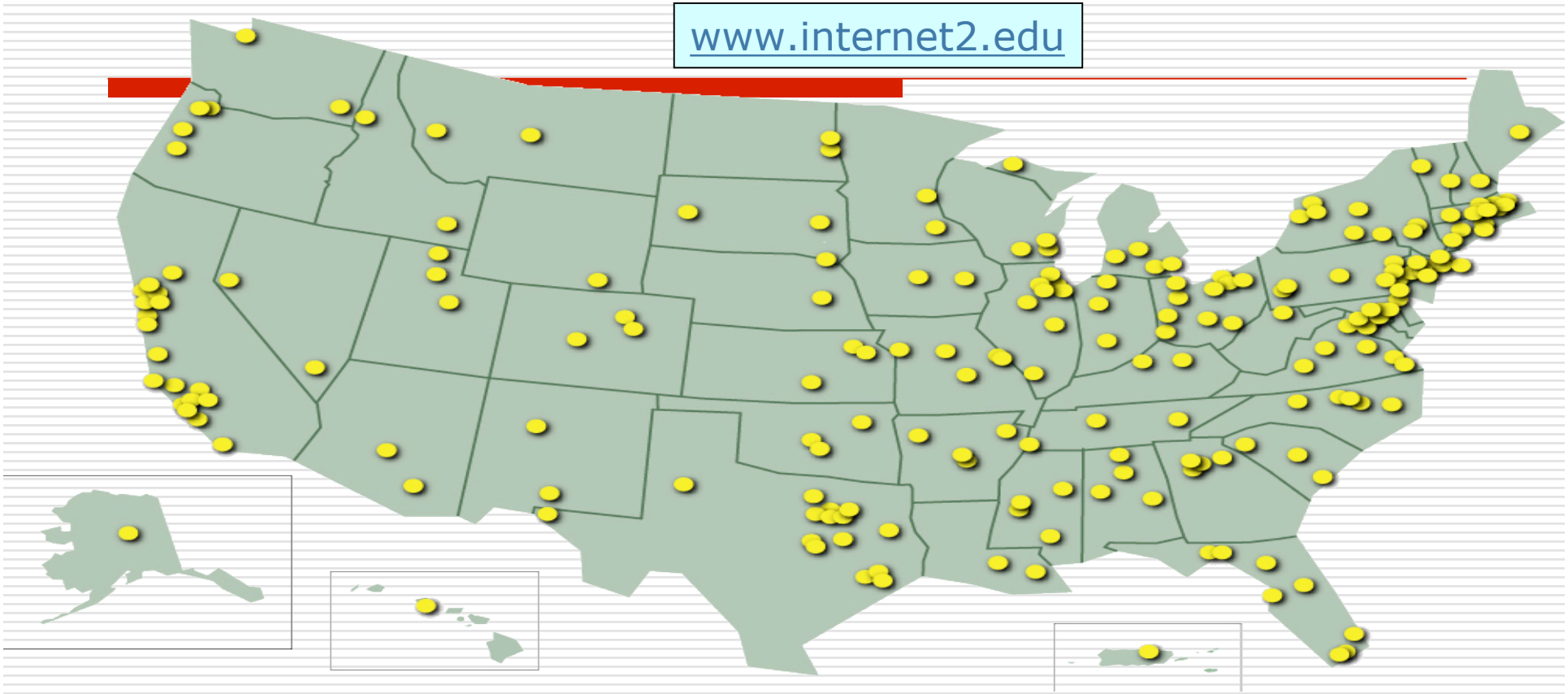
- Provide services still NOT affordable from the commercial Internet:
  - Multicast, IPv6
- Pioneer advanced services and support innovative network usage
- Enable diverse researchers to collaborate in different programs
- To let you know of emerging global issues & problems as of today's Internet:
  - Security, QoS(Quality of service), Addressing (IPv4, IPv6), The exploding need for URLs, Spam, etc.

EREN

Internet 2

INTERNET2

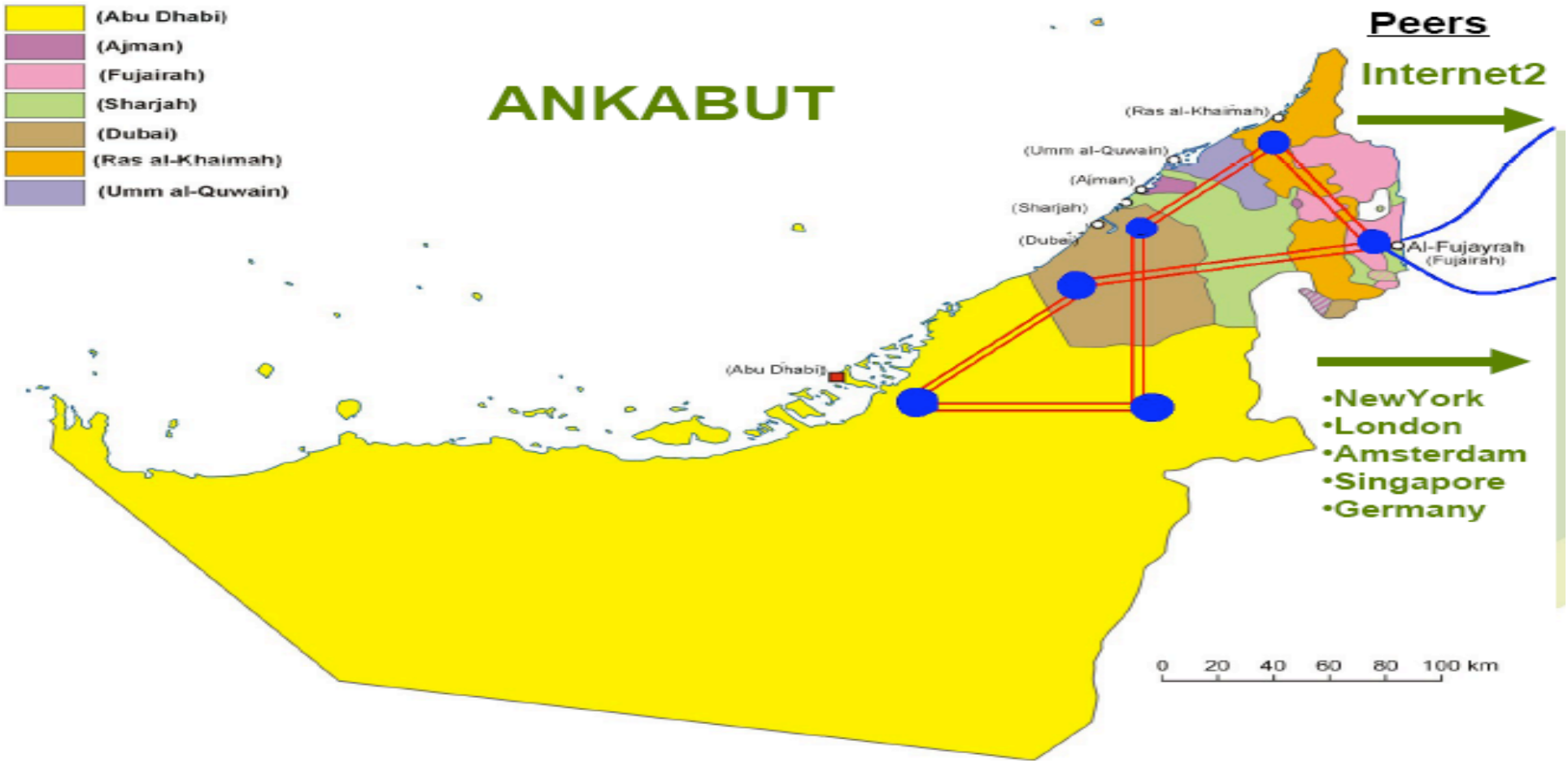
www.internet2.edu



212 University Members, 52 Corporate Members, 51 Affiliate Members, 31 R&E Network Members, 37 State Education Networks, 50 International Partners,. And Growing

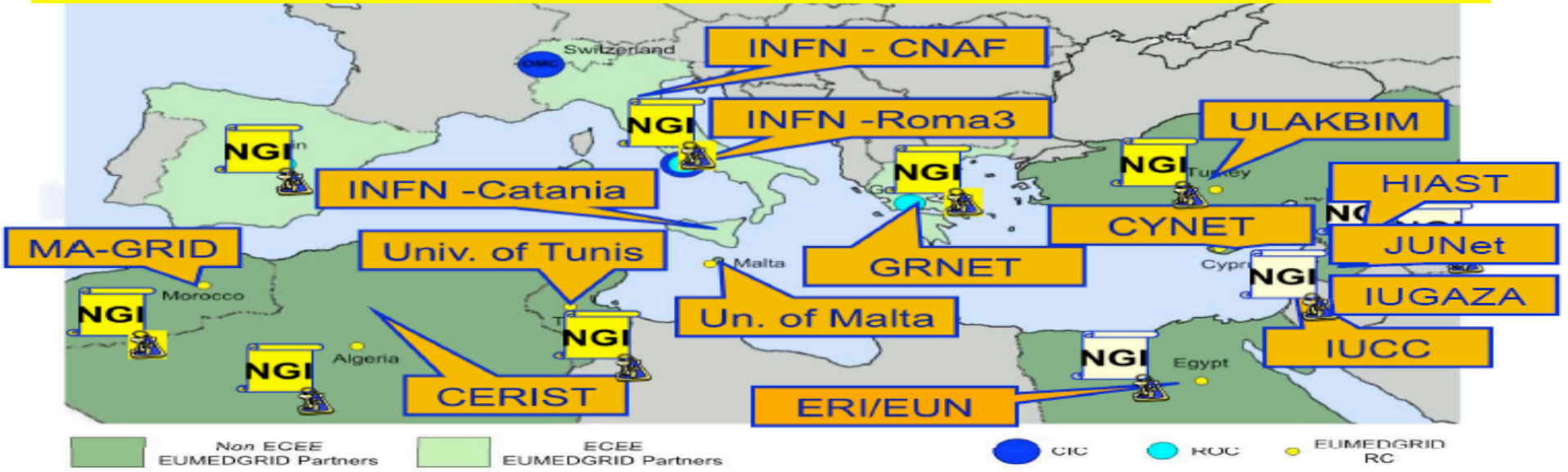
Internet 2: Regional

ANKABUT NREN : 1st Regional Connected to Internet2



EUMEDCONNECT 2

So far, 24 EUMEDGRID sites have been deployed in 13 countries, giving a total of 575 connected Servers and about 84 TBs of storage capacity



4000 academic / Research sites connected : ME Region also

www.eumedconnect2.net

What's Next?

- Explore related websites:
  - www.internet2.edu
  - www.eumedconnect2.net
- Subscribe to related mailing lists and SIG (Special Interest Groups) to attend virtual and physical events and updates:
  - middleeast-interest@internet2.edu
  - nren-sig@internet2.edu
- Download past events to see what hot issues & how to be engaged.
- You can form a local focus or WG to highlight regional Internet concerns and Q / A.
- Spread the words. Information should NOT stay ONLY on your HD! "Knowledge" is Power, & "Knowledge Share" is Success.
- Start Awareness Campaigns among your peers.

Thanks For your Attention

Questions?